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_» ___09___ 2024 г.

ПОЛОЖЕНИЕ

О РЕГЛАМЕНТЕ УПРАВЛЕНИЯ ДОСТУПОМ СУБЬЕКТОВ ДОСТУПА К ОБЬЕКТОМ 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.

СОДЕРЖАНИЕ

1 ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Настоящее Положение определяет права и привилегии субъектов доступа, описывает разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационных системах персональных данных ФГБОУ ВО ОмГМУ Минздрава России (далее – Организации, ИС) правил разграничения доступа, а также контроль соблюдения этих правил.

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 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Аутентификационная информация - информация, используемая для установления подлинности (верификации) субъекта доступа в информационной системе.

Аутентификация - проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной системе).

Идентификатор - представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа в информационной системе.

Идентификация - присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

Локальный доступ - доступ субъектов доступа к объектам доступа, осуществляемый непосредственно через подключение (доступ) к компоненту информационной системы или через локальную вычислительную сеть (без использования информационно-телекоммуникационной сети).

Многофакторная аутентификация - аутентификация с использованием двух (двухфакторная) или более различных факторов аутентификации.

Непривилегированная учетная запись - учетная запись пользователя (процесса, выполняемого от его имени) информационной системы.

Объект доступа - единица информационного ресурса информационной системы (файл, техническое средство, узел сети, линия (канал) связи, мобильное устройство, программа, том, каталог, запись, поле записей и иные объекты), доступ к которой регламентируется правилами разграничения доступа и по отношению к которой субъекты доступа выполняют операции.

Пользователь - лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее результаты ее функционирования.

Привилегированная учетная запись - учетная запись администратора информационной системы.

Роль - предопределенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и информационной системой.

Субъект доступа - пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа.

Удаленный доступ - процесс получения доступа (через внешнюю сеть) к объектам доступа информационной системы из другой информационной системы

(сети) или со средства вычислительной техники, не являющегося постоянно (непосредственно) соединенным физически или логически с информационной системой, к которой он получает доступ.

Управление доступом - ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа.

4 ОБЩИЕ ПОЛОЖЕНИЯ

4.1 Разграничение прав осуществляется на основании Модели угроз и нарушителя безопасности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, при её обработке в информационных системах персональных данных Организации, а также исходя из характера и режима обработки информацию ограниченного доступа, не содержащую сведения, составляющие государственную тайну (далее – Информация) в ИС.

4.2 Уровень прав доступа представлен в Таблице 1.

Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС, осуществляется в соответствии с их должностными обязанностями. Доступ к объектам доступа с учетом разделения полномочий (ролей) обеспечивается в соответствии с матрицей доступа (утверждается отдельным локальным нормативным актом Организации).

Таблица 1 – Роли пользователей

№ п/п	Группа	Уровень доступа	Разрешенные действия
1.	Администратор ИС	Доступ на правах администратора к Информации, техническим средствам (далее - ТС) и прикладному программному обеспечению (далее - ПО). Без доступа к средствам	– модернизация, настройка и мониторинг работоспособности комплекса ТС (серверов, рабочих станций); – установка, модернизация, настройка и мониторинг работоспособности системного и базового ПО; – установка, настройка и мониторинг прикладного ПО;

№ п/п	Группа	Уровень доступа	Разрешенные действия
		защиты информации (далее - СЗИ)	– соблюдение правил, оговоренных в инструкции администратора.
2.	Администратор информационной безопасности (далее - ИБ)	Доступ на правах администратора к СЗИ. Без доступа на изменение к Информации, ТС и прикладному ПО	– разработка, управление и реализация эффективной политики информационной безопасности системы; – управление (администрирование) системой защиты информации ИС; – выявление инцидентов и реагирование на них; – управление конфигурацией информационной системы (далее - ИС) и ее системы защиты; – контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в ИС; – управление правами доступа пользователей к функциям системы; – проверка состояния используемых СЗИ от несанкционированного доступа (далее - НСД), проверка правильности их настройки; – обеспечение функционирования и поддержание работоспособности СЗИ; – проведение инструктажа эксплуатационного персонала и пользователей средств вычислительной техники (далее - СВТ) по правилам работы с используемыми СЗИ; – контроль и предотвращение несанкционированного изменения целостности ресурсов; – контроль аппаратной конфигурации защищаемых компьютеров и предотвращение попытки ее несанкционированного изменения
3.	Ответственный за эксплуатацию средств криптографической защиты информации (далее - СКЗИ)	Доступ на правах администратора к сертифицированным СКЗИ. Без доступа на изменение к Информации, ТС, прикладному ПО, СЗИ	– поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним; – контроль за соблюдением условий использования криптосредств, установленных эксплуатационной и технической документацией на СКЗИ и настоящей инструкцией; – учет Пользователей криптосредств; – надежное хранение эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей дистрибутивов криптосредств,

№ п/п	Группа	Уровень доступа	Разрешенные действия
			бумажных и машинных носителей Информации; – расследования и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации; – разработка и принятие мер по предотвращению возможных негативных последствий нарушений
4.	Ответственный за обработку и защиту информации	Доступ на правах пользователя к Информации, ТС, прикладному ПО и СЗИ. Без доступа на изменение ПО, СЗИ и ТС	– контроль (мониторинг) за обеспечением уровня защищенности информации – информирование пользователей о требованиях законодательства Российской Федерации об Информации, локальных актов по вопросам обработки и защиты Информации. – внутренний контроль (проверки) над соблюдением законодательства Российской Федерации об Информации, в том числе требований к защите Информации
5.	Пользователь	Доступ на правах пользователя к Информации, ТС, прикладному ПО и СЗИ. Без доступа на изменение ПО, СЗИ и ТС	– сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, предоставление записей, содержащих Информацию

4.3 Должен быть утвержден перечень лиц, имеющих доступ в помещения, в которых расположены технические средства ИС (далее – Помещения), в соответствии с правами, минимально необходимыми для выполнения ими своих должностных обязанностей. Должен быть исключен неконтролируемый доступ в Помещения.

