Приложение №20
к приказу
от 02.09.2025г. № 01.09-0209-4

ИНСТРУКЦИЯ
по организации защиты информации о событиях безопасности в информационных систем персональных данных в муниципальном бюджетном общеобразовательном учреждении г. Астрахани «СОШ№30»

1. Общие положения

1.1. Настоящая Инструкция предназначена для организации защиты информации о событиях безопасности в информационных систем персональных данных в муниципальном бюджетном общеобразовательном учреждении г. Астрахани «СОШ№30» (далее – школа) Действие настоящей Инструкции распространяется на Администратора безопасности информационных систем персональных данных (далее – Администратор).

2. События безопасности

2.1. К событиям безопасности, подлежащим регистрации в информационных системах персональных данных, принадлежащих школы, должны быть отнесены любые проявления состояния информационных систем персональных данных и системы защиты информации, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов информационных систем персональных данных, нарушения процедур, установленных организационно-распорядительными документами по защите информации, а также на нарушение штатного функционирования средств защиты информации.

2.2. В информационных системах персональных данных школы подлежат регистрации следующие события:

- вход/выход, а также попытки входа пользователей в информационные системы персональных данных и загрузки/останова операционной системы;
- подключение машинных носителей информации и вывод информации на носители информации;
- запуск/завершение программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;
- попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям,

полям записей) и иным объектам доступа;

– попытки удаленного доступа.

2.3. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны обеспечивать возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

2.3.1. При регистрации входа/выхода пользователей в информационные системы персональных данныхи загрузки/останова операционной системы состав и содержание информации должны, как минимум, включать дату и время входа/выхода в систему/из системы или загрузки/останова операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки/останова операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

2.3.2. При регистрации подключения машинных носителей информации и вывода информации на носители информации состав и содержание регистрационных записей должны, как минимум, включать дату и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.

2.3.3. При регистрации запуска/завершения программ и процессов (заданий, задач), связанных с обработкой защищаемой информации состав и содержание регистрационных записей должны, как минимум, включать дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

2.3.4. При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей должны, как минимум, включать дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

2.3.5. При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) состав и содержание информации должны, как минимум, включать дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер).

2.3.6. При регистрации попыток удаленного доступа к информационной системе состав и содержание информации должны, как минимум, включать дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе.

3. Защита информации о событиях безопасности

3.1. В информационных системах персональных данных школы должна обеспечиваться защита информации о событиях безопасности.

3.2. Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

3.3. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам.

3.4. Требования к защите информации о событиях безопасности:

– в информационных системах персональных данных обеспечивается резервное копирование записей регистрации (аудита);

– в информационных системах персональных данных обеспечивается резервное копирование записей регистрации (аудита) на носители однократной записи (неперезаписываемые носители информации);

– в информационных системах персональных данных для обеспечения целостности информации о зарегистрированных событиях безопасности должны применяться в соответствии с законодательством Российской Федерации криптографические методы;

– оператор предоставляет доступ к записям регистрации событий безопасности (аудита) ограниченному кругу сотрудников.

4. Ответственность

4.1. Ответственность за организацию парольной защиты в подразделении возлагается на Администратора безопасности информационной системы персональных данных.

4.2. Периодический контроль за соблюдением требований данной инструкции возлагается на Администратора безопасности информационной системы персональных данных.