МИНИСТЕРСТВО ОБРАЗОВАНИЯ НОВОСИБИРСКОЙ ОБЛАСТИ

ПРИКАЗ

24 ИЮН 2022 1252

г. Новосибирск

Об утверждении Правил управления доступом субъектов доступа к объектам доступа в информационных системах министерства образования Новосибирской области и Матрицы доступа субъектов доступа по отношению к объектам доступа в информационных системах министерства образования Новосибирской области

В целях выполнения Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», реализации Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», **п р и к а з ы в а ю :**

1. Утвердить прилагаемые:

1) Правила управления доступом субъектов доступа к объектам доступа в информационных системах министерства образования Новосибирской области;

2) Матрицу доступа субъектов доступа по отношению к объектам доступа в информационных системах министерства образования Новосибирской области.

2. Контроль за исполнением настоящего приказа оставляю за собой.

Министр С.В. Федорчук

Галушко Г.А.
238-73-41

УТВЕРЖДЕНЫ
приказом Минобразования
Новосибирской области
от 24 ИЮН 2022 № 1252

ПРАВИЛА
управлении доступом субъектов доступа к объектам доступа в информационных системах министерства образования Новосибирской области
(далее – Правила)

I. Общие положения

1. Правила разработаны в целях реализации мер защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – информация), по управлению доступом субъектов доступа к объектам доступа в информационных системах (далее – ИС) министерства образования Новосибирской области (далее – Министерство, оператор).

2. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в ИС правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

II. Термины и определения

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).

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.

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.

III. Управление учетными записями пользователей

3. В ИС Министерства должны реализовываться следующие функции управления учетными записями пользователей:

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 функциональных обязанностей) при заведении учетной записи пользователя;

заведение, активация, блокирование и уничтожение учетных записей пользователей;

пересмотр и, при необходимости, корректировка учетных записей пользователей с установленной периодичностью;

регламентирование порядка 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 ИС;

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

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

5. По истечении установленного срока использования временных учетных записей должно осуществляться автоматическое блокирование временных учетных записей пользователей.

Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей ИС Министерства осуществляют лица с полномочиями системных администраторов ИС Министерства.

IV. Правила разграничения доступа

6. В зависимости от особенностей функционирования ИС, с учетом угроз безопасности информации в ИС Министерства реализуется один или комбинация следующих методов управления доступом:

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;

ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа (совокупность действий и обязанностей, связанных с определенным видом деятельности).

7. 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 техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, объектам, создаваемым прикладным и специальным программным обеспечением, параметрам настройки средств защиты информации, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации, а также иным объектам доступа.

8. Оператором должно обеспечиваться разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС, в соответствии с их должностными обязанностями (функциями), и санкционирование доступа к объектам доступа в соответствии с разделением полномочий (ролей).

9. В ИС Министерства должно осуществляться ограничение количества неуспешных попыток входа в ИС (доступа к ИС), а также обеспечиваться 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) на установленный период времени.

10. В ИС Министерства должно обеспечиваться блокирование сеанса доступа пользователя после установленного времени его бездействия (неактивности) в ИС или по запросу пользователя ИС.

11. Блокирование сеанса доступа пользователя в ИС должно обеспечивать временное приостановление работы пользователя со средством вычислительной техники, с которого осуществляется доступ к ИС (без выхода из ИС).

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

13. Блокирование сеанса доступа пользователя в ИС должно сохраняться до прохождения им повторной идентификации.

14. В ИС Министерства запрещены любые действия до прохождения ими процедур идентификации и аутентификации (кроме необходимых для прохождения процедур идентификации и аутентификации).

V. Управление информационными потоками

15. В ИС Министерства должно осуществляться управление информационными потоками, обеспечивающее разрешенный маршрут прохождения информации между пользователями, устройствами в рамках ИС и между ИС или при взаимодействии с сетью Интернет (или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными потоками, включающих контроль конфигурации ИС, 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 ИС и (или) входящие в ИС.

VI. Правила применения удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети

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

17. Защита удаленного доступа должна обеспечиваться для всех видов доступа и включает:

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

предоставление удаленного доступа только лицам, которым он необходим для выполнения установленных должностных обязанностей (функций) или для осуществления технической поддержки на основании договора;

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.

VII. Управление взаимодействием с информационными системами сторонних организаций (внешними ИС)

18. В ИС Министерства должно осуществляться управление взаимодействием с внешними ИС и включать определение порядка обработки, хранения и передачи информации с использованием внешних ИС.

19. Оператор разрешает обработку, хранение и передачу информации с использованием внешней ИС при выполнении следующих условий:

при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней информационной системы;

при наличии подтверждения выполнения во внешней ИС предъявленных к ней требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

VIII. Ответственность

20. Оператор и должностные лица несут ответственность за правонарушения в сфере информации, информационных технологий и защиты информации в соответствии с законодательством Российской Федерации.

УТВЕРЖДЕНА
приказом Минобразования
Новосибирской области
от 24 ИЮН 2022 № 1252

МАТРИЦА
доступа субъектов доступа по отношению к объектам доступа в информационных системах министерства образования Новосибирской области (далее – Матрица)

1. Матрица устанавливает полномочия субъектов доступа по доступу к объектам доступа в информационных системах (далее – ИС) министерства образования Новосибирской области (далее – Министерство).

2. Предоставление пользователям прав доступа к объектам доступа информационных систем осуществляется, основываясь на задачах, решаемых пользователями в ИС Министерства.

