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
«__» 09 2024 г.

ПОЛОЖЕНИЕ

О РЕГЛАМЕНТЕ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ СУБЪЕКТОВ ДОСТУПА И ОБЪЕКТОВ ДОСТУПА В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

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.

Настоящее положение не может быть полностью или частично воспроизведено, тиражировано и распространено в качестве официального без разрешения ОмГМУ

СОДЕРЖАНИЕ

1 ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Настоящее Положение определяет порядок и процедуры присвоения субъектам и объектам доступа уникального признака (идентификатора), сравнения предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверки принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности), а также организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных ФГБОУ ВО ОмГМУ Минздрава России (далее – Организации, ИС) и контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

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 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ, ЯВЛЯЮЩИХСЯ ВНУТРЕННИМИ ПОЛЬЗОВАТЕЛЯМИ

3.1 При доступе в ИС осуществляется идентификация и аутентификация пользователей, являющихся работниками Организации (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также

процессов, запускаемых от имени системных учетных записей. К внутренним пользователям относятся должностные лица Организации:

- администратор ИС;

- администратор информационной безопасности (далее - ИБ);

- ответственные работники по работе с ИС, выполняющие свои должностные обязанности (функции) в соответствии с должностными регламентами (инструкциями), утвержденными в учреждении и которым в ИС присвоены учетные записи.

3.2 В качестве внутренних пользователей дополнительно рассматриваются должностные лица обладателя информации, заказчика, уполномоченного лица и (или) оператора иной информационной системы, а также лица, привлекаемые на договорной основе для обеспечения функционирования ИС (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с организационно-распорядительными документами Организации. Для каждого внутреннего пользователя в ИС должны быть заведены учетные записи.

3.3 Пользователи ИС однозначно идентифицируются и аутентифицируются для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации в соответствии с Регламентом управления доступом субъектов доступа к информационным системам персональных данных Организации.

3.4 Аутентификация пользователя в ИС осуществляется с использованием паролей. Также на усмотрение администратора ИБ могут применяться аппаратные средства в случае многофакторной (двухфакторной) аутентификации.

3.5 В ИС обеспечивается возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

4 УПРАВЛЕНИЕ ИДЕНТИФИКАТОРАМИ, В ТОМ ЧИСЛЕ СОЗДАНИЕ, ПРИСВОЕНИЕ, УНИЧТОЖЕНИЕ ИДЕНТИФИКАТОРОВ

4.1 В ИС устанавливаются и реализуются следующие функции управления идентификаторами пользователей и устройств:

- формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;

- присвоение идентификатора пользователю и (или) устройству;

- предотвращение повторного использования идентификатора пользователя и (или) устройства в течение одного года.

- блокирование идентификатора пользователя после 90 дней неиспользования.

4.2 В качестве ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств определен Администратор ИБ.

5 УПРАВЛЕНИЕ СРЕДСТВАМИ АУТЕНТИФИКАЦИИ И ПРИНЯТИЕ МЕР В СЛУЧАЕ УТРАТЫ И (ИЛИ) КОМПРОМЕТАЦИИ СРЕДСТВ АУТЕНТИФИКАЦИИ

5.1 В ИС устанавливаются и реализуются следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств:

- изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты ИС;

- выдача средств аутентификации пользователям;

генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации);

- установление характеристик пароля: длина пароля не менее восьми символов, алфавит пароля не менее 60 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки 5 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации на 5 минут, смена паролей не более чем через 120 дней;

- блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации;

назначение необходимых характеристик средств аутентификации (в том числе механизма пароля);

- обновление аутентификационной информации (замена средств аутентификации) с периодичностью не более, чем через 120 дней;

защита аутентификационной информации от неправомерных доступа к ней и модифицирования.

5.2 В случае компрометации личного пароля пользователя ИС должны быть немедленно предприняты меры в зависимости от полномочий владельца скомпрометированного пароля:

- внеплановая смена личного пароля или удаление учетной записи пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и т.п.) должна производиться администратором ИБ немедленно после окончания последнего сеанса работы данного пользователя с системой;

- внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации и другие обстоятельства) администратора ИБ и других работников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС.

5.3 В качестве ответственного за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации устройств определен администратор ИБ.

6 ЗАЩИТА ОБРАТНОЙ СВЯЗИ ПРИ ВВОДЕ АУТЕНТИФИКАЦИОННОЙ ИНФОРМАЦИИ

6.1 В ИС осуществляется защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

6.2 Защита обратной связи «система – субъект доступа» в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками «*», «•» или иными знаками.

7 ОТВЕТСТВЕННОСТЬ ПРИ ОРГАНИЗАЦИИ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

7.1 Ответственность за реализацию правил идентификации и аутентификации субъектов доступа и объектов доступа в соответствии с требованиями настоящего Регламента возлагается на администратора ИБ.

7.2 Ответственность за поддержание установленного порядка и соблюдение требований настоящего Регламента возлагается на администратора ИБ и пользователей ИС.

7.3 Периодический контроль за выполнением всех требований настоящего Регламента осуществляется комиссией по проведению мероприятий по защите информации.

ПРИЛОЖЕНИЕ А

Лист ознакомления
с регламентом идентификации и аутентификации субъектов доступа и объектов доступа 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.