МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 5

П Р И К А З

29.08.2022 г. № Ш5-13-779/2

г. Сургут

Об организации работ по защите персональных данных,
обрабатываемых в информационных системах
персональных данных

Во исполнении требований Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», в рамках реализации работ по защите персональных данных, обрабатываемых в информационных системах персональных данных, во исполнение постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке и информационных системах персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить:
   - Перечень ИСПДн (Приложение 1);
   - Порядок доступа в помещения, в которых ведется обработка ПДн в ИСПДн (Приложение 2);
   - Правила парольной защиты (Приложение 3);
   - Правила антивирусной защиты (Приложение 4);
   - Правила обновления общесистемного и прикладного программного обеспечения ИСПДн (Приложение 5);
   - Порядок работы с электронным журналом обращений пользователей информационной системы к ПДн (Приложение 6);
   - Порядок предоставления информации органам государственной власти и местного самоуправления, физическим и юридическим лицам; обработки запросов субъекта персональных данных или уполномоченного органа по защите прав субъекта персональных данных (Приложение 7);
   - Порядок проведения служебного расследования, нарушений режима информационной безопасности ИСПДн (Приложение 8);
   - Порядок приостановки предоставления доступа к ПДн в случае обнаружения нарушений порядка их обработки (Приложение 9);

- Порядок уничтожения носителей персональных данных (Приложение 10).

2. Утвердить инструкции:
   - Инструкцию по учету лиц, допущенных к работе с персональными данными (Приложение 11);
   - Инструкцию ответственному за организацию работ по обработке ПДн (Приложение 12);
   - Инструкцию администратору безопасности информации (Приложение 13);
   - Инструкцию пользователю ИСПДн (Приложение 14);
   - Инструкцию по учету машинных носителей информации (Приложение 15);
   - Инструкция по организации резервирования и восстановления программного обеспечения, работоспособности технических средств, баз персональных данных информационных систем персональных данных (Приложение 16).
3. Утвердить формы журналов:
   - Журнал учета машинных носителей персональных данных (Приложение 17);
   - Журнал периодического тестирования средств защиты информации (Приложение 18);
   - Журнал инструктажа персонала (Приложение 19);
   - Журнал учета мероприятий по защите персональных данных (Приложение 20);
   - Журнал о событиях безопасности (Приложение 21);
   - Журнал учета средств защиты информации, эксплуатационной и технической документации к ним (Приложение 22);
   - Журнал учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн (Приложение 23);
   - Журнал учета процедуры резервного копирования (Приложение 24);
   - Перечень событий безопасности, критичных для функционирования информационной системы, определения состава и содержания информации о событиях безопасности (Приложение 25).

4. Назначить заместителя директора по УВР, С.З. Абдулжалиеву, ответственным за организацию работ по обработке ПДн.

5. Ответственному за организацию работ по обработке ПДн в своей деятельности руководствоваться инструкцией ответственного за организацию работ по обработке ПДн.

6. Назначить техника, Латыпову Маргариту Фаритовну, администратором безопасности информации.

7. Администратору безопасности информации в своей деятельности руководствоваться инструкцией администратора безопасности информации.

8. Ответственному за организацию обработки персональных данных подать уведомление оператора об обработке ПДн в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по

Сибирскому федеральному округу, а также поддерживать актуализацию уведомления.

9. Контроль исполнения приказа оставляю за собой.

Директор

Подписано электронной подписью
Сертификат:
3A87F1D9FD6BA452E7A054E60B3942E381262401
Владелец:
Петкова Наталья Юрьевна
Действителен: 08.10.2021 с по 08.01.2023

Н.Ю. Петкова

Приложение 1
к Приказу от 29.08.2022 г.
№ Ш5-13-779/2

Перечень информационных систем персональных данных (ИСПДн)

№ п/п	Наименование ИСПДн	Место расположения ИСПДн	Структура ИСПДн	Наличие подключений к ССОП и сетям МИО (Интернет)	Режим обработки ПДн	Разграничение доступа пользователей	Нахождение ИСПДн (ее составных частей) в пределах России	Уровень защищенности ИСПДн
1	ФИС ФРДО	628418, Российская Федерация, Тюменская область, Ханты-Мансийский Автономный округ - Югра, г. Сургут, ул. Пушкина, д.15/1	Локальная система	Имеется	Однопользователь-ский	С разграничением прав	Все технические средства и БД ИСПДн находятся на территории РФ	УЗ 3

Приложение 2
к Приказу от 29.08.2022 г.
№ Ш5-13-779/2

Порядок доступа в помещения, в которых ведется обработка ПДн в ИСПДн

Порядок разработан в соответствии с требованиями Приказа ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Порядок доступа в помещения

В помещения допускаются лица, согласно утвержденному перечню.

Ответственность в рабочее время за исключение неконтролируемого доступа третьих лиц в помещения, где ведется работа в ИСПДн, несут сотрудники, допущенные в данные помещения, при этом запрещается оставлять помещения, в случае отсутствия в них Работников, незакрытыми или с ключами в дверях.

Контроль и управление физическим доступом осуществляется ответственным за организацию обработки персональных данных.

Сотрудники, ведущие обработку информации на автоматизированных рабочих местах, размещают экраны мониторов так, чтобы исключить возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны.

По возможности исключаются случаи размещения устройства вывода (отображения, печати) информации напротив оконных проемов, входных дверей, технологических отверстий, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра.

Список лиц, имеющих доступ в помещения, где расположены информационные системы персональных данных

Лица, являющиеся работниками МБОУ СОШ №5 (далее Оператор) и имеющие права доступа к информационным системам персональных данных Оператора, имеют право бесконтрольного допуска в помещения, в которых расположены их рабочие места или допуск в которые необходим для выполнения своих трудовых обязательств.

Допуск лиц, не имеющих права доступа к информационным системам персональных данных Оператора, в помещения, где расположены информационные системы персональных данных, осуществляется только в сопровождении ответственных лиц или других работников Оператора, имеющих право посещения данного помещения.

Приложение 3
к Приказу от 29.08.2022
№ Ш5-13-779/2

Правила парольной защиты

1. Общие положения

Целью применения и реализации Правил парольной защиты является недопущение утечки ПДн, а также их несанкционированной модификации или уничтожения. Правила действуют для всех пользователей и администраторов ИСПДн оператора.

Правила парольной защиты регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в ИСПДн, а также контроль над действиями пользователей при работе с паролями.

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 ПДн.

Личные пароли должны генерироваться и распределяться централизованно, либо создаваться пользователями ИСПДн самостоятельно с учетом следующих требований:

- пароль должен быть не менее 6-ти символов;
- в числе символов пароля ***обязательно должны присутствовать*** буквы в верхнем и нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от значений 24-х предыдущих паролей;
- максимальный срок действия пароля пользователя составляет 120 дней;
- минимальный срок действия пароля пользователя составляет 2 дня;
- пользователь не имеет права сообщать личный пароль другим лицам (разрешается только с согласования администратора безопасности при наличии технологической необходимости использования имен и паролей работников в их отсутствие в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п. По возвращению работники обязаны сразу же сменить своих пароли на новые значения).

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.

Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в квартал.

Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри МБОУ СОШ №5 и т.п.) должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой на основании письменного указания начальника отдела.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри МБОУ СОШ №5 и другие обстоятельства) ответственного за обеспечение безопасности ПДн или администратора безопасности ПДн.

2. Контроль

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

Приложение 4
к Приказу от 29.08.2022
№ Ш5-13-779/2

Правила антивирусной защиты

1. Общие требования

Правила антивирусной защиты определяют требования к организации защиты ИСПДн от разрушающего воздействия вредоносных программ и устанавливают ответственность руководителя и Работников, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

Целью защиты ИСПДн от вредоносных программ является предотвращение и нейтрализация негативных воздействий вредоносных программ на средства вычислительной техники.

К использованию в ИСПДн допускаются только лицензионные по требованиям безопасности информации средства защиты от вредоносных программ.

Установка и начальная настройка средств защиты от вредоносных программ в ИСПДн осуществляется представителями организации – лицензиата ФСТЭК России или администратором безопасности ПДн, обслуживание – администратором безопасности ПДн.

Администратор безопасности ПДн должен организовывать осуществление периодического обновления сигнатур средств защиты от вредоносных программ и контроль их работоспособности не реже чем один раз в неделю.

