


УТВЕРЖДАЮ
Директор
Муниципального бюджетного
общеобразовательного
учреждения г. Астрахани
«Средняя общеобразовательная
школа №32»


/ Сидорина О.Н.

от «06» апреля 2022 г. № 01-10-492



ПОЛОЖЕНИЕ
о разрешительной системе доступа сотрудников к ресурсам
информационных систем персональных данных МБОУ г. Астрахани
«Средняя общеобразовательная школа №32»

2022 г.

1. Общие положения

Настоящими Правилами осуществления внутреннего контроля соответствия обработки защищаемой информации, в т.ч. персональных данных, в информационных системах персональных данных (далее – ИСПДн) МБОУ г. Астрахани «Средняя общеобразовательная школа №32» (далее – Учреждение) требованиям безопасности информации определяются процедуры, направленные на выявление и предотвращение нарушений установленных требований по защите информации в ИСПДн.

Настоящие Правила определяют порядок внутреннего контроля соответствия обработки защищаемой информации, в т.ч. персональных данных, требованиям безопасности информации в ИСПДн и действуют постоянно.

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю России от 18.02.2013 года №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и руководящими документами по вопросам обеспечения защиты информации.

1.2. Разрешительная система доступа сотрудников к ресурсам информационных систем персональных данных (далее – ИСПДн) МБОУ г. Астрахани «Средняя общеобразовательная школа №32» (далее – Учреждение) представляет собой совокупность процедур оформления прав субъектов на доступ к информационным ресурсам ИСПДн и ответственных лиц, осуществляющих реализацию этих процедур.

1.3. Объектами доступа являются:

- информационные ресурсы и технические средства ИСПДн;
- технологическая информация системы защиты информации ИСПДн.

1.4. Субъектами доступа являются:

- уполномоченные сотрудники Учреждения;
- лица, привлекаемые на договорной основе для обеспечения функционирования информационной системы (обслуживание, установка, настройка ПО).

1.5. Субъекты доступа несут персональную ответственность за соблюдение ими установленного в Учреждения порядка обеспечения защиты информационных ресурсов.

1.6. Ответственными лицами, осуществляющими реализацию процедур оформления прав субъектов на доступ к информационным ресурсам ИСПДн, являются администраторы ИСПДн (системный и безопасности).

2. Доступ к информационным ресурсам сотрудников Учреждения

2.1. Лица, доступ которым к защищаемой информации, обрабатываемой в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей, допускаются к ним на основании списков, утверждаемых руководителем Учреждения.

2.2. Допуск сотрудников к защищаемой информации, осуществляется в объеме, необходимом для выполнения ими должностных обязанностей. Права доступа сотрудников к защищаемой информации и выполняемые роли определяются в Матрице доступа (Приложение к Положению).

2.3. Администратором безопасности проверяется соответствие требуемых прав доступа с реально необходимыми для выполнения должностных (функциональных) обязанностей данного сотрудника.

2.4. После определения роли пользователя и в соответствии с обозначенными для него правами в матрице доступа администратор безопасности ИСПДн в соответствии с документацией на средства защиты производит необходимые действия по созданию (изменению, удалению) учетной записи пользователя, присвоению ему начального значения пароля и заявленных прав доступа к ресурсам ИСПДн, включению его в соответствующие группы пользователей и другие необходимые действия. Для всех пользователей ИСПДн устанавливается режим принудительного запроса смены пароля не реже одного раза в 180 дней, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 3 до 15 минут.

2.5. В случае производственной необходимости пользователю ИСПДн могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими сотрудниками при работе в ИСПДн одного и того же имени пользователя ("группового имени") запрещается.

2.6. При изменении должностных обязанностей сотрудника, связанных с переводом в другое подразделение, переводом на другую должность и т.п.,

учетная запись пользователя подлежит изменению (корректировке), при этом старые полномочия аннулируются.

2.7. После внесения изменений в матрицу доступа администратор безопасности ИСПДн производит настройку (при их наличии) специализированных средств защиты рабочих станций (автоматизированных рабочих мест).

2.8. Все изменения в правах доступа выполняются администраторами не позднее трех суток с момента получения заявки на внесение изменений.

2.9. Блокирование учетных записей на время отпуска пользователей ИСПДн осуществляется администратором безопасности ИСПДн.

2.10. Работнику, зарегистрированному в качестве нового пользователя системы, администратором безопасности присваивается идентификатор (учетная запись) и начальное значение пароля. При этом необходимо учитывать, что повторное использование идентификатора пользователя исключается в течение одного года.

