МУНИЦИПАЛЬНОЕ КАЗЁННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ВОРОБЬЁВСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА ИМЕНИ ГЕРОЯ СОВЕТСКОГО СОЮЗА НИКОЛАЯ ТИМОФЕЕВИЧА ВОРОБЬЁВА»
(МКОУ «Воробьёвская СОШ имени Н.Т.Воробьёва»)

ИНН 0807003088 ОГРН 1020800671264
Республика Калмыкия. Приютненский район, с. Воробьёвка, ул. Мира, д. 51
email: irjkfdci@yandex.ru

Утверждаю:
«25» 08 2022г.
Директор школы:
_____/Фоменко Е.В.

Приказ №37 от «25» 08 2022г.
Принято на заседании
педагогического совета
Протокол № 1 от «24» 08 2022г.

ПОЛОЖЕНИЕ

о разрешительной системе доступа в информационных системах персональных данных МКОУ «Воробьёвская СОШ имени Н.Т.Воробьёва»

с.Воробьёвка, 2022 год.

1.Общие положения

1.1.Настоящее Положение о разрешительной системе доступа в информационных системах персональных данных МКОУ «Воробьёвская СОШ имени Н.Т.Воробьёва» (далее – Положение), разработано в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).

1.2.Настоящее Положение определяет методы управления доступом, типы доступа и правила разграничения доступа субъектов доступа к объектам доступа в ИСПДн.

1.3.Положение обязательно для исполнения всеми работниками МКОУ «Воробьёвская СОШ имени Н.Т.Воробьёва» (далее – Учреждение), непосредственно осуществляющими защиту ПДн.

2.Субъекты и объекты доступа

2.1.К субъектам доступа ИСПДн, относятся работники, выполняющие свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств ИСПДн в соответствии с должностными инструкциямии которым в ИСПДн присвоены учетные записи.

2.2.К объектам доступа в ИСПДн, относятся:

- средства вычислительной техники;
- средства связи и передачи данных;
- средства обеспечения бесперебойной работы средств вычислительной техники и средств связи и передачи данных;
- основные конфигурационные файлы операционных систем, средств связи и передачи данных и средств защиты информации (далее – СЗИ);
- средства настройки и управления операционной системой, средств связи и передачи данных и СЗИ;
- прикладное программное обеспечение;
- периферийные устройства;
- машинные носители информации;
- обрабатываемые, хранимые данные.

3.Методы разграничения доступа

3.1.Методы разграничения доступа к ИСПДн реализуются в соответствии с особенностями функционирования ИСПДн и включают комбинацию следующих методов:

- ролевой метод управления доступом;
- дискреционный метод управления доступом.

3.2.Реализация ролевого метода управления доступом в ИСПДн представлена в таблице 1.

Таблица 1

№ п/п	Роль субъекта доступа	Уровень доступа к объектам доступа
1	Администратор ИСПДн	-обладает полной информацией о конфигурации системы защиты ПДн (структуре системы защиты ПДн, составе, местах установки и параметров настройки СЗИ); -обладает полной информацией о конфигурации ИСПДн (структуре ИСПДн, состава, мест установки и параметров программного обеспечения и технических средств); -обладает правами настройки и конфигурирования СЗИ; -обладает правами настройки и конфигурирования средств связи передачи данных; -обладает правами настройки и конфигурирования операционных систем и прикладного программного обеспечения; -обладает правами внесения изменений в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения
2	Ответственный за обеспечение безопасности ПДн в ИСПДн	-обладает полной информацией о конфигурации ИСПДн (структуре ИСПДн, составе, местах установки и параметров программного обеспечения и технических средств); -обладает правами настройки и конфигурирования средств связи передачи данных; -обладает правами настройки и конфигурирования операционных систем и прикладного программного обеспечения; -обладает правами внесения изменений в программное обеспечение ИСПДн на стадии ее разработки, внедрения

		и сопровождения
3	Пользователь ИСПДн	-обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к ИСПДн.