Пользователи ИСПДн обязаны руководствоваться в работе настоящими правилами антивирусной защиты и «Инструкцией пользователя ИСПДн».

2. Применение средств защиты от вредоносных программ

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

В ИСПДн запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

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.) пользователь самостоятельно (или вместе с администратором безопасности ПДн) должен провести внеочередной антивирусный контроль своего персонального компьютера.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу персонального компьютера;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности ПДн;
- провести «лечение» или удаление зараженных файлов.

3. Ответственность

Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями Настоящих Правил возлагается на администратора безопасности ПДн.

Ответственность за проведение мероприятий антивирусной защиты ИСПДн и соблюдение требований Настоящих Правил возлагается на ответственного за обеспечение безопасности в организации, администратора безопасности ПДн и всех пользователей ИСПДн.

Приложение 5
к Приказу от 29.08.2022
№ Ш5-13-779/2

Правила обновления общесистемного и прикладного программного обеспечения ИСПДн

1. Общие положения

В системе управления ИСПДн должна обеспечиваться и регламентироваться деятельность, связанная с установкой нового оборудования, либо его компонентов, патчей, а также обновлений операционных систем (далее – ОС) и других приложений.

Тестирование нового оборудования и обновлений программного обеспечения (далее – ПО) не должно осуществляться на ресурсах действующей информационной инфраструктуры.

Правила и порядок обновления ПО, ОС и приложений в целях информационной безопасности ИСПДн направлены на защиту ресурсов от:

- нарушения штатной работы информационных ресурсов и сервисов;
- разрушения;
- нарушения штатного функционирования оборудования;
- несанкционированной модификации;
- несанкционированного копирования.

2. Правила управления обновлениями ПО ИСПДн в информационной инфраструктуре оператора.

Отслеживание появления новых уязвимостей в используемой ОС, появление патчей, изготовленных производителями с целью устранения указанных уязвимостей, должно регламентироваться и производиться в плановом порядке.

Установке патчей должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий от вновь устанавливаемых патчей.

В случае обнаружения негативного воздействия, устанавливаемого патча на штатное функционирование информационной инфраструктуры, данный патч устанавливаться не должен.

Установке новых версий ПО или внесению изменений и дополнений в действующее ПО должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий указанного ПО.

Установка протестированных патчей может быть произведена только на основании решения администратора безопасности ПДн.

Установка новых версий ПО или внесение изменений и дополнений в действующее ПО может быть произведено только по согласованию с администратором безопасности ПДн.

Применение организационно-технических и/или аппаратно-программных решений может быть произведено только по согласованию с администратором безопасности ПДн.

3. Контроль

Контроль за выполнением требований Настоящих Правил должен осуществлять администратор безопасности ПДн в МБОУ СОШ №5.

Приложение 6
к Приказу от 29.08.2022
№ Ш5-13-779/2

Порядок работы с электронным журналом обращений пользователей информационной системы к ПДн

1. Общие положения

Правила и порядок протоколирования и анализа (аудита) значимых событий в информационной системе персональных данных (далее – ИСПДн), направлены на превентивную фиксацию и изучение действий субъектов и объектов в ИСПДн.

Все события, происходящие в операционной системе, ИСПДн, других критических приложений и средствах защиты информации должны протоколироваться в специальные электронные журналы аудита.

Аудит событий, зафиксированных в указанных электронных журналах, должен анализироваться в плановом порядке на постоянной основе.

Требования к аудиту подразделяются на четыре группы:

- защита и управление доступом к системному журналу событий;
- определение множества подлежащих регистрации событий;
- фиксация и хранение зарегистрированных событий в журнале;
- анализ журнала событий и формирование отчетов.

2. Настройки безопасности систем аудита

Электронные журналы аудита должны записываться и вестись в автоматизированном режиме.

Настройки журналов аудита должны однозначно интерпретировать все значимые события ИСПДн.

Электронные журналы аудита не должны быть доступны на чтение, уничтожение и модификацию пользователям ИСПДн.

Электронные журналы аудита должны быть доступны на чтение и архивирование сотруднику, выполняющему функции ответственного за обеспечение безопасности персональных данных.

Затирание старых событий журнала происходит по необходимости по мере заполнения журнала.

3. Контроль

Контроль выполнения положений и требований порядка работы с электронным журналом обращений пользователей информационной системы к персональным данным должен осуществлять администратор безопасности персональных данных в МБОУ СОШ №5.

Приложение 7
к Приказу от 29.08.2022
№ Ш5-13-779/2

Порядок предоставления информации органам государственной власти и местного самоуправления, физическим и юридическим лицам; обработки запросов субъекта персональных данных или уполномоченного органа по защите прав субъекта персональных данных.

1. Общие положения

Оператор - Муниципальное бюджетное общеобразовательное учреждение средняя общеобразовательная школа №5, должен предоставлять информацию, содержащую персональные данные (далее – ПДн) субъекта, третьим лицам только с письменного согласия субъекта ПДн за исключением случаев, предусмотренных частью 2 статьи 9 Федерального Закона от 27.07.2006 №152-ФЗ «О персональных данных».

Информация, содержащая ПДн субъекта и предоставляемая третьим лицам, должна быть достоверной и не избыточной, по отношению к целям, заявленным этими лицами, при сборе ПДн.

При передаче обработки ПДн другому лицу на основании договора, оператор должен зафиксировать в нем обязанность указанного лица в обеспечении конфиденциальности ПДн и безопасности данных при их обработке.

2. Предоставление информации по обращению субъекта персональных данных

Все обращения субъектов ПДн регистрируются в «Журнале регистрации обращений субъектов персональных данных», утвержденный Приказом о политике в отношении обработки ПДн.

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

1. подтверждение факта обработки персональных данных оператором;
2. правовые основания и цели обработки персональных данных;
3. цели и применяемые оператором способы обработки персональных данных;
4. наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
5. обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
6. сроки обработки персональных данных, в том числе сроки их хранения;
7. порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;
8. информацию об осуществленной или о предполагаемой трансграничной передаче данных;
9. наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
10. иные сведения, предусмотренные Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» или другими федеральными законами.

Оператор при обращении к нему субъекта ПДн или его законного представителя обязан сообщить субъекту ПДн или его представителю информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с этими ПДн в течение тридцати дней с даты получения запроса субъекта ПДн или его представителя. Или отказать в предоставлении информации субъекту ПДн или его представителю предоставив в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» или иного федерального

закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса.

Оператор обязан предоставить безвозмездно субъекту ПДн или его представителю возможность ознакомления с ПДн, относящимися к этому субъекту ПДн:

- В срок, не превышающий семи рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения.
- В срок, не превышающий семи рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие ПДн.

3. Трансграничная передача данных

При трансграничной передаче ПДн оператор должен руководствоваться положениями статьи 12 №152-ФЗ «О персональных данных».

4. Предоставление информации по обращению уполномоченного органа по защите прав субъекта персональных данных

Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных необходимую информацию в течение тридцати дней с даты получения запроса.

5. Контроль

Контроль выполнения положений и требований порядка обработки запросов субъекта ПДн или уполномоченного органа по защите прав субъекта ПДн, должен осуществлять ответственный за организацию работ по обработке ПДн Оператора.

Приложение 8
к Приказу от 29.08.2022
№ Ш5-13-779/2

Порядок проведения служебного расследования, нарушений режима информационной безопасности информационной системы персональных данных

1. Общие положения

Данный порядок устанавливает правила классификации нарушений информационной безопасности и процедуры служебного расследования (назначения, проведения и выработки выводов) для определения уровня защищенности информационной системы персональных данных (далее – ИСПДн) МБОУ СОШ №5 (далее Оператор) и мер по возможному предотвращению инцидентов информационной безопасности.

2. Классификация инцидентов информационной безопасности

Нарушения режима информационной безопасности и их последствия классифицируются по значимости на:

- Нарушения I категории.
- Нарушения II категории.
- Нарушения III категории.

Служебное расследование назначается по нарушениям I и II категорий.

3. Перечень инцидентов информационной безопасности

Инциденты I категории, к каковым относятся нарушения, повлекшие за собой разглашение (утечку) защищаемых персональных данных (далее – ПДн) и/или утрату содержащих их отчуждаемых носителей, уничтожение (искажение) ИСПДн, выведение из строя технических и программных средств, а именно:

- подбор административного пароля (успешный);
- несанкционированная реконфигурация параметров ИСПДн;
- утрата или кража резервной копии базы ПДн;
- необоснованная передача массивов ПДн;
- умышленное нарушение работоспособности ИСПДн;
- несанкционированный доступ к ПДн ИСПДн;
- несанкционированное внесение изменений в ИСПДн;
- умышленное заражение компьютеров и серверов ИСПДн вирусами;
- проведение работ с ИСПДн, повлекшее за собой необратимую потерю данных.