3. Допуск к информационным ресурсам сторонних организаций, деятельность которых не связана с исполнением функций Учреждения

3.1. К организациям, деятельность которых не связана с исполнением функций организации, могут относиться:

- правоохранительные органы;
- судебные органы;
- органы статистики;
- органы исполнительной и законодательной власти субъектов Российской Федерации;
- средства массовой информации и пр.

3.2. Допуск к информационным ресурсам сторонних организаций, деятельность которых не связана с исполнением функций организации, регламентируется законодательством Российской Федерации, договорами и соглашениями об информационном обмене и другими нормативными актами.

3.3. Доступ к информационным ресурсам ИСПДн сторонних организаций осуществляется на основании письменных запросов.

В письменном запросе указывается:

- основание (с приведением ссылки на нормативный акт), в соответствии с которым предоставляется информация;
- для каких целей необходима информация;
- конкретное наименование предоставляемой информации и ее объем;
- способ доступа (предоставления).

3.4. Основанием для доступа (предоставления) информации служит резолюция руководителя Учреждения на соответствующем документе (запросе).

3.5. Для доступа к информационным ресурсам ИСПДн сотруднику сторонней организации должна быть заведена временная учетная запись на ограниченный срок, достаточный для проведения необходимых работ (настройки, тестирования или иных работ).

4. Допуск к информационным ресурсам Учреждения сторонних организаций, выполняющих работы в Учреждении на договорной основе

4.1. К организациям, выполняющим работы на договорной основе, могут относиться:

- организации, выполняющие строительные работы и осуществляющие ремонт зданий, систем инженерно-технического обеспечения (отопления, освещения, водоснабжения, канализации, электропитания, кондиционирования и т.п.);

- организации, осуществляющие монтаж и настройку технических средств автоматизированных систем, сопровождение прикладного программного обеспечения;

- организации, оказывающие услуги в области защиты информации (проведение специальных проверок и исследований, монтаж и настройка средств защиты информации, контроль эффективности системы защиты информации, аттестация объектов информатизации и т.п.);

- организации, осуществляющие поставку товаров для обеспечения повседневной деятельности (мебели, канцтоваров, оргтехники, расходных материалов и т.п.);

- организации и частные лица, оказывающие юридические услуги, услуги по информационно-техническому обеспечению, осуществляющие преподавательскую деятельность и т.п.

4.2. Порядок допуска определяется в договоре на выполнение работ (оказание услуг).

4.3. Решением о допуске является подписанный в установленном порядке договор на выполнение работ или оказание услуг.

4.4. Для доступа к информационным ресурсам ИСПДн сотруднику сторонней организации должна быть заведена временная учетная запись на ограниченный срок, достаточный для проведения необходимых работ (настройки, тестирования или иных работ).

4.5. Лица, привлекаемые на договорной основе для обеспечения функционирования информационной системы (ремонт, гарантийное

обслуживание, регламентные и иные работы) также относятся к категории внутренних пользователей ИС и им должны быть присвоены учетные записи в соответствии с правилами, определенными организационно-распорядительными документами по защите информации.

4.6. В договор на оказание услуг в обязательном порядке включается условие о неразглашении сведений, составляющих персональные данные, а также служебной информации, ставшей известной в ходе выполнения работ, если для их выполнения предусмотрено использование таких сведений. Со всех работников сторонней организации, участвующих в выполнении работ, в этом случае берется подписка о неразглашении таких сведений.

5. Контроль функционирования разрешительной системы допуска к информационным ресурсам Учреждения

5.1. Контроль функционирования разрешительной системы допуска к информационным ресурсам организуется в соответствии с:

- планом основных мероприятий по защите информации на текущий год;
- функциональными обязанностями должностных лиц;
- приказом руководителя Учреждения.

5.2. Контроль функционирования разрешительной системы допуска к информационным ресурсам ИСПДн осуществляется ответственными лицами не реже одного раза в три месяца. Организация контроля возлагается на администратора безопасности.

№ п/п	Фамилия, имя, отчество сотрудника (учетная запись)	Должность сотрудника	Уровень полномочий (роль)	Вид выполняемых функций	Наименование (тип) ресурса	Место хранения, размещения защищаемого ресурса	Права (тип) доступа к защищаемым ресурсам	Примечание
Пользователи								

№ п/п	Фамилия, имя, отчество сотрудника (учетная запись)	Должность сотрудника	Уровень полномочий (роль)	Вид выполняемых функций	Наименование (тип) ресурса	Место хранения, размещения защищаемого ресурса	Права (тип) доступа к защищаемым ресурсам	Примечание