4.4 Работники Организации, которые в рамках своих должностных обязанностей обрабатывают Информацию, должны быть внесены в Перечень лиц, имеющих доступ в помещения, в которых расположены технические средства ИС, и доступ к обработке информации в ИС.

5 ПРАВИЛА РАЗГРАНИЧЕНИЯ ДОСТУПА

5.1 В ИС организовано (реализовано):

5.1.1 Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей, возлагается на администратора ИБ, внутри виртуальных машин на администратора ВИ, путем следующих функций:

– определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная);

– объединение учетных записей в группы (при необходимости);

– верификация пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;

– заведение, активация, блокирование и уничтожение учетных записей пользователей (при необходимости);

– пересмотр и, при необходимости, корректировка учетных записей не реже одного раза в три месяца;

– порядок заведения и контроля использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов;

– уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе;

– предоставление пользователям прав доступа к объектам доступа ИС, основываясь на задачах, решаемых пользователями в ИС и взаимодействующими с ней информационными системами;

– использование автоматизированных средств поддержки управления учетными записями пользователей;

– автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования.

Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, работникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).

Заведение временных учетных записей осуществляется на основании подписанного администратором ИБ и ответственным за обработку и защиту Информации, утвержденного руководителем Организации соответствующего Акта, содержащего цель, место, наименование и сроки их использования, по истечении которых осуществляется автоматическое блокирование временных учетных записей пользователей.

5.1.2 Дискреционный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа. Типы доступа должны включать операции по чтению, записи, удалению, выполнению и иные операции, разрешенные к выполнению пользователем (группе пользователей).

Правила разграничения доступа реализуются на основе матрицы доступа и обеспечивают управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе к ТС, устройствам (в том числе внешним), объектам файловой системы, запускаемым и исполняемым модулям, объектам систем управления базой данных, параметрам настройки СЗИ, в том числе внутри виртуальных машин, информации о

конфигурации системы защиты информации и иной информации о функционировании системы защиты информации.

В ИС правила разграничения доступа должны обеспечивать:

– управление доступом субъектов при входе в ИС;

– управление доступом субъектов к ТС, устройствам, внешним устройствам;

– управление доступом субъектов к объектам, создаваемым общесистемным (общим) ПО.

5.1.3 В ИС осуществляется управление информационными потоками, которое обеспечивает разрешенный маршрут прохождения информации между пользователями, устройствами в рамках информационной системы и между информационными системами или при взаимодействии с сетью Интернет (или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными потоками, включающих контроль конфигурации информационной системы, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации). Управление информационными потоками должно блокировать передачу защищаемой информации через сеть Интернет (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из информационной системы и (или) входящие в информационную систему.

5.1.4 Ограничение неуспешных попыток входа в ИС (доступа к ИС), в том числе виртуальных машин, равно 3 (трем), при этом должно быть обеспечено блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения

количества неуспешных попыток входа в ИС (доступа к ИС) не менее чем на 5 (пять) минут (с возможностью разблокирования только администратором ИБ).

5.1.5 Блокирование сеанса доступа в ИС, в том числе виртуальных машин, после 15 минут времени бездействия (неактивности) пользователя или по его запросу.

Блокирование сеанса доступа пользователя в ИС обеспечивает временное приостановление работы пользователя со СВТ или с виртуальной машиной, с которого осуществляется доступ к ИС (без выхода из ИС).

Для заблокированного сеанса осуществляется блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.

Блокирование сеанса доступа пользователя в ИС сохраняется до прохождения им повторной идентификации и аутентификации.

5.1.6 Запрет всех действий пользователей до прохождения процедур идентификации и аутентификации в ИС (кроме необходимых для прохождения процедур идентификации и аутентификации), в том числе виртуальных машин.

Администратору ИБ разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования ИС в случае сбоев в работе или выходе из строя отдельных ТС (устройств).

В ИС обеспечивается защита информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа ИС (в том числе внутри виртуальных машин) через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и (или) мобильных ТС (защита удаленного доступа).

Защита удаленного доступа включает:

– разрешение только проводного (коммутируемого), и широкополосного доступов для удаленного доступа к объектам доступа информационной системы;

– ограничение на использование удаленного доступа в соответствии с задачами (функциями) ИС, для решения которых такой доступ необходим;

– предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций), с письменного согласия руководителя Организации;

– мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа ИС;

– контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа ИС до начала информационного взаимодействия с ИС (передачи защищаемой информации);

– использование ограниченного (минимально необходимого) количества точек подключения к ИС при организации удаленного доступа к объектам доступа ИС;

– исключение удаленного доступа от имени привилегированных учетных записей (администраторов) для администрирования ИС и ее системы защиты информации.

ПРИЛОЖЕНИЕ А

Лист ознакомления
с Регламентом управления доступом субъектов доступа к объектам 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 ОА и ИТ

_____ Р.А. Ахмеров
«09» 09 2024 г.

СОГЛАСОВАНО
Начальник юридического отдела

_____ О.В. Глевская
«11» 09 2024 г.

СОГЛАСОВАНО
Заместитель начальника управления организации и контроля качества образования

_____ С.В. Плоткина
«12» 09 2024 г.