Инциденты II категории, к каковым относятся: нарушения, в результате которых возникают предпосылки к разглашению (утечке) защищаемых ПДн, утрате содержащих их отчуждаемых носителей, уничтожению (искажению) ИСПДн, выведению из строя технических и программных средств, а именно:

- ошибка при входе в ИСПДн (набор не назначенного пароля, более трех раз подряд, периодически);
- несанкционированное (неоднократное) оставление включенного персонального компьютера (далее – ПК);
- перезагрузка компьютера, при сбоях в работе ПК, (неоднократная) в т.ч. аварийная (неоднократная) перезагрузка, путем нажатия кнопки RESET;
- утрата учтенного отчуждаемого съемного носителя;
- попытка входа под чужим именем, паролем, многократная неудачная;
- попытка входа под чужим именем пользователя, паролем, удачная;
- несанкционированная очистка журналов аудита;
- несанкционированное копирование ПДн на внешние носители;
- несанкционированная установка (удаление) программного обеспечения (далее – ПО) ИСПДн;

– несанкционированное изменение конфигурации ПО ИСПДн;
– попытка получения прав администратора на локальном ПК (увеличения собственных прав, получение прав на отладку программ) удачная и неудачная;
– попытка получения прав администратора в домене или на удаленной машине удачная и неудачная;
– неумышленное заражение локального или сетевого ПК компьютерными вирусами;
– несанкционированное использование сканирующего ПО;
– несанкционированное использование анализаторов протоколов (снифферов);
– несанкционированный просмотр, вывод на печать и т.п. ПДн.

Инциденты III категории, к каковым относятся нарушения, не несущие признаков нарушений I и II категорий, а именно:
– ошибка при входе в ИСПДн (набор неправильного пароля, сетевого имени более трех раз подряд, не периодическая);
– попытка неудачного доступа к ПДн ИСПДн (периодическая);
– перевод времени на ПК;
– выполнение собственных производственных обязанностей на компьютере в неразрешенное время;
– перезагрузка компьютера, при сбоях в работе ПК, (однократная) в т.ч. аварийная перезагрузка, путем нажатия кнопки RESET;
– нецелевое использование корпоративных ресурсов (печать, Internet, mail, и т.п.).

4. Назначение и проведение служебного расследования

Служебное расследование назначается по нарушениям I и II категорий.

Состав комиссии, а также сроки проведения служебного расследования назначаются распоряжением сотрудника, ответственного за обеспечение безопасности ПДн, по каждому отдельному факту нарушения или по факту группы нарушений.

Служебное расследование может быть инициировано на основании устного заявления, докладной или служебной записки любого сотрудника оператора по выявленному отдельному факту нарушения, либо по факту группы нарушений.

5. Состав комиссии для проведения служебного расследования

В состав комиссии входят лица, назначенные приказом «О создании комиссии для организации работы по защите персональных данных».

В случае необходимости Председатель комиссии может привлекать к работе:
– администраторов управления информатизации и телекоммуникаций;
– непосредственного начальника нарушителя;
– экспертов из других подразделений;
– привлеченных специалистов организаций-лицензиатов.

6. Члены комиссии имеют право:

Требовать документального подтверждения факта нарушений информационной безопасности ИСПДн Оператора.

Устанавливать причины допущенных нарушений любым из способов, не противоречащим законодательству РФ.

Брать письменные объяснения по поводу выявленных нарушений у любого сотрудника оператора.

7. Ответственность.

Ответственность за выявление и классификацию инцидента информационной безопасности, требующего проведения процедуры служебного расследования несет администратор безопасности ПДн.

Ответственность за назначение процедуры служебного расследования несет Директор Оператора.

Ответственность за проведение процедуры служебного расследования несет администратор безопасности ПДн в ИСПДн Оператора.

Ответственность за содержание, обоснованность, актуализацию Настоящего Порядка, а также надлежащее выполнение его положений несет ответственный за обеспечение безопасности ПДн.

8. Оформление результатов работы комиссии

Результаты работы Комиссии должны быть оформлены в виде аналитического экспертного заключения на имя руководителя, ответственного за обеспечение безопасности ПДн, с предложениями по необходимым организационным выводам, а также по расширению или дополнению «Примерного перечня нарушений».

Результатом работы Комиссии должен стать АКТ, в котором изложены:

- документальное подтверждение факта нарушений информационной безопасности ИСПДн Оператора;
- установленные причины выявленных нарушений в ИСПДн Оператора;
- сформированные предложения по устранению причин выявленных инцидентов информационной безопасности в ИСПДн Оператора.

Приложение 9
к Приказу от 29.08.2022
№ Ш5-13-779/2

Порядок приостановки предоставления доступа к персональным данным в случае обнаружения нарушений порядка их обработки

1. Общие положения

Целью установления Настоящего Порядка является предотвращение утечки и несанкционированного доступа к персональным данным (далее – ПДн) при выявлении нарушений режима безопасности при обработке и/или чтении ПДн в информационной системе персональных данных (далее – ИСПДн).

Работа с ПДн должна приостанавливаться только при обнаружении нарушений I и/или II категорий.

2. Действие должностных лиц в случае обнаружения нарушений

Сотрудник, обнаруживший нарушения при работе с ПДн обязан сообщить об этом своему непосредственному руководителю.

Администратор безопасности ПДн в ИСПДн МБОУ СОШ №5, обязан:

- установить категорию выявленного нарушения;
- при установлении I или II категории нарушения инициировать проведение служебного расследования;
- оповестить все отделы и Работников, работающих с ПДн о прекращении доступа к ресурсам ИСПДн на время проведения служебного расследования.

Все отделы и сотрудники, работающие с ПДн обязаны:

- временно (на время проведения служебного расследования) приостановить свою деятельность по работе с ИСПДн;
- содействовать проведению служебного расследования.

Работа с ПДн может возобновляться только после устранения всех выявленных нарушений, их последствий.

Информация о возможности возобновления работы с ИСПДн должна доводиться до всех заинтересованных подразделений лицом, установившим запрет на работы в ИСПДн.

Приложение 10
к Приказу от 29.08.2022
№ Ш5-13-779/2

Порядок уничтожения носителей персональных данных в МБОУ СОШ №5

(далее – Оператор)

1. Работа с бумажными носителями (документами)

По окончании срока хранения бумажные носители уничтожаются путём измельчения на мелкие части, исключающие возможность последующего восстановления информации, или сжигаются.

2. Работа с машиночитаемыми носителями

Виды и периоды уничтожения персональных данных, хранимых в электронном виде («файлах») на жестком диске компьютера (далее - НЖМД) и машиночитаемых носителях: компакт дисках (далее – CD-R/RW, DVD-R/RW в зависимости от формата), приведены в таблице 1.

Таблица 1

№ п/п	Информация, вид носителя	Срок хранения	Действия по окончании срока хранения
1	Базы данных ИСПДн: – Носитель: файлы на НЖМД сервера с БД ИСПДн.	До достижения целей обработки ПДн.	Удаление файла с НЖМД

По окончании указанных в Таблице 1 сроков хранения, подлежащие уничтожению файлы с персональными данными, удаляются средствами автоматизированного комплекса, использующегося для обработки персональных данных. Машиночитаемые носители, подлежащие уничтожению, физически уничтожаются с целью невозможности восстановления и дальнейшего использования. Это достигается путём деформирования, нарушения единой целостности носителя или его сжигания.

В случае допустимости повторного использования носителя формата FDD, CD-RW, DVD-RW, применяется программное удаление («затирание») содержимого диска путём его форматирования с последующей записью новой информации на данный носитель.

3. Порядок оформления документов об уничтожении носителей

В ходе процедуры уничтожения носителей необходимо присутствие членов экспертной комиссии, осуществляющей уничтожение персональных данных и иной конфиденциальной информации.

Уничтожение носителей, содержащих персональные данные осуществляет экспертная комиссия, утверждённая директором Оператора.

