федеральное государственное бюджетное образовательное учреждение высшего образования
«ОМСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ»
Министерства здравоохранения Российской Федерации

УТВЕРЖДАЮ
Ректор ФГБОУ ВО ОмГМУ
Минздрава России
_____ М.А. Ливзан
«10» 09 2024 г.

ПОЛОЖЕНИЕ

О РЕГЛАМЕНТЕ РЕГИСТРАЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ

КОНТРОЛЬНЫЙ

Омск 2024

ПРЕДИСЛОВИЕ

1. РАЗРАБОТАНО заведующим сектора информационной безопасности Ключенко А.А.

2. ПРИНЯТО ученым советом 19.09.2024 г., протокол № 10.

3. ВВЕДЕНО в действие с 23.09.2024 г. распоряжением от 20.09.2024 г. впервые.

СОДЕРЖАНИЕ

1 ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Настоящее Положение определяет состав и содержание информации о событиях безопасности, подлежащих регистрации, правила и процедуры сбора, записи, хранения и защиты информации о событиях безопасности в информационных системах персональных данных ФГБОУ ВО ОмГМУ Минздрава России (далее – Организации, ИС).

1.2 Требования настоящего Положения обязательны для пользователей (далее – Пользователи) и администраторов (далее – Администраторы) информационных систем персональных данных ФГБОУ ВО ОмГМУ Минздрава России.

2 НОРМАТИВНЫЕ ССЫЛКИ

В настоящем Положении использованы ссылки на следующие документы:

– Федеральный закон от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закона от 27 июля 2006 № 152-ФЗ «О персональных данных».

3 ОПРЕДЕЛЕНИЕ СОБЫТИЙ БЕЗОПАСНОСТИ, ПОДЛЕЖАЩИХ РЕГИСТРАЦИИ, И СРОКОВ ИХ ХРАНЕНИЯ

3.1 В ИС подлежат регистрации в текущий момент времени события безопасности, утвержденные Перечнем событий безопасности в Организации, подлежащих регистрации.

3.2 Состав и содержание информации о событиях безопасности, подлежащих регистрации, определяются в соответствии с пунктом 3 настоящего Регламента.

3.3 Сроки хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в ИС, в течение 3 месяцев.

3.4 Срок хранения информации о зарегистрированных событиях безопасности составляет не менее трех месяцев, если иное не установлено требованиями законодательства Российской Федерации.

4 ОПРЕДЕЛЕНИЕ СОСТАВА И СОДЕРЖАНИЯ ИНФОРМАЦИИ О СОБЫТИЯХ БЕЗОПАСНОСТИ, ПОДЛЕЖАЩИХ РЕГИСТРАЦИИ

4.1 Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить 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.

4.2 Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, приведены в Перечне событий безопасности в Организации, подлежащих регистрации.

5 СБОР, ЗАПИСЬ И ХРАНЕНИЕ ИНФОРМАЦИИ О СОБЫТИЯХ БЕЗОПАСНОСТИ В ТЕЧЕНИИ УСТАНОВЛЕННОГО ВРЕМЕНИ ХРАНЕНИЯ

5.1 Процедуры сбора, записи и хранения информации о событиях безопасности в течение установленного времени хранения предусматривают:

- возможность выбора администратором информационной безопасности событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности, определенных в соответствии с Перечнем событий безопасности в Организации, подлежащих регистрации;

- генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с Перечнем

событий безопасности в Организации, подлежащих регистрации, с составом и содержанием информации, установленными для соответствующего типа события;

- хранение информации о событиях безопасности в течение времени, установленного в соответствии с пунктом 2 настоящего Регламента.

5.2 Объем памяти для хранения информации о событиях безопасности рассчитывается и выделяется администратором информационной безопасности ИС с учетом типов событий безопасности, подлежащих регистрации в соответствии с Перечнем событий безопасности в Организации, подлежащих регистрации, составом и содержанием информации о событиях безопасности, подлежащих регистрации, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

6 РЕАГИРОВАНИЕ НА СБОИ РЕГИСТРАЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ

6.1 В ИС реагирование на сбои при регистрации событий безопасности (в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти) должно предусматривать:

- предупреждение (сигнализация, индикация) администратора информационной безопасности о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;

- реагирование на сбои при регистрации событий безопасности путем изменения администратором информационной безопасности параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов ИС, запись поверх устаревших хранимых записей событий безопасности.

7 МОНИТОРИНГ (ПРОСМОТР, АНАЛИЗ) РЕЗУЛЬТАТОВ РЕГИСТРАЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ И РЕАГИРОВАНИЕ НА НИХ

7.1 Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться администратором информационной безопасности не реже одного раза в неделю для всех событий, подлежащих регистрации в соответствии с Перечнем событий безопасности в Организации, подлежащих регистрации, и обеспечивать своевременное выявление признаков инцидентов безопасности в ИС.

7.2 В случае выявления признаков инцидентов безопасности в ИС администратор информационной безопасности осуществляет планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности.

8 ГЕНЕРИРОВАНИЕ ВРЕМЕННЫХ МЕТОК И (ИЛИ) СИНХРОНИЗАЦИЯ СИСТЕМНОГО ВРЕМЕНИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

8.1 В ИС осуществляется генерирование надежных меток времени и синхронизация системного времени.

8.2 Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в ИС достигается посредством применения внутренних системных часов информационной системы или путем синхронизации системного времени.

9 ЗАЩИТА ИНФОРМАЦИИ О СОБЫТИЯХ БЕЗОПАСНОСТИ

9.1 Защита информации о событиях безопасности (записях регистрации (аудита)) в ИС должна обеспечиваться применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в

проектной и организационно-распорядительной документации по защите информации, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

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

ПРИЛОЖЕНИЕ А

Лист ознакомления
с регламентом регистрации событий безопасности в информационных системах персональных данных

№ п/п	ФИО	Должность	Дата ознакомления	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				

ЛИСТ СОГЛАСОВАНИЯ

СОГЛАСОВАНО
Проректор по последипломному образованию
_____ А.С. Колчин
«12» 09 2024 г.

СОГЛАСОВАНО
Начальник юридического отдела
_____ О.В. Глевская
«11» 09 2024 г.

СОГЛАСОВАНО
Начальник ОА и ИТ
_____ Р.А. Ахмеров
«09» 09 2024 г.

СОГЛАСОВАНО
Заместитель начальника управления организации и контроля качества образования
_____ С.В. Плоткина
«12» 09 2024 г.