3. В Министерстве для управления доступом используется ролевой метод управления доступом.

4. В ИС Министерства обеспечено разделение полномочий (ролей) субъектов доступа ИС, роли пользователей определены в соответствии с минимально необходимыми правами и привилегиями.

5. Учет имеющихся у работников ролей, а также их изменений ведется ответственным за защиту информации, не содержащей сведения, составляющие государственную тайну, содержащейся в информационных системах Министерства (далее – ответственный за защиту информации).

6. Для субъектов доступа определены роли, приведенные в Таблице 1.

Таблица 1 – Роли субъектов доступа

Идентификатор роли	Наименование роли	Уровень полномочий
Р1	Администратор ИС (системный администратор)	Привилегированная роль в ИС, разрешены действия (операции) по управлению (администрированию) ИС (администрирование программных и технических средств обработки защищаемой информации, в том числе внесение изменений в базовую конфигурацию ИС), без права управления (администрирования) средствами защиты информации
Р2	Администратор системы защиты информации	Привилегированная роль в ИС, разрешены действия (операции) по управлению (администрированию) системой защиты

Идентификатор роли	Наименование роли	Уровень полномочий
	(Администратор безопасности)	информации ИС (администрирование программных и программно-аппаратных средств обеспечения безопасности – средств защиты информации, внесение изменений в их конфигурацию)
Р3	Пользователь	Непривилегированная роль в ИС, имеет следующие разрешения: – ограниченный доступ к ресурсам АРМ ИС (информации, техническим средствам, прикладному программному обеспечению и средствам защиты информации): без права управления (администрирования) ИС и системой защиты ИС, без права внесения изменений в конфигурацию технических и программных средств ИС (в том числе средств защиты информации); – действия (операции) по обработке информации в ИС с использованием технологии локального доступа

7. Перечень категорий лиц, имеющих доступ к информационным ресурсам ИС Министерства, с указанием их роли приведен в таблице 2.

Таблица 2 – Перечень категорий лиц, имеющих доступ к информационным ресурсам ИС Министерства

№ п/п	Категория лиц	Роль
1.	Работники Министерства и государственного бюджетного учреждения дополнительного профессионального образования Новосибирской области «Новосибирский институт повышения квалификации и переподготовки работников образования» (пользователи ИС (внутренние), ответственный за организацию обработки персональных данных, ответственный за защиту информации, ответственный за эксплуатацию средств криптографической защиты информации)	Р3
2.	Работники государственного бюджетного учреждения Новосибирской области «Центр защиты информации Новосибирской области»	Р2
3.	Работники Министерства, обеспечивающие администрирование системы защиты информации	
4.	Работники государственного бюджетного учреждения Новосибирской области «Центр информационных	Р1

	технологий Новосибирской области»	
5.	Работники Министерства, обеспечивающие функционирование ИС	

8. Для субъектов доступа ИС Министерства установлены разрешения согласно таблице 3.

Таблица 3 – Разрешения, установленные для субъектов доступа

Разрешения	Разрешить	Запретить	Разрешить	Запретить
	Р1/Р2		Р3	
Обзор папок	☐	☐	☐	☐
Выполнение файлов	☐	☐	☐	☐
Чтение данных	☐	☐	☐	☐
Чтение атрибутов	☐	☐	☐	☐
Чтение дополнительных атрибутов	☐	☐	☐	☐
Создание файлов/Запись данных	☐	☐	☐	☐
Создание папок/Запись данных	☐	☐	☐	☐
Запись атрибутов	☐	☐	☐	☐
Удаление папок и файлов	☐	☐	☐	☐
Чтение разрешений	☐	☐	☐	☐
Смена разрешений прав доступа к файлам и папкам	☐	☐	☐	☐
Смена владельца файла или папки	☐	☐	☐	☐
Печать	☐	☐	☐	☐
Управление принтерами	☐	☐	☐	☐
Управление документами	☐	☐	☐	☐

9. Наличие доступа к объектам доступа ИС Министерства в зависимости от полномочий (роли) отражено в таблице 4.

Таблица 4 – Наличие доступа к объектам ИС министерства образования Новосибирской области

Объект доступа	Наличие доступа, условия и ограничения по доступу		
	Р1	Р2	Р3
Устройства			
Автоматизированное рабочее место (АРМ)	+ без доступа к обрабатываемой информации	+ без доступа к обрабатываемой информации	+
Сетевое и коммутационное оборудование	+	+	без права конфигурирования

Объект доступа	Наличие доступа, условия и ограничения по доступу		
	Р1	Р2	Р3
			оборудования
Съемные машинные носители (CD/DVD, флеш-накопители и т.д.)	+ без доступа к обрабатываемой информации	+ без доступа к обрабатываемой информации	+
Объекты файловой системы			
Жесткий диск, личный каталог	+	+	+
Жесткий диск, служебные (в том числе системные) каталоги	+	+	+ ограниченный доступ
Запускаемые и исполняемые модули			
Запускаемые и исполняемые модули прикладного программного обеспечения, непосредственно участвующего в обработке информации	+ без доступа к обрабатываемой информации	+ без доступа к обрабатываемой информации	+ без права конфигурирования программного обеспечения
Запускаемые и исполняемые модули прикладного программного обеспечения, непосредственно не участвующего в обработке информации	+	+	+ без права конфигурирования программного обеспечения