В состав экспертной комиссии по уничтожению носителей, содержащих персональные данные, входят:

- руководители структурных подразделений Оператора, использующих носители персональных данных, выделенные для уничтожения;
- администратор безопасности Оператора;
- сотрудник, ответственный за организацию работ по обработке персональных данных.

После осуществления работ по уничтожению носителей, выделенных для уничтожения, комиссия составляет и подписывает соответствующий акт об уничтожении носителей персональных данных.

Приложение 1
к Порядку уничтожения носителей персональных данных в МБОУ СОШ №5

УТВЕРЖДАЮ
Директор
МБОУ СОШ №5

_____ Н. Ю. Петкова

« ___ » _____ 202 г.

Акт о выделении носителей персональных данных и персональных данных с их носителей на уничтожение

Комиссия в составе:

	ФИО	Должность
Председатель		
Члены комиссии		

провела отбор носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации _____информация, записанная на них в процессе эксплуатации, подлежит гарантированному уничтожению (опись прилагается):

№ п/п	Дата	Тип носителя	Регистрационный номер носителя ПДн	Примечание
1				
2				
3				
4				

Всего носителей _____ (_____)
(цифрами и прописью)

Председатель комиссии: _____/_____/

Члены комиссии: _____/_____/
_____/_____/
_____/_____/

Приложение 2
к Порядку уничтожения носителей персональных данных в МБОУ СОШ №5

УТВЕРЖДАЮ
Директор
МБОУ СОШ №5

_____ Н. Ю. Петкова

« ___ » _____ 202 г.

Акт уничтожения носителей персональных данных и персональных данных с их носителей

Комиссия в составе:

	ФИО	Должность
Председатель		
Члены комиссии		

составила настоящий акт о том, что согласно описи, утвержденной актом №____ от _____ 20__ года, были уничтожены отобранные носители персональных данных, информация на которых, подлежит гарантированному уничтожению в соответствии с требованиями руководящих документов по защите информации _____:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя ПДн	Примечание
1				
2				
3				
4				

Всего носителей _____ (_____)
(цифрами и прописью)

Перечисленные носители ПДн уничтожены путем _____.
(разрезания, сжигания, механического уничтожения,
сдачи предприятию по утилизации вторичного сырья и т.п.)

Председатель комиссии: _____/_____/

Члены комиссии: _____/_____/
_____/_____/
_____/_____/

Приложение 11
к Приказу от 29.08.2022
№ Ш5-13-779/2

Инструкция по учету лиц, допущенных
к работе с персональными данными в информационных системах персональных данных
МБОУ СОШ №5

1. Общие сведения

1.1 Настоящая инструкция разработана в соответствии с требованиями Положения об утверждении требований к защите персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн), утвержденного Постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 и определяет порядок учета лиц, допущенных к работе с ПДн в ИСПДн.

1.2 Настоящая инструкция определяет порядок допуска Работников и третьих лиц к ПДн, обрабатываемым в информационной системе Оператора, а также их уровень прав доступа к обрабатываемым ПДн в ИСПДн Оператора.

1.3 Основанием для допуска Работников и третьих лиц к ПДн является должностная инструкция пользователя ИСПДн и трудовой договор.

1.4 Основанием для прекращения допуска Работников и третьих лиц к ПДн является прекращение трудовых отношений.

1.5 Допуск лиц к работе с ПДн в ИСПДн осуществляется в соответствии со списком лиц, утвержденным Приказом «Об утверждении положения о защите персональных данных работников.

1.6 К работе допускаются лица, ознакомившиеся с руководящими документами по защите ПДн и прошедшие инструктаж.

1.7 Учет лиц, допущенных к работе с ПДн в ИСПДн, ведется в журнале инструктажа персонала (Приложение 19).

2. Действия по учету лиц, допущенных к работе с ПДн в ИСПДн.

2.1 Руководители структурных подразделений предоставляют сотруднику ответственному за организацию работ по обработке ПДн список Работников, доступ которых к ПДн, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей.

2.2 Сотрудник ответственный за организацию работ по обработке ПДн в соответствии с полученным списком из пункта 1 составляет список лиц, имеющих доступ к ИСПДн, и передает директору Оператора на утверждение.

2.3 Лица, допущенные к ИСПДн должны расписаться в журнале инструктажа персонала.

Приложение 12
к Приказу от 29.08.2022
№ Ш5-13-779/2

Инструкция ответственному за организацию работ по обработке ПДн

1. Общие положения

1.1 Инструкция ответственного за организацию обработки персональных данных (далее – инструкция) определяет основные обязанности и права ответственного за организацию обработки персональных данных (далее – ПДн).

1.2 Инструкция регулирует отношения и порядок взаимодействия между ответственным за организацию обработки ПДн и работниками Оператора, которые обрабатывают ПДн, в связи с реализацией трудовых отношений, в связи с оказанием услуг и осуществлением возложенных на них функций, а также в соответствии с действующим законодательством Российской Федерации, за исключением случаев, перечисленных в части 2 статьи 1 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

1.3 Ответственный за организацию обработки ПДн в своей деятельности руководствуется действующим законодательством Российской Федерации, а также настоящей должностной инструкцией.

2. Должностные обязанности

2.1 Ответственный за организацию обработки ПДн обязан:

– организовывать работу в структурных подразделениях по разработке и принятию организационно-распорядительной документации, устанавливать правила обработки ПДн, которые определяют:

- порядок доступа к ПДн;
- организацию приема и обработки обращений и запросов субъектов ПДн или их представителей;
- процедуры, направленные на предотвращение и выявление нарушений действующего законодательства Российской Федерации о ПДн и устранения последствий таких нарушений.

– организовывать ознакомление Работников, непосредственно осуществляющих обработку персональных данных, с действующим законодательством Российской Федерации о персональных данных и организационно-распорядительной документации, определяющими правила обработки персональных данных и требования по защите персональных данных:

- Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

– руководить осуществлением приема необходимых правовых, организационных и технических мер для защиты ПДн в соответствии с действующим законодательством Российской Федерации о ПДн;

– осуществлять согласование мероприятий при создании новых информационных систем персональных данных;

– организовать своевременное направление в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Сибирскому федеральному округу уведомления о намерении осуществлять обработку ПДн и изменения в него;

– организовывать и руководить проведением внутренних проверок организации состояния работ по вопросам информационной безопасности для осуществления периодического контроля:

- условий обработки ПДн и их соответствие действующему законодательству Российской Федерации о ПДн и принятыми в соответствии с ним организационно-распорядительной документации;
- организации приема и обработки и запросов субъектов ПДн или их представителей;
- выполнения, установленных в соответствии с действующим законодательством Российской Федерации и организационно-распорядительной документации, требований к защите ПДн;

– координировать работу структурных подразделений на принятие мер, направленных на совершенствование защиты обрабатываемых ПДн;

– осуществлять методическое руководство работой при разработке условий обработки ПДн и эффективности мер по защите ПДн;

– организовывать работу по планированию прохождения обучения Работников по вопросам обеспечения защиты ПДн.

3. Права

3.1 Ответственный за организацию обработки ПДн имеет право:

– запрашивать в структурных подразделениях, в которых ведется обработка ПДн или планируется ведение обработки ПДн, любые сведения, необходимые для организации условий обработки ПДн и принятия необходимых правовых, организационных и технических мер для защиты ПДн;

– принимать участие в рассмотрении жалоб и обращений граждан или юридических лиц по вопросам, связанным с обработкой ПДн, а также принимать решения по результатам рассмотрения указанных жалоб и обращений;

– участвовать в расследовании нарушений в области защиты ПДн и принимать решения по устранению недостатков и предупреждению подобного рода нарушений;

– требовать от структурных подразделений уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем ПДн, при обращении (запросе) субъекта ПДн или его представителя либо уполномоченного органа по защите прав субъектов ПДн, либо по результатам проведенной внутренней проверки организации состояния работ по вопросам информационной безопасности;

– принимать меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований действующего законодательства Российской Федерации о ПДн;

– вносить предложения о совершенствовании нормативного правового регулирования обработки и защиты ПДн.

4. Ответственность

Ответственный за организацию обработки ПДн несет ответственность за ненадлежащее выполнение возложенных на него обязанностей, изложенных в настоящей должностной инструкции, в соответствии с действующим законодательством Российской Федерации.

5. Заключительные положения

Инструкция подлежит пересмотру в случае изменения законодательства Российской Федерации о ПДн.

