УТВЕРЖДАЮ
министр цифрового развития
и связи Кузбасса
_____ М.В. Садиков
«17» марта 2020 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
органам местного самоуправления и подведомственным учреждениям по осуществлению управления доступом субъектов доступа к объектам доступа в информационных системах персональных данных

I. Общие положения

1. Настоящее Положение определяет права и привилегии субъектов доступа, описывает разграничение доступа субъектов доступа к объектам доступа на основе совокупности правил разграничения доступа, установленных в информационных системах персональных данных (далее - ИСПДн), а также контроль соблюдения этих правил в ОМСУ и подведомственных учреждений.

2. Разграничение прав осуществляется на основании "Модели угроз безопасности персональных данных при их обработке в ИСПДн", а также исходя из характера и режима обработки персональных данных в ИСПДн.

3. Уровень прав доступа представлен в таблице 1.

Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИСПДн, осуществляется в соответствии с их должностными обязанностями. Доступ к объектам доступа с учетом разделения полномочий (ролей) обеспечивается в соответствии с матрицей субъектов доступа по отношению к защищаемым информационным ресурсам в ИСПДн (далее - матрица доступа).

Таблица 1. Уровень прав доступа.

№ п/п	Группа	Уровень доступа к ПДн, ТС, прикладному ПО и СЗИ	Разрешенные действия
1	Администратор ИСПДн	Доступ на правах администратора к ПДн, ТС и прикладному ПО. Без доступа к СЗИ	1) модернизация, настройка и мониторинг работоспособности комплекса ТС (серверов, рабочих станций); 2) установка, модернизация, настройка и мониторинг работоспособности системного и базового ПО; 3) установка, настройка и мониторинг

№ п/п	Группа	Уровень доступа к ПДн, ТС, прикладному ПО и СЗИ	Разрешенные действия
			прикладного ПО; 4) соблюдение правил, оговоренных в инструкции администратора
2	Администратор ИБ ИСПДн	Доступ на правах администратора к СЗИ. Без доступа на изменение к ПДн, ТС и прикладному ПО	1) разработка, управление и реализация эффективной политики информационной безопасности системы; 2) управление (администрирование) системой защиты информации ИСПДн; 3) выявление инцидентов и реагирование на них; управление конфигурацией ИСПДн и ее системы защиты; 4) контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в ИСПДн; управление правами доступа пользователей к функциям системы; 5) проверка состояния используемых СЗИ от НСД, проверка правильности их настройки; 6) обеспечение функционирования и поддержание работоспособности СЗИ; проведение инструктажа эксплуатационного персонала и пользователей СВТ по правилам работы с используемыми СЗИ; 7) контроль и предотвращение несанкционированного изменения целостности ресурсов; 8) контроль аппаратной конфигурации защищаемых компьютеров и предотвращение попытки ее несанкционированного изменения
3	Администратор ВИ	Доступ на правах администратора к прикладному ПО. Без доступа на изменение ПДн, ТС и СЗИ	1) установка, модернизация, настройка и мониторинг работоспособности ВИ; 2) доступ к операциям создания, запуска, останова, создания копий, удаления виртуальных машин; 3) доступ к конфигурации виртуальных машин
4	Администратор резервного копирования	Доступ на правах администратора к прикладному ПО. Без доступа на	1) настройка и контроль работы процедуры резервного копирования; 2) изготовление резервных копий информации;

№ п/п	Группа	Уровень доступа к ПДн, ТС, прикладному ПО и СЗИ	Разрешенные действия
		изменение ПДн, ТС и СЗИ	3) анализ объемов данных резервного копирования; 4) контроль состояния оборудования системы резервного копирования; 5) замена неработоспособных или выработавших свой ресурс носителей резервной информации или оборудования системы резервного копирования; 6) восстановление программ и данных из резервных копий в случае порчи или утери данных
5	Ответственный за эксплуатацию СКЗИ	Доступ на правах администратора к сертифицированным СКЗИ. Без доступа на изменение к ПДн, ТС, прикладному ПО, СЗИ	1) поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним; 2) контроль за соблюдением условий использования криптосредств, установленных эксплуатационной и технической документацией на СКЗИ и настоящей инструкцией; 3) учет Пользователей криптосредств; 4) надежное хранение эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей дистрибутивов криптосредств, бумажных и машинных носителей ПДн; 5) расследования и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации; 6) разработка и принятие мер по предотвращению возможных негативных последствий нарушений
6	Пользователь	Доступ на правах пользователя к ПДн, 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 ПДн

4. Доступ в помещения, в которых расположены технические средства ИСПДн (далее - Помещения), осуществляется в соответствии с перечнем лиц, утверждаемым приказом. Допускается утверждение списка лиц, допущенных

в помещения, где производится обработка информации, содержащей персональные данные, отдельным документом с обязательным размещением такого списка с внутренней стороны входной двери.

II. Правила разграничения доступа

5. В ИСПДн реализуется:

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

а) определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная и (или) иные типы записей);

б) объединение учетных записей в группы (при необходимости);

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

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

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

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

ж) предоставление пользователям прав доступа к объектам доступа ИСПДн, основываясь на задачах, решаемых пользователями в ИСПДн и взаимодействующими с ней ИСПДн.

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, сотрудникам 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 персональных данных соответствующего Акта, содержащего цель, место, наименование и сроки;

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 (группой 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 СУБД, параметрам настройки СЗИ, в том числе внутри виртуальных машин, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации.

В ИСПДн правила разграничения доступа должны обеспечивать:

а) управление доступом субъектов при входе в ИСПДн;

б) управление доступом субъектов к ТС, устройствам, внешним устройствам;

в) управление доступом субъектов к объектам, создаваемым общесистемным (общим) ПО;

г) управление доступом субъектов внутри виртуальной инфраструктуры.

3) в ИСПДн осуществляется управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной системы, включающее:

а) фильтрацию информационных потоков в соответствии с установленными правилами управления потоками;

б) разрешение передачи информации в ИСПДн только по установленному маршруту;

в) изменение (перенаправление) маршрута передачи информации в случаях необходимости, по согласованию с администратором информационной безопасности.

4) права и привилегии, назначаемые пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование ИСПДн, являются минимально необходимыми для выполнения ими своих должностных обязанностей (функций);

5) ограничение неуспешных попыток входа в ИСПДн (доступа к ИСПДн), равное 5 (пяти), при этом обеспечивается блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в ИСПДн (доступа к ИСПДн) не менее чем на 5 (пять) минут;

6) блокирование сеанса доступа в ИСПДн, после 10 минут времени бездействия (неактивности) пользователя или по его запросу.

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

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

Блокирование сеанса доступа пользователя в ИСПДн сохраняется до прохождения им повторной идентификации и аутентификации;

7) запрет всех действий пользователей до прохождения процедур идентификации и аутентификации в ИСПДн (кроме необходимых для прохождения процедур идентификации и аутентификации).

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

Применяемые термины и сокращения:

Аутентификационная информация (информация аутентификации)	-	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 с использованием двух

аутентификация		(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.

ВИ	-	виртуальная инфраструктура.
ИБ	-	информационная безопасность.
ИСПДн	-	информационная система персональных данных.
НСД	-	несанкционированный доступ.
ОМСУ	-	органы местного самоуправления Кемеровской области - Кузбасса.
ПО	-	программное обеспечение.
СВТ	-	средство вычислительной техники.
СЗИ	-	средство защиты информации.
СКЗИ	-	средство криптографической защиты информации.
СУБД	-	система управления базой данных.
ТС	-	техническое средство.

Начальник отдела данных
и информационной безопасности С.С. Фомин