УТВЕРЖДЕНА
приказом ГКУ НСО ЦСПН
Каргатского района
от «09» 04 2025 г.
№ 12

Инструкция по регистрации событий безопасности

1. Общие положения

1.1. Настоящая Инструкция разработана в целях реализации мер по регистрации событий безопасности, по обеспечению сбора, записи, хранения и защиты информации о событиях безопасности в информационных системах (далее – ИС) ГКУ НСО ЦСПН Каргатского района, а также возможности просмотра и анализа информации о таких событиях и реагирования на них.

1.2. Настоящая Инструкция определяет:

– порядок составления и утверждения перечня событий безопасности, подлежащих регистрации и сроки их хранения;

– порядок определения состава и содержания информации о событиях безопасности, подлежащих регистрации;

– порядок сбора, записи и хранения информации о событиях безопасности в течение определённого времени хранения;

– порядок мониторинга (просмотра, анализа) результатов регистрации событий безопасности и реагирования на них;

– порядок защиты информации о событиях безопасности.

2 Перечень событий безопасности подлежащих регистрации

2.1. Перечень событий безопасности, подлежащих регистрации в ИС, составляет администратор безопасности ИС.

2.2 Администратор безопасности ИС обеспечивает средствами защиты информации, установленными в ИС регистрацию следующих событий:

– вход (выход), а также попытки входа субъектов доступа в ИС 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 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 Администратор безопасности ИС отслеживает, чтобы записи событий содержали в себе:

– дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная);
– идентификатор субъекта доступа (устройства);
– спецификация защищаемого файла (логическое имя, тип);
– используемый интерфейс доступа;
– и (или) иную информацию о попытках доступа к информационным ресурсам ИС.

3 Порядок сбора, записи, хранения и мониторинга информации о событиях безопасности

3.1. Настройку журналов регистрации событий информационной безопасности в средствах защиты информации ИС осуществляет администратор безопасности ИС.

3.2. Сведения о настройке средств защиты информации в рамках сбора и регистрации событий информационной безопасности в ИС представлены в разделе «Настройка средств защиты информации» инструкции администратора безопасности ИС.

3.3. Администратор безопасности ИС должен **не реже 1 раза в неделю** просматривать журналы регистрации событий безопасности на предмет возможны инцидентов безопасности.

3.4. В случае выявления признаков инцидентов безопасности администратором безопасности ИС осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности в соответствии с Инструкцией по выявлению инцидентов и реагированию на них.

3.5. Настройки журналов регистрации событий информационной безопасности должны обеспечивать запись информации о поступающих событиях безопасности без переполнения памяти **в течение 1 месяца**.

3.6. Информация о событиях безопасности в ИС, не подлежащая автоматической регистрации (нерегистрируемые программно-аппаратные сбои и неисправности, нарушения организационно-правового плана) должна фиксироваться администратором безопасности ИС при её обнаружении в журнале событий безопасности самостоятельно.

3.7. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) предоставляется только администратору безопасности ИС.

3.8 В ИС должно осуществляться генерирование надежных меток времени и (или) синхронизация системного времени.

3.9 Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в ИС достигается посредством применения внутренних системных часов ИС.

4. Ответственность при управлении событиями информационной безопасности

4.1. Ответственность при управлении событиями информационной безопасности в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности ИС.

4.2. Ответственность за соблюдение требований настоящей Инструкции возлагается на всех сотрудников, эксплуатирующих ИС.