Приложение 13
к Приказу от 29.08.2022
№ Ш5-13-779/2

Инструкция администратору информационной безопасности

1. Общие положения

1.1. Настоящая инструкция определяет основные обязанности, права и ответственность администратора безопасности информации в информационных системах персональных данных (далее – ИСПДн).

1.2. Администратор безопасности информации назначается в соответствии с приказом директора МБОУ СОШ №5.

1.3. Администратор безопасности информации осуществляет контроль выполнения требований и организационных мероприятий по обеспечению защиты информации при использовании автоматизированных рабочих мест (далее – АРМ) дополнительно к своим непосредственным обязанностям.

2. Обязанности администратора безопасности информации ИСПДн

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

- Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2.2 Осуществлять установку, настройку и сопровождение средств защиты информации.

2.3 Вести журнал учета средств защиты информации, эксплуатационной и технической документации к ним (Приложение 22).

2.4 Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.

2.5 Вести журнал периодического тестирования средств защиты информации (Приложение 18).

2.6 Участвовать в приемке новых программных средств.

2.7 Обеспечить доступ к защищаемой информации пользователям ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.

2.8 Уточнять в установленном порядке обязанности пользователей ИСПДн по обработке объектов защиты.

2.9 Вести контроль над процессом осуществления резервного копирования объектов защиты и журнал учета процедуры резервного копирования (Приложение 24).

2.10 Анализировать состояние защиты ИСПДн и ее отдельных подсистем.

2.11 Контролировать неизменность состояния средств защиты их параметров и режимов защиты.

2.12 Контролировать физическую сохранность средств и оборудования ИСПДн.

2.13 Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а также правильность работы с элементами ИСПДн и средствами защиты.

2.14 Контролировать исполнение пользователями парольной политики.

2.15 Реализовывать парольную политику.

2.16 Контролировать работу пользователей в сетях общего пользования и (или) международного обмена.

2.17 Своевременно анализировать журнал учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений (Приложение 21).

2.18 Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач.

2.19 Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты ИСПДн.

2.20 Оказывать помощь пользователям ИСПДн в части применения средств защиты и консультировать по вопросам введенного режима защиты.

2.21 Периодически представлять руководству отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации.

2.22 В случае отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.23 Вести Журнал учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн (Приложение 23).

2.24 Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

2.25 Осуществлять разграничение прав доступа средствами ОС, средствами специального ПО в соответствии с должностными обязанностями каждого работника, имеющего права доступа к обрабатываемым персональным данным в ИСПДн.

2.26 Вести и актуализировать матрицу доступа в электронном виде.

3. Права администратора безопасности информации ИСПДн

3.1. Администратор безопасности информации имеет право инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн.

3.2. Администратор безопасности информации имеет право обращаться к ответственному за организацию обработки персональных данных и/или ответственному за эксплуатацию ИСПДн с требованием прекращения работы в ИСПДн при несоблюдении установленной технологии обработки информации и невыполнении требований по защите.

4. Ответственность администратора безопасности информации ИСПДн

4.1. На администратора безопасности информации ИСПДн возлагается персональная ответственность за качество проводимых им работ по обеспечению безопасности ПДн в ИСПДн.

4.2. Администратор безопасности информации ИСПДн несет ответственность по действующему законодательству за разглашение сведений ограниченного распространения, ставших известными ему по роду работы.

Приложение 14
к Приказу от 29.08.2022
№ Ш5-13-779/2

Инструкция пользователю ИСПДн

1 Общие положения

1.1. Настоящая инструкция определяет общие положения работы пользователей в защищенной от несанкционированного доступа информационных системах персональных данных (далее – ИСПДн).

1.2. Пользователь ИСПДн (далее – Пользователь) осуществляет обработку персональных данных (далее – ПДн) в ИСПДн

1.3. Пользователем является каждый сотрудник Оператора, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.4. Пользователь отвечает за правильность функционирования ИСПДн, входа в систему и все действия при работе в ИСПДн.

1.5. Пользователь в своей работе руководствуется настоящей инструкцией, и нормативными документами ФСТЭК России и регламентирующими документами МБОУ СОШ №5.

1.6. Методическое руководство работой пользователя осуществляется ответственным за организацию работ по обработке ПДн.

2 Должностные обязанности

2.1. Допуск пользователей для работы на автоматизированное рабочее место осуществляется в соответствии со списком лиц, допущенных к работе с ПДн.

2.2. В процессе первичной регистрации пользователя руководитель отдела, в котором работает пользователь, заявляет Администратору информационной безопасности перечень необходимых для работы пользователя ресурсов, перечень ПДн, состав необходимого общесистемного программного обеспечения для решения поставленных задач.

2.3. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору информационной безопасности по внутреннему телефону.

2.4. Обо всех выявленных нарушениях, связанных с информационной безопасностью МБОУ СОШ №5, а также для получений консультаций по вопросам информационной безопасности, необходимо обратиться к администратору информационной безопасности по электронной почте suria2016@yandex.ru или по телефону 58-50-01.

2.5. Пользователь обязан:

- знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации;
- выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в матрице доступа к обрабатываемым персональным данным в ИСПДн;
- знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов;
- соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других (раздел 3);
- при работе со съемными носителями пользователь должен каждый раз перед началом работы проверить их на наличие вирусов с использованием штатных антивирусных программ;

- в случае обнаружения вирусов на машинных носителях информации (съемных носителях, жестком магнитном диске, твердотельном носителе) пользователь обязан немедленно сообщить администратору информационной безопасности;
- в случае оставления рабочей станции без визуального контроля доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>, либо комбинацией клавиш Win + L;
- принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах, возложенных на него функций.

2.6. Пользователям запрещается:

- разглашать защищаемую информацию третьим лицам;
- копировать защищаемую информацию на внешние носители без разрешения администратора безопасности;
- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- несанкционированно открывать общий доступ к папкам на своей рабочей станции;
- запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;
- отключать (блокировать) средства защиты информации;
- обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;
- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;
- привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных;
- самостоятельно вносить изменения в аппаратно-программную конфигурацию ИСПДн, изменять месторасположение средств отображения информации.

2.7. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет дисциплинарную, административную, гражданско–правовую или уголовную ответственность граждан и юридических лиц.

3 Правила работы в сетях общего доступа и (или) международного обмена

3.1 Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

3.2 При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирус и других);
- передавать по Сети защищаемую информацию без использования механизмов защиты;
- запрещается скачивать из Сети программное обеспечение и другие файлы;
- запрещается посещение сайтов сомнительной репутации (порно сайты, сайты, содержащие нелегально распространяемое ПО и другие);
- запрещается нецелевое использование подключения к Сети.

4 Права и ответственность пользователей ИСПДн

4.1 Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн.

4.2 Пользователи, виновные в несоблюдении Настоящей инструкции расцениваются как нарушители Федерального закона РФ от 27.07.2006 г. №152-ФЗ «О персональных данных» и несут гражданскую, административную, уголовную, дисциплинарную и иную предусмотренную законодательством РФ ответственность.

Приложение 15
к Приказу от 29.08.2022
№ Ш5-13-779/2

Инструкция по учету машинных носителей информации

1. Общие положения

1.1. Настоящая Инструкция устанавливает основные требования к организации учета и использования машинных носителей данных, предназначенных для обработки и хранения персональных данных (далее – ПДн).

1.2. Учет машинных носителей информации осуществляется в соответствии с формой учетной документации.

1.3. Все машинные носители данных, используемые при работе со средствами вычислительной техники (далее – СВТ) для обработки и хранения ПДн, должны обязательно регистрироваться и учитываться. Допускается автоматизированный учет машинных носителей информации.

1.4. Проверка наличия машинных носителей данных, предназначенных для обработки и хранения ПДн, проводится в сроки, установленные настоящей Инструкцией.

2. Учет машинных носителей информации

2.1 К машинным носителям информации относятся:

- съемные носители информации;
- несъемные жесткие магнитные диски;
- твердотельные накопители.

2.2 Персональную ответственность за сохранность полученных машинных носителей данных и предотвращении несанкционированного доступа к записанной на них информации несет сотрудник, получивший эти носители.

2.3 При обработке ПДн на СВТ должен вестись учет машинных носителей данных.

2.4 При обработке ПДн на СВТ должен соблюдаться следующий общий порядок учета, хранения и уничтожения машинных носителей данных.

