Приложение 1
к приказу № 188
от 09.07.2020

ПОЛОЖЕНИЕ
о разрешительной системе доступа в информационных системах МОУ СОШ № 37

1. Термины и определения

1.1. Дискреционный метод управления доступом – метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа.

1.2. Доступ к информации - ознакомление с информацией, ее обработка, в частности копирование, модификация или уничтожение информации.

1.3. Матрица доступа – таблица, отображающая правила разграничения доступа.

1.4. Объект доступа – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

1.5. Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

1.6. Ролевой метод управления доступом – метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа.

1.7. Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

1.8. Субъект доступа – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

1.9. Типы доступа – операции, разрешенные к выполнению субъектом доступа при доступе к объектам доступа.

2. Общие положения

2.1. Настоящее Положение о разрешительной системе доступа в информационных системах МОУ СОШ № 37 (далее – Положение), разработано в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативно-методическими документами федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах (далее – ИС).

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

2.3. Положение обязательно для исполнения всеми работниками МОУ СОШ № 37 (далее – Учреждение), непосредственно осуществляющими защиту ПДн.

3. Субъекты и объекты доступа

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

3.2. К объектам доступа в ИС, 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.

4. Методы разграничения доступа

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

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

4.2. Реализация ролевого метода управления доступом в ИС представлена в таблице 1.

Таблица 1

№ п/п	Роль субъекта доступа	Уровень доступа к объектам доступа
1	Администратор безопасности	- обладает полной информацией о конфигурации системы защиты ПДн (структуре системы защиты ПДн, составе, местах установки и параметров настройки СЗИ); - обладает полной информацией о конфигурации ИС (структуре ИС, 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 ИС на стадии ее разработки, внедрения и сопровождения.
2	Администратор	- обладает полной информацией о конфигурации ИС (структуре ИС, 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 ИС на стадии ее разработки, внедрения и сопровождения.
3	Пользователь	- обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к ИС.

4.3. 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 (далее – Матрица доступа), форма которой установлена в Приложении к настоящему Положению.

5. Типы доступа

5.1. В ИС 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.

5.2. Разрешенные к выполнению, субъектами доступа при доступе к объектам доступа в ИС, типы доступа, определены в Матрице доступа.

6. Правила разграничения доступа

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

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

6.2. Права и обязанности пользователей зафиксированы в «Инструкции пользователя информационных систем МОУ СОШ № 37».

6.3. Права и обязанности администратора зафиксированы в «Инструкции администратора информационных систем МОУ СОШ № 37».

6.4. Права и обязанности администратора безопасности зафиксированы в «Инструкции ответственного за обеспечение безопасности персональных данных в информационных системах МОУ СОШ № 37».

6.5. Управление (заведение, активацию, блокирование и уничтожение) учетными записями пользователей ИС, осуществляет администратор ИС.

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

6.7. В ИС реализованы следующие функции управления учетными записями пользователей ИС:

- 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 ИС;
- пересмотр и корректировка учетных записей пользователей ИС;
- порядок заведения и контроля использования временных учетных записей Пользователей ИС;
- оповещение администратора ИС, осуществляющего управление учетными записями пользователей ИС, об изменении сведений о пользователях ИС, их ролях, обязанностях, полномочиях, ограничениях;
- уничтожение временных учетных записей пользователей ИС, предоставленных для однократного (ограниченного по времени) выполнения задач в ИС;
- предоставление пользователям ИС прав доступа к объектам доступа ИС, основываясь на задачах, решаемых пользователями ИС.

6.8. Временная учетная запись может быть заведена для пользователя ИС 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 ИС с временным доступом к ИС).

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

6.10. При передаче информации между устройствами, сегментами в рамках ИС, осуществляется управление информационными потоками, включающее:
- фильтрацию информационных потоков в соответствии с правилами управления потоками;
- разрешение передачи информации в ИС 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.

6.11. Управление информационными потоками обеспечивает разрешенный маршрут прохождения информации между пользователями ИС, устройствами, сегментами в рамках ИС, а также при взаимодействии с сетью Интернет (или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными потоками, включающих контроль конфигурации ИС, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации).

6.12. 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 ИС и (или) входящие в ИС.

6.13. В ИС установлено и зафиксировано в «Инструкции по парольной защите информации в МОУ СОШ № 37:

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

6.14. В ИС обеспечивается блокирование сеанса доступа пользователя ИС по запросу.

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

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

6.17. Регламентация и контроль использования съемных машинных носителей ПДн, описаны в «Порядке обращения со съемными машинными носителями персональных данных в МОУ СОШ № 37.

6.18. В ИС при взаимодействии с внешними информационными системами, взаимодействие с которыми необходимо для функционирования ИС, предоставление доступа к ИС осуществляется только авторизованным (уполномоченным) пользователям ИС в соответствии с Матрицей доступа.

7. Ответственность

7.1. Все работники Учреждения, осуществляющие обработку и защиту ПДн обязаны ознакомиться с данным Положением под подпись.

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

7.3. Контроль выполнения работниками Учреждения правил разграничения доступа в ИС осуществляется Ответственным за обеспечение безопасности ПДн в ИС.

8. Срок действия и порядок внесения изменений

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

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

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