Приложение № 7
к приказу «Об обеспечении безопасности персональных данных в информационных системах персональных данных ФГБУЗ ММЦ им. Н.И. Пирогова ФМБА России» № 01-147 от 12.07.2022

Правила регистрации и аудита (просмотр, анализ) событий безопасности в информационных системах персональных данных Федерального государственного бюджетного учреждения здравоохранения «Мурманский многопрофильный центр имени Н.И. Пирогова Федерального медико-биологического агентства

I. Общие положения

1. Настоящее положение определяет процедуры и объёмы аудита, сроки и способ хранения и защиты информации о событиях безопасности в информационных системах персональных данных Федерального государственного бюджетного учреждения здравоохранения «Мурманский многопрофильный центр имени Н.И. Пирогова Федерального медико-биологического агентства» (далее Учреждение и ИСПДн).

2. Контроль за исполнением настоящих процедур осуществляет администратор информационной безопасности (далее – Администратор ИБ).

3. Администратор ИБ имеет право привлекать для данных видов работ организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

II. Определение событий безопасности, подлежащих регистрации, сроков их хранения, а также состава и содержания информации о событиях безопасности

1. События безопасности, подлежащие регистрации в информационной системе, и сроки их хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в ИСПДн.

2. Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, их состав и содержание определяется Администратором ИБ исходя из возможностей реализации угроз безопасности информации и фиксируется в Перечне событий безопасности, подлежащих регистрации в ИСПДн (далее – Перечень), утверждаемом приказом «Об обеспечении безопасности персональных данных в информационных системах персональных данных ФГБУЗ ММЦ им. Н.И. Пирогова ФМБА России» № 01-147 от 12.07.2022, приложение 13.

3. В ИСПДн регистрируется:

– вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (выключения) 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.

III. Сбор, запись и хранение информации о событиях безопасности

1. Администратор ИБ в соответствии с утвержденным Перечнем, устанавливает в настройках средств защиты информации, операционной системы и прикладного программного обеспечения события безопасности, подлежащие регистрации в текущий момент времени, а также их состав и содержание.

2. Объем памяти для хранения информации о событиях безопасности (объем журнала) рассчитывается и выделяется с учетом типов событий безопасности, подлежащих регистрации, составом и содержанием информации о событиях безопасности, подлежащих регистрации, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, установленного срока хранения информации о зарегистрированных событиях безопасности.

3. При возможности технической реализации производится архивирование журнала событий безопасности.

IV. Реагирование на сбои при регистрации событий безопасности

1. При наличии технической возможности реализуется оповещение (предупреждение) Администратора ИБ о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности.

2. Администратор ИБ, получив такое оповещение (предупреждение) о сбое, совместно с администратором ИСПДн проводит процедуры реагирования на сбой при регистрации событий, в том числе:

– выявляет причины сбоя при регистрации событий;

– производит перезапуск технических и (или) программных средств, участвующих в регистрации событий, а в случае необходимости их переустановку (перенастройку);

– проводит при необходимости очистку устаревших записей о событиях безопасности.

V. Аудит (просмотр, анализ) результатов регистрации событий

безопасности и реагирования на них

1. Администратор ИБ проводит аудит (просмотр и анализ) записей регистрации (аудита) всех событий, подлежащих регистрации в соответствии с периодичностью, установленной в Перечне.

2. Периодичность аудита (просмотра и анализа) записей регистрации (аудита) событий устанавливается исходя из обеспечения своевременного выявления признаков инцидентов информационной безопасности в ИСПДн.

3. В случае выявления признаков инцидентов информационной безопасности в ИСПДн Администратором ИБ осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности.

VI. Защита информации о событиях безопасности

1. Доступ к информации о событиях безопасности (в том числе к архивам событий безопасности) и настройкам механизмов регистрации событий должен иметь только Администратор ИБ.

2. Резервные копии записей регистрации (аудита) событий безопасности, записанные на съемные машинные носители информации, хранятся в металлических хранилищах (сейфах), доступ к которым имеет только Администратор ИБ.

VII. Пересмотр набора событий безопасности, подлежащих регистрации

1. Пересмотр и обновление (при необходимости) набора событий безопасности производится не реже одного раза в год.

2. Осуществляется пересмотр и обновление набора событий безопасности при:

- проведении работ по модернизации ИСПДн;
- внедрении новых информационных технологий;
- проведении процедуры оценки эффективности;
- иных событиях, влияющих на информационную безопасность.