2.4.1 Учет машинных носителей данных из п. 2.1, предназначенных для записи ПДн производится в Журнале учета машинных носителей ПДн (Приложение 17).

2.4.2 Каждому носителю информации присваивается учетный номер, который состоит из серийного номера машинного носителя, номера объекта и порядкового номера по Журналу учета машинных носителей ПДн.

2.4.3 Если на машинном носителе отсутствует серийный номер, то на носитель (корпус носителя) наносится учетный номер. Если невозможно маркировать непосредственно машинный носитель данных, то маркируется упаковка, в которой хранится носитель.

2.4.4 Хранение их должно осуществляться в условиях, исключающих возможность хищения, приведения в негодность или уничтожения содержащейся на них информации.

2.4.5 Машинные носители данных (см. п. 2.1.) после стирания с них ПДн, с учета не снимают, а хранятся наравне с другими машинными носителями.

2.4.6 В последующем эти носители используются для записи ПДн. Если носители не пригодны для дальнейшего использования, они подлежат уничтожению по соответствующему акту.

2.4.7 О фактах утраты машинных носителей с ПДн незамедлительно докладывается администратору безопасности Оператора и проводится служебное расследование.

2.4.8 Машинные носители ПДн выдаются операторам или другим лицом, участвующим в обработке информации, составляющей ПДн, для работы под расписку в Журнале учета машинных носителей ПДн. По завершению работы машинные носители данных сдаются ответственному за их хранение.

2.4.9 Копирование информации, составляющей ПДн, с машинных носителей производится с разрешения администратора безопасности Оператора.

2.4.10 Машинные носители с ПДн, утратившими практическое значение или пришедшие в негодность, уничтожаются по соответствующему акту.

2.5 При подготовке документов должны соблюдаться следующие особенности учета, хранения и уничтожения машинных носителей данных.

2.5.1 Машинные носители ПДн, предназначенные для записи ПДн, выдаются Работникам по письменному разрешению руководителей структурных подразделений, в необходимом для работы количестве под расписку в Журнале учета машинных носителей ПДн.

2.5.2 Несъемные жесткие магнитные диски и твердотельные накопители закрепляются за сотрудником, ответственным за СВТ, в котором они установлены.

2.5.3 В случае повреждения машинных носителей данных, содержащих ПДн, сотрудник, в пользовании которого они находятся, обязан сообщить о случившемся ответственному за его сохранность.

2.5.4 В случае необходимости (командировка, отпуск и т. д.) съемные носители с ПДн, сдаются сотрудником ответственному лицу на постоянное или временное хранение.

2.5.5 Копирование ПДн, с машинных носителей с целью передачи другим Работникам производится с разрешения руководителя подразделения сотрудником, постоянно работающим с данной информацией.

2.5.6 Копирование осуществляется только на тех СВТ, на которых разрешена обработка ПДн, и только на те носители, которые соответствуют грифу «конфиденциально».

2.5.7 Хранящиеся на носителях и потерявшие актуальность ПДн должны своевременно стираться (уничтожаться). Ответственность за это несет владелец информации.

2.6 Руководство Оператора не реже одного раза в год создает комиссию по проверке наличия и условий хранения ПДн.

Приложение 16
к Приказу от 29.08.2022
№ Ш5-13-779/2

Инструкция по организации резервирования и восстановления программного обеспечения, работоспособности технических средств, баз персональных данных информационных систем персональных данных

1. Общие требования

1.1. Настоящая инструкция разработана в соответствии с требованиями к защите персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн), утвержденных Постановлением правительства №1119 от 1 ноября 2012 г., и определяет меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

1.2. Целью настоящего документа является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации, обеспечение возможности незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

1.3. Инструкция определяет правила и объемы резервирования, а также порядок восстановления ИСПДн в Оператора.

2. Порядок реагирования на инцидент

2.1. В настоящем документе под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также потерей защищаемой информации.

2.2. Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;
- в результате преднамеренных действий пользователей и третьих лиц;
- в результате нарушения правил эксплуатации технических средств ИСПДн;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.3. В кратчайшие сроки, не превышающие одного рабочего дня, ответственный за реагирование сотрудник Оператора (администратор безопасности ПДн) предпринимает меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

3. Технические меры

3.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

- системы жизнеобеспечения;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

3.2. Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации;
- системы вентиляции и кондиционирования;
- системы резервного питания.

3.3. Все критичные помещения Оператора (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации.

3.4. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, могут применяться системы вентиляции и кондиционирования воздуха.

3.5. Для предотвращения потерь информации при кратковременном отключении

электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);
- резервные линии электропитания в пределах комплекса зданий.

4. Резервируемое общесистемное и специальное программное обеспечение, программное обеспечение средств защиты информации и базы ПДн

4.1. Необходимо осуществлять резервное копирование актуальной информации и данных, используемых для полного восстановления базы данных, содержащих ПДн.

4.2. Резервное копирование осуществляется во внешнее хранилище (стример, сервер резервного копирования, ЖМД, ГМД, CD-ROM, USB накопитель).

4.3. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль в соответствии с инструкцией по антивирусной защите.

5. Порядок резервирования и хранения резервных копий (ответственный за резервирование, периодичность)

5.1. Ежедневно, по окончанию работы с ПДн на персональной электронно-вычислительной машине, должно осуществляться резервное копирование актуальных ПДн во внешнее хранилище, создавая тем самым резервный электронный архив актуальных ПДн.

5.2. Еженедельно, в пятницу, по окончании рабочего дня, должно осуществляться полное копирование данных, необходимых для восстановления работы базы данных, содержащих ПДн, во внешнее хранилище.

5.3. Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учета процедуры резервного копирования.

5.4. Электронные носители, на которые осуществляется резервное копирование актуальных ПДн и их копии должны быть поставлены на соответствующий учет.

5.5. Электронные носители, на которые осуществляется резервное копирование актуальных ПДн, должны храниться в специально оборудованном для хранения месте, обеспечивающем сохранность этих носителей.

5.6. Ответственность за организацию резервного копирования в ИСПДн в соответствии с требованиями настоящей Инструкции возлагается на сотрудника, ответственного за организацию работ по обработке ПДн в ИСПДн Оператора.

5.7. Ответственность за проведение мероприятий резервного копирования в ИСПДн и соблюдение требований настоящей Инструкции возлагается на администратора безопасности ПДн и всех пользователей ИСПДн.

6. Порядок восстановления работоспособности ИСПДн

6.1. В случае потери работоспособности ИСПДн, должно быть обеспечено ее восстановление из резервной копии.

6.2. Восстановление из резервной копии осуществляется в соответствии с документацией, прилагающейся к системе резервного копирования ПО.

Приложение 17
к Приказу от 29.08.2022
№ Ш5-13-779/2

Журнал учета машинных носителей персональных данных

ИНВ. № _____

Журнал начат «____» _____ 20__ г.
_____/ Должность
_____/ ФИО должностного лица

Журнал завершен «____» _____ 20__ г.
_____/ Должность
_____/ ФИО должностного лица

На _____ листах

№ п/п	Регистрационный номер/дата	Тип/ёмкость машинного носителя персональных данных	Номер экземпляра/ количество экземпляров	Место установки (использования) /дата установки	Ответственное должностное лицо (ФИО)	Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения машинного носителя ПДн	Сведения об уничтожении машинных носителей ПДн, стирании информации (подпись, дата)
1	2	3	4	5	6	7	8	9	10

Приложение 18
к Приказу от 29.08.2022
№ Ш5-13-779/2

Журнал периодического тестирования средств защиты информации

ИНВ. № _____

Журнал начат «____» _____ 20__ г.
_____/ Должность
_____/ ФИО должностного лица

Журнал завершен «____» _____ 20__ г.
_____/ Должность
_____/ ФИО должностного лица

На _____ листах

№ п/п	Наименование средства защиты информации от НСД или криптосредства	Регистрационные номера СЗИ от НСД или криптосредства	Дата тестирования	Фамилия и подпись ответственного пользователя, проводившего тестирование	Наименование теста, используемые средства для проведения теста	Результат тестирования (успешный/неуспешный), комментарий	Дата очередного тестирования
1	2	3	4	5	6	7	8

Приложение 19
к Приказу от 29.08.2022
№ Ш5-13-779/2

Журнал инструктажа персонала

ИНВ. № _____

Журнал начат «____» _____ 20__ г.
_____/ Должность
_____/ ФИО должностного лица

Журнал завершен «____» _____ 20__ г.
_____/ Должность
_____/ ФИО должностного лица

На _____ листах

Инструктаж по автоматизированной обработке персональных данных прошел, с нижеперечисленными документами ознакомлен:

– Федеральный Закон от 27.07.2006 №152-ФЗ «О персональных данных»;

– Постановление Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

– Инструкция пользователя ИСПДн;

– Правила парольной защиты;

– Правила антивирусной защиты.