3.3.Реализация дискреционного метода управления доступом достигается путем назначения прав доступа для каждой пары «Роль субъекта доступа» – «Объект доступа» явного и недвусмысленного перечисления допустимых типов доступа в соответствии с «Матрицей доступа работников к ресурсам информационных систем персональных данных МКОУ «Воробьёвская СОШ имени Н.Т.Воробьёва» (далее – Матрица доступа), форма которой установлена в Приложении к настоящему Положению.

4.Типы доступа

4.1.В ИСПДн определены следующие типы доступа субъектов доступа к объектам доступа:

- чтение (R) – субъекту доступа разрешено просматривать содержимое объекта доступа;
- запись (W) – субъекту доступа разрешено просматривать, записывать и создавать новый объект доступа;
- выполнение (E) – субъекту доступа разрешено запускать/выполнять объект доступа;
- печать (P) – субъекту доступа разрешена печать;
- сканирование (S) – субъекту доступа разрешено сканирование;
- полный (F) – субъект доступа имеет полный доступ к объектам доступа.
- Разрешенные к выполнению, субъектами доступа при доступе к объектам доступа в ИСПДн, типы доступа, определены в Матрице доступа.

5.Правила разграничения доступа

5.1.В ИСПДн правила разграничения доступа реализованы совокупностью правил, регламентирующих порядок и условия доступа субъекта к объектам доступа в ИСПДн:

- разделение обязанностей и назначение минимально необходимых прав Пользователям ИСПДн, Администратору ИСПДн и Ответственному за обеспечение безопасности ПДн в ИСПДн;
- управление (заведение, активация, блокирование и уничтожение) учетными записями Пользователей ИСПДн;
- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками в ИСПДн;
- ограничение неуспешных попыток доступа в ИСПДн;
- разрешение (запрет) действий Пользователей ИСПДн, разрешенных до идентификации и аутентификации;
- реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;
- контроль использования в ИСПДн технологий беспроводного доступа;
- контроль использования в ИСПДн мобильных технических средств;
- управление взаимодействием с ИСПДн организаций (внешние информационные системы).

5.2.Права и обязанности Пользователей ИСПДн зафиксированы в «Инструкции пользователя информационных систем персональных данных МКОУ «Воробьёвская СОШ имени Н.Т.Воробьёва».

5.3.Права и обязанности Администратора ИСПДн зафиксированы в «Инструкции администратора информационных систем персональных данных МКОУ «Воробьёвская СОШ имени Н.Т.Воробьёва».

5.4.Права и обязанности Ответственного за обеспечение ПДн в ИСПДн зафиксированы в «Инструкции ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных МКОУ «Воробьёвская СОШ имени Н.Т.Воробьёва».

5.5.Управление (заведение, активацию, блокирование и уничтожение) учетными записями Пользователей ИСПДн, осуществляет Администратор ИСПДн.

5.6.Администратор ИСПДн определяет и назначает права доступа субъектов к объектам доступа в ИСПДн в соответствии с исполняемой ролью субъекта в ИСПДн и Матрицей доступа.

5.7.В ИСПДн реализованы следующие функции управления учетными записями Пользователей ИСПДн:

- определение типа учетной записи (пользователь, администратор, системная);объединение учетных записей в группы (пользователи, администраторы);
- верификация пользователя при заведении учетной записи пользователя;заведение, активация, блокирование и уничтожение учетных записей Пользователей ИСПДн;
- пересмотр и корректировка учетных записей Пользователей ИСПДн;
- порядок заведения и контроля использования временных учетных записей Пользователей ИСПДн;оповещение Администратора ИСПДн, осуществляющего управление учетными записями Пользователей ИСПДн, об изменении сведений о Пользователях ИСПДн, их ролях, обязанностях, полномочиях, ограничениях;
- уничтожение временных учетных записей Пользователей ИСПДн, предоставленных для однократного (ограниченного по времени) выполнения задач в ИСПДн;
- предоставление Пользователям ИСПДн прав доступа к объектам доступа ИСПДн, основываясь на задачах, решаемых Пользователями ИСПДн.

5.8.Временная учетная запись может быть заведена для Пользователя ИСПДн на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям ИСПДн с временным доступом к ИСПДн).

5.9.В ИСПДн осуществляется автоматическое блокирование временных учетных записей Пользователей ИСПДн по окончании установленного периода времени для их использования.

