|  |  |
| --- | --- |
|  | Приложение № 20 утверждено |
|  | распоряжением администрации городского поселения р.п.Средняя Ахтуба от 29 мая 2019г. № 136-р |
|  |  |  |

**ИНСТРУКЦИЯ**

**по организации защиты информации о событиях безопасности**

**в информационных систем персональных данных в Администрации**

**городского поселения р.п.Средняя Ахтуба Среднеахтубинского**

**муниципального района Волгоградской области**

# Общие положения

## Настоящая Инструкция предназначена для организации защиты информации о событиях безопасности в информационных систем персональных данных в Администрации городского поселения р.п.Средняя Ахтуба Среднеахтубинского муниципального района Волгоградской области (далее – Администрация).

## Действие настоящей Инструкции распространяется на Администратора безопасности информационных систем персональных данных (далее – Администратор).

# События безопасности

## К событиям безопасности, подлежащим регистрации в информационных системах персональных данных, принадлежащих Администрации, 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.

## В информационных системах персональных данных Администрации 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.

## 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.

## При регистрации входа/выхода пользователей в информационные системы персональных данных и 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.

## 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.

## 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).

## 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).

## 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).

## 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.

# Защита информации о событиях безопасности

## В информационных системах персональных данных Администрации должна обеспечиваться защита информации о событиях безопасности.

## 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.

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

## 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.

# Ответственность

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

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