№ п/п	Дата	Фамилия	Имя	Отчество	Должность	Подпись
1	2	3	4	5		
1		Абдулжалиева	Сурия	Заурбековна		
2		Агаева	Галимат	Гусеновна		
3		Аджибатырова	Гульнара	Базаралиевна		
4		Аджибатырова	Фатима	Мурзабековна		
5		Азимова	Фарангис	Фарходовна		
6		Акзянова	Ольга	Михайловна		
7		Акчермышев	Георгий	Александрович		
8		Алантьева	Екатерина	Валерьевна		
9		Апакаева	Наталья	Владимировна		
10		Аптрахимова	Фания	Идиаловна		
11		Артыкбаева	Жамиля	Туремуратовна		
12		Атаева	Екатерина	Романовна		
13		Афанасьев	Вечеслав	Владимирович		
14		Бабаева	Мария	Имамудиновна		
15		Бабинов	Александр	Леонидович		
16		Бакланова	Светлана	Евгеньевна		
17		Баранова	Екатерина	Юрьевна		
18		Бахарева	Анастасия	Витальевна		
19		Беззубченко	Наталья	Петровна		
20		Безукладникова	Ольга	Владимировна		
21		Белкина	Виктория	Викторовна		
22		Березина	Екатерина	Сергеевна		

23		Биксина	Марина	Викторовна		
24		Брагина	Елена	Алексеевна		
25		Бузаладзе	Паата	Нугзарович		
26		Бунякина	Светлана	Леонидовна		
27		Бурундукова	Елена	Николаевна		
28		Бучельникова	Елена	Сергеевна		
29		Вахмянина	Олеся	Александровна		
30		Вебер	Эльвина	Павловна		
31		Галиакбарова	Эльвира	Галимовна		
32		Гасанагаева	Файиза	Абдулвагабовна		
33		Гиндуллина	Эльвина	Ринатовна		
34		Глимьянова	Финария	Финатовна		
35		Глушенкова	Валентина	Николаевна		
36		Головач	Олеся	Васильевна		
37		Горячий	Дмитрий	Сергеевич		
38		Григорян	Лариса	Меликовна		
39		Губенко	Виктория	Николаевна		
40		Гумерова	Айгуль	Вадисовна		
41		Давидовская	Зоя	Константиновна		
42		Давлетшина	Гульназ	Хайдаргалиевна		
43		Добрягина	Елена	Дмитриевна		
44		Елсукова	Дарья	Александровна		
45		Елсукова	Екатерина	Владимировна		
46		Ефремова	Алена	Анатольевна		
47		Журавлева	Виктория	Владимировна		
48		Заблудаева	Наталья	Викторовна		
49		Залибекова	Барият	Исаевна		
50		Ибрагимова	Вилера	Самигулловна		
51		Иващенко	Любовь	Юрьевна		
52		Игликова	Люзия	Вакилевна		
53		Измайлова	Марина	Алексеевна		
54		Ильбулова	Гульшат	Вакилевна		
55		Ильина	Елена	Сергеевна		

56		Каменева	Светлана	Ивановна		
57		Квич	Виктория	Валерьевна		
58		Киреева	Марина	Валентиновна		
59		Киршина	Яна	Анатольевна		
60		Ковалева	Диана	Игоревна		
61		Кокарева	Анжелика	Леонидовна		
62		Коломиец	Светлана	Анатольевна		
63		Коновалова	Наталья	Владимировна		
64		Коновалова	Наталья	Александровна		
65		Короткова	Наталья	Александровна		
66		Корякина	Ольга	Викторовна		
67		Коць	Светлана	Николаевна		
68		Красова	Ирина	Сергеевна		
69		Крылова	Жанна	Васильевна		
70		Кузигова	Людмила	Владиславовна		
71		Кузнецова	Татьяна	Александровна		
72		Лебедкина	Татьяна	Владимировна		
73		Лихожон	Светлана	Николаевна		
74		Лобанова	Ольга	Николаевна		
75		Лукьянчук	Галина	Николаевна		
76		Лучик	Сергей	Григорьевич		
77		Ляшева	Кристина	Сергеевна		
78		Макарова	Лариса	Викторовна		
79		Малинкин	Станислав	Вячеславович		
80		Маслова	Елена	Николаевна		
81		Маснюк	Михаил	Иванович		
82		Матвеев	Алексей	Дмитриевич		
83		Матронова	Надежда	Сергеевна		
84		Мельникова	Нина	Ивановна		
85		Менгишова	Менлихан	Юсуповна		
86		Мехликова	Татьяна	Владимировна		
87		Миникаева	Лариса	Егоровна		
88		Мирзаева	Галина	Владимировна		

89		Мишагина	Галина	Ивановна		
90		Мухамедьярова	Гульнара	Тимиргалеевна		
91		Назимов	Багатыр	Арсенович		
92		Назимова	Диана	Юрьевна		
93		Насырова	Элмира	Бийтемировна		
94		Низельник	Евгений	Александрович		
95		Обосян	Алиса	Владимировна		
96		Ольхова	Валерия	Романовна		
97		Омельченко	Юлия	Владимировна		
98		Омельчук	Татьяна	Юрьевна		
99		Павлова	Наталья	Владимировна		
100		Панкратова	Наталья	Евгеньевна		
101		Парфенова	Екатерина	Сергеевна		
102		Пашкова	Ольга	Ивановна		
103		Петкова	Наталья	Юрьевна		
104		Петухова	Илона	Николаевна		
105		Погорелова	Татьяна	Владимировна		
106		Подгорбунских	Олег	Игоревич		
107		Посудневский	Виктор	Юрьевич		
108		Пошивайлова	Надежда	Владимировна		
109		Приданникова	Кристина	Александровна		
110		Раева	Людмила	Викторовна		
111		Решетникова	Елена	Леонидовна		
112		Ружин	Константин	Иванович		
113		Сабирова	Равиля	Равилевна		
114		Сагаева	Лилия	Борисовна		
115		Садовская	Генриета	Айдаровна		
116		Салимзянова	Гульназ	Варисовна		
117		Сахтаева	Зарема	Исламалиевна		
118		Секерина	Лилия	Кимовна		
119		Семенюченко	Екатерина	Дмитриевна		
120		Семчук	Ирина	Михайловна		
121		Симоненко	Светлана	Евгеньевна		

122		Скубилина	Сюзанна	Эдуардовна		
123		Смирнова	Ольга	Алексеевна		
124		Сотникова	Наталья	Анатольевна		
125		Стольникова	Анна	Олеговна		
126		Таштимирова	Саида	Муратовна		
127		Терлеева	Оксана	Валерьевна		
128		Титенко	Георгий	Константинович		
129		Ткаличева	Светлана	Владимировна		
130		Толочиева	Наталья	Владимировна		
131		Туз	Евгений	Михайлович		
132		Усольцева	Татьяна	Александровна		
133		Файзырова	Эльмира	Фанузовна		
134		Федорова	Ольга	Юрьевна		
135		Фролова	Светлана	Станиславовна		
136		Фурс	Валерия	Александровна		
137		Харитонова	Ирина	Александровна		
138		Хлебникова	Наталья	Валерьевна		
139		Чернова	Алла	Владимировна		
140		Чуркина	Нина	Сергеевна		
141		Шайтор	Мария	Александровна		
142		Шакирзянова	Елена	Наильевна		
143		Шамбилова	Марина	Мадениетовна		
144		Шангареева	Рида	Рамзиевна		
145		Шишкина	Евгения	Вадимовна		
146		Шмакова	Ольга	Анатольевна		
147		Щербакова	Ольга	Сергеевна		
148		Эмирагаева	Анета	Муталибовна		
149		Юманова	Вера	Николаевна		
150		Яковлева	Инга	Александровна		
151						
152						
153						
154						

155						
156						
157						
158						
159						
160						
161						
162						
163						
164						
165						
166						
167						
168						
169						
170						
171						
172						
173						
174						
175						
176						
180						
181						
182						
183						
184						
185						
186						
187						
188						
189						
190						