5.10.При передаче информации между устройствами, сегментами в рамках ИСПДн, осуществляется управление информационными потоками, включающее:

- фильтрацию информационных потоков в соответствии с правилами управления потоками;
- разрешение передачи информации в ИСПДн только по установленному маршруту;
- изменение (перенаправление) маршрута передачи информации только в установленных случаях;
- запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи в установленных случаях.

5.11.Управление информационными потоками обеспечивает разрешенный маршрут прохождения информации между Пользователями ИСПДн, устройствами, сегментами в рамках ИСПДн, а также при взаимодействии с сетью Интернет (или другими информацион-

но-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными потоками, включающих контроль конфигурации ИСПДн, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации).

5.12.Управление информационными потоками блокирует передачу защищаемой информации через сеть Интернет (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, не санкционированно исходящие из ИСПДн и (или) входящие в ИСПДн.

5.13.В ИСПДн установлено и зафиксировано в «Инструкции по парольной защите информации в МКОУ оробьёвская СОШ имени Н.Т.Воробьёва»:

- количество неуспешных попыток входа (доступа) ИСПДн за установленный период времени;
- блокирование сеанса доступа Пользователя ИСПДн после установленного времени его бездействия (неактивности).

5.14.В ИСПДн обеспечивается блокирование сеанса доступа Пользователя ИСПДн по запросу.

5.15.Для заблокированного сеанса осуществляется блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.

5.16.Администратору ИСПДн и Ответственному за обеспечение безопасности ПДн в ИСПДн разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования ИПСДн в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

5.17.В ИСПДн в качестве мобильных технических средств рассматриваются съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства).

5.18.Регламентация и контроль использования съемных машинных носителей ПДн, описаны в «Инструкции по обращению со съемными машинными носителями персональных данных в МКОУ «Воробьёвская СОШ имени Н.Т.Воробьёва».

5.19.В ИСПДн при взаимодействии с внешними информационными системами, взаимодействие с которыми необходимо для функционирования ИСПДн, предоставление доступа к ИСПДн осуществляется только авторизованным (уполномоченным) Пользовате-

лям ИСПДн в соответствии с Матрицей доступа.

6.Ответственность

6.1.Все работники Учреждения, осуществляющие обработку и защиту ПДн обязаны ознакомиться с данным Положением.

6.2.Работники Учреждения несут персональную ответственность за выполнение требований настоящего Положения.

6.3.Контроль выполнения работниками Учреждения правил разграничения доступа в ИСПДн осуществляется Ответственным за обеспечение безопасности ПДн в ИСПДн.

7.Срок действия и порядок внесения изменений

7.1.Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно.

7.2.Настоящее Положение подлежит пересмотру не реже одного раза в три года.

7.3.Изменения и дополнения в настоящее Положение вносятся приказом Директора Учреждения.

Приложение 1

к Положению о разрешительной

системе доступа в информационныхсистемах персональных данных

МКОУ «Воробьёвская СОШ имени Н.Т.Воробьёва»

ФОРМА

Матрица доступа работников к ресурсам информационных систем персональных данных МКОУ «Воробьёвская СОШ имени Н.Т.Воробьёва»

Субъект доступа	Объект доступа							
	Основные конфигурационные файлы операционной системы	Средства настройки управления операционной системой	Основные конфигурационные файлы средствзащиты информации	Средства настройки управления средствзащиты информации	Прикладное программное обеспечение	Периферийные устройства	Съемные машинные носители информации	Обрабатываемые, хранимые данные
Администратор информационной системы								
Ответственный за обеспечение безопасности персональных данных в информационных системах								
Пользователь								

Типы доступа:

– чтение (R) – субъекту доступа разрешено просматривать содержимое объекта доступа;

- запись (W) – субъекту доступа разрешено просматривать, записывать и создавать новый объект доступа;
- выполнение (E) - субъекту доступа разрешено запускать/выполнять объект доступа;
- печать (P) – субъекту доступа разрешена печать;
- сканирование (S) – субъекту доступа разрешено сканирование;
- полный (F) – субъект доступа имеет полный доступ к объектам доступа.