Приложение 20
к Приказу от 29.08.2022
№ Ш5-13-779/2

Журнал учета мероприятий по защите персональных данных

ИНВ. № _____

Журнал начат «____» _____ 20__ г.
_____ / Должность
_____ / ФИО должностного лица

Журнал завершен «____» _____ 20__ г.
_____ / Должность
_____ / ФИО должностного лица

На _____ листах

№ п/п	Наименование проводимого мероприятия	Дата провидения мероприятия	Исполнитель мероприятия		Результат (отчет, действия) мероприятия	Подпись и расшифровка подписи
			ФИО	Должность		
1	2	3	4	5	6	7
1.	Контроль целостности аппаратной конфигурации и наличия защитных пломб	Ежедневно		Администратор безопасности		
2.	Контроль над выполнением антивирусной защиты	Ежедневно				
3.	Контроль над соблюдением режима обработки ПДн	Еженедельно				
4.	Контроль над соблюдением режима защиты ПДн	Ежедневно				
5.	Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена	Ежедневно				
6.	Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	Ежемесячно		Администратор безопасности		
7.	Контроль за обеспечением резервного копирования	Еженедельно				
8.	Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Ежегодно		Администратор безопасности		
9.	Соблюдение условий доступа в помещения, где обрабатываются и хранятся материальные носители персональных данных, а также в помещения, где размещены рабочие места и иные узлы ИСПДн	Еженедельно				

10.	Соблюдение правил работы со съемными (машинными) носителями персональных данных	Еженедельно				
11.	Пересмотр матрицы доступа к ПДн	Каждые 6 месяцев				
12.	Направление в уполномоченный орган (Роскомнадзор) уведомления о своем намерении осуществлять обработку персональных данных с использованием средств автоматизации в случаях, когда этого требует законодательство				Уведомление направляется при вводе в эксплуатацию новых информационных систем персональных данных, либо при внесении изменений в существующие	
13.	Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно			При наличии изменений в процессах обработки ПДн, ИСПДн, документообороте	
14.	Установка сроков обработки ПДн и процедуры их уничтожения по окончании срока обработки				Для каждой ИСПДн оператором ПД должны быть установлены сроки обработки ПД.	
15.	Сопровождение заявок на предоставление доступа к информационным ресурсам ИСПДн			Администратор ИСПДн	Разграничение прав доступа к ПДн сотрудников организации согласно заявке на предоставление пользователю прав допуска к ресурсам ИСПДн (сотрудники наделяются минимальными полномочиями доступа, необходимыми для выполнения ими своих обязанностей, например, могут иметь права только на просмотр ПДн). Заявка утверждается директором организации и при необходимости пересматривается	

					(увольнение, прием новых сотрудников и прочее). Заявки на сотрудников подшиваются и хранятся у администратора ИСПДн	
16.	Повышение квалификации сотрудников в области защиты персональных данных					
17.	Инвентаризация информационных ресурсов с целью выявления присутствия и обработки в них ПДн					
18.	Классификация ИСПДн			Комиссия по защите персональных данных		
19.	Выявление угроз безопасности и разработка моделей угроз и нарушителя					
20.	Получение письменного согласия субъектов на обработку ПДн	Постоянно				
21.	Пересмотр договоров с субъектами в части обработки ПДн					
22.	Уничтожение ПДн	При достижении целей обработки ПДн		Комиссия по уничтожению ПДн		

23.	Оценка эффективности реализованных в рамках системы защиты мер по обеспечению безопасности ПДн	Раз в 3 года			Проводится самостоятельно или организацией – лицензиатом ФСТЭК	
24.						
25.						
26.						
27.						
28.						

Приложение 21
к Приказу от 29.08.2022
№ Ш5-13-779/2

Журнал о событиях информационной безопасности

ИНВ. № _____

Журнал начат «____» _____ 20__ г.
_____ / Должность
_____ / ФИО должностного лица

Журнал завершен «____» _____ 20__ г.
_____ / Должность
_____ / ФИО должностного лица

На _____ листах

№ п/п	Дата	Время	Данные сообщившего (ФИО, должность, отдел)	Наименование объекта	Описание события	Планируемое время решения	Фактическое время решения	Причины	Работы, проведенные для устранения
1	2	3	4	5	6	7	8	9	10

Приложение 22
к Приказу от 29.08.2022
№ Ш5-13-779/2

Журнал учета средств защиты информации, эксплуатационной и технической документации к ним

ИНВ. № _____

Журнал начат «____» _____ 20__ г.
_____ / Должность
_____ / ФИО должностного лица

Журнал завершен «____» _____ 20__ г.
_____ / Должность
_____ / ФИО должностного лица

На _____ листах

Номер п/п	Индекс и наименование средства защиты информации	Серийный (заводской) номер	Номер специального защитного знака	Наименование организации, установившей СЗИ	Место установки	Примечание
1	2	3	4	5	6	7

Приложение 23
к Приказу от 29.08.2022
№ Ш5-13-779/2

Журнал учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн

ИНВ. № _____

Журнал начат «____» _____ 20__ г.
_____ / Должность
_____ / ФИО должностного лица

Журнал завершен «____» _____ 20__ г.
_____ / Должность
_____ / ФИО должностного лица

На _____ листах

№ п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	ФИО исполнителей и их подписи	ФИО ответственного за эксплуатацию ПЭВМ, подпись	Подпись специалиста по защите информации	Примечание (ссылка на заявку)
1	2	3	4	5	6	7

Приложение 24
к Приказу от 29.08.2022
№ Ш5-13-779/2

Журнал учета процедуры резервного копирования

ИНВ. № _____

Журнал начат «____» _____ 20__ г.
_____ / Должность
_____ / ФИО должностного лица

Журнал завершен «____» _____ 20__ г.
_____ / Должность
_____ / ФИО должностного лица

На _____ листах

№ п/п	Регистрационный номер/дата проведения резервного копирования	Тип/ёмкость машинного носителя персональных данных	Наименование ИСПДн	Ответственное должностное лицо (ФИО)
1	2	3	4	5

Приложение 25
к Приказу от 29.08.2022
№ Ш5-13-779/2

**Перечень событий безопасности,
критичных для функционирования информационной системы, определения состава и содержания информации о событиях безопасности**

Событием информационной безопасности является состояние системы, сервиса или сети, которое свидетельствует о возможном нарушении принятых мер по защите персональных данных (далее – ПДн), либо о прежде неизвестной ситуации, которая может иметь отношение к безопасности.

События безопасности критичные для информационной системы персональных данных Оператора.

1. Не выполнилось обновление базы сигнатур антивирусного ПО.
2. Не выполнилось резервное копирование.
3. Компрометация (факт несанкционированного доступа к защищенной информации, а также подозрение осуществления такого доступа) информационной системы. Данные могут быть скомпрометировать в результате:
    - физической потери носителя;
    - передачи информации по незащищенным каналам в незашифрованном виде;
    - несанкционированного доступа постороннего лица;
    - перехвата информации вредоносными программами;
    - прослушивания канала связи;
    - сознательной передачи носителя с данными третьему лицу.
4. Проникновение в информационную систему вредоносных программ (специально созданных для электронно-вычислительной машины (далее – ЭВМ) различного рода программ с целью нарушения нормального функционирования компьютерных программ в соответствии с их документацией для достижения указанных в законе преступных результатов – заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети).
5. Несоблюдение требований к информационной безопасности, принятых в организации и описанных в организационно-распорядительной документации организации.
6. Отказ в обслуживании сервисов, средств обработки информации, оборудования, средств защиты информации, входящих в состав ИСПДн;
7. Нарушение конфиденциальности и целостности ПДн, обрабатываемых в ИСПДн:
    - компрометация ПДн;
    - случайное или несанкционированное уничтожение (полное или частичное), модификация ПДн.

Состав и содержание информации о событиях безопасности:

1. Дата и время наступления события.
2. Наименование объекта.
3. Описание события.
4. Причины.

Журнал о событиях безопасности может вестись как в электронном, так и в бумажном виде (журнал учета нештатных ситуаций ИСПДн). Некоторые события безопасности могут фиксироваться в логах операционного системного программного обеспечения. Срок их хранения в логах 6 месяцев

Доступ к журналу о событиях безопасности и логам операционного системного программного обеспечения имеет только лицо ответственное за обеспечение безопасности персональных данных в организации.