Минобрнауки России
Федеральное государственное бюджетное научное учреждение
«Федеральный исследовательский центр
Институт прикладной физики им. А.В. Гапонова-Грехова
Российской академии наук»
(ИПФ РАН)

ПРИКАЗ

23.05.2024 № 204

Нижний Новгород

О разрешительной системе доступа

Во исполнение Федерального закона №152-ФЗ от 27.07.2006 г. «О персональных данных» и прочих нормативных документов по защите информации, п р и к а з ы в а ю:

1. Утвердить прилагаемое Положение о разрешительной системе доступа в информационных системах персональных данных Федерального государственного бюджетного научного учреждения «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук» (далее - Положение).
2. Требования прилагаемого Положения довести до работников, непосредственно осуществляющих защиту персональных данных.
3. Контроль за исполнением настоящего приказа оставляю за собой.

Директор
академик РАН Г.Г. Денисов

Приложение № 1 к приказу
от "23".05.2024 г. № 204

ПОЛОЖЕНИЕ
о разрешительной системе доступа в информационных системах персональных данных Федерального государственного бюджетного научного учреждения «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук»

1. Основные термины и определения

Дискреционный метод управления доступом - 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.

Доступ к информации - ознакомление с информацией, ее обработка, в частности, копирование модификация или уничтожение информации.

Матрица доступа - таблица, отображающая правила разграничения доступа.

Объект доступа – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Правила разграничения доступ - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Ролевой метод управления доступом - метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа.

Субъект доступа – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Типы доступа - операции, разрешенные к выполнению субъектом доступа при доступе к объектам доступа.

2. Общие положения

2.1 Настоящее Положение о разрешительной системе доступа (далее – Положение) в информационных системах персональных данных Федерального государственного бюджетного научного учреждения «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук», разработано в соответствии с законодательством Российской Федерации о персональных данных и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности персональных данных при их обработке в информационных системах персональных данных.

2.2 Настоящее Положение определяет методы управления доступом, типы доступа и правила разграничения доступа субъектов доступа к объектам доступа в информационных системах персональных данных.

2.3 Настоящее Положение вступает в силу с момента его утверждения директора Института и действует бессрочно, до замены его новым Положением.

2.4 Все изменения в Положение вносятся приказом директора организации.

2.5 Положение обязательно для исполнения всеми работниками Института, непосредственно осуществляющими защиту персональных данных.

3. Субъекты и объекты доступа

3.1 К субъектам доступа информационных системах персональных данных, относятся

работники Института, выполняющие свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств информационной системы персональных данных в соответствии с должностными инструкциями и которым в информационной системе персональных данных присвоены учетные записи.

3.2 К объектам доступа в информационных системах персональных данных, относятся:

- основные конфигурационные файлы операционной системы;
- средства настройки и управления операционной системой;
- основные конфигурационные файлы средств защиты информации;
- средства настройки и управления средств защиты информации;
- прикладное программное обеспечение;
- периферийные устройства;
- съемные машинные носители информации;
- обрабатываемые, хранимые данные.

4. Методы управления доступом

4.1 Методы управления доступом реализуются в соответствии с особенностями функционирования информационной системы персональных данных и с учетом угроз безопасности персональных данных и включают комбинацию следующих методов:

- ролевой метод управления доступом;
- дискреционный метод управления доступом.

4.2 Реализация ролевого метода управления доступом в информационных системах персональных данных представлена в таблице 1.

Таблица 1

№ п/п	Роль субъекта доступа	Уровень доступа к объектам доступа
1	Администратор информационной системы персональных данных	- обладает полной информацией о системном и прикладном программном обеспечении информационной системы персональных данных; - обладает полной информацией о технических средствах и конфигурации информационной системы персональных данных; - обладает правами конфигурирования и административной настройки технических средств информационной системы персональных данных; - обладает правами внесения изменений в программное обеспечение информационной системы персональных данных на стадии ее разработки, внедрения и сопровождения.
2	Ответственный за защиту информации	- обладает правами администратора информационной системы персональных данных; - обладает полной информацией об используемых в информационной системе персональных данных средствах защиты; - обладает правами конфигурирования средств защиты, используемых в информационной системе персональных данных.
3	Пользователь	- обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к обрабатываемой информации.

4.2 Дискреционный метод управления доступом в информационных системах персональных данных реализуется с помощью «Матрицы доступа работников, к ресурсам информационной системы персональных данных» (Приложение 1).

4.3 В рамках «Матрицы доступа работников, к ресурсам информационной системы персональных данных» определены следующие типы доступа субъектов доступа к объектам доступа:

- чтение (R) – субъекту доступа разрешено просматривать содержимое объекта доступа;
- запись (W) – субъекту доступа разрешено просматривать, записывать и создавать новый объект доступа;
- выполнение (E) - субъекту доступа разрешено запускать/выполнять объект доступа;
- печать (P) – субъекту доступа разрешена печать;
- сканирование (S) - субъекту доступа разрешено сканирование;
- полный (F) - субъект доступа имеет полный доступ к объектам доступа.

5. Правила разграничения доступа

5.1 В информационных системах персональных данных правила разграничения доступа субъектов к объектам доступа должны быть реализованы совокупностью правил, регламентирующих:

- разделение обязанностей и назначение минимально необходимых прав пользователям, администратору информационной системы персональных данных и ответственному за защиту информации;
- управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей;
- управление информационными потоками между устройствами, сегментами информационной системы персональных данных, а также между информационными системами персональных данных;
- ограничение неуспешных попыток входа в информационную систему персональных данных (доступа к информационной системе персональных данных);
- разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;
- контроль использования в информационной системе персональных данных технологий беспроводного доступа;
- контроль использования в информационной системе персональных данных съемных машинных носителей персональных данных.

5.2 Права и обязанности пользователей информационной системы персональных данных зафиксированы в «Инструкции пользователя по работе в информационных системах персональных данных Федерального государственного бюджетного научного учреждения «Федеральный исследовательский центр Институт прикладной физики Российской академии наук»».

5.3 Права и обязанности администратора информационной системы персональных данных зафиксированы в «Инструкции администратора информационных систем персональных данных Федерального государственного бюджетного научного учреждения «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук»».

5.4 Права и обязанности ответственному за защиту информации зафиксированы в «Инструкции ответственного за защиту информации в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук»»

5.5 Управление (заведение, активацию, блокирование и уничтожение) учетными записями пользователей в информационной системе, осуществляет администратор информационной системы персональных данных.

5.6 В информационных системах персональных данных может быть заведена временная учетная запись 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 персональных данных).

5.7 В информационных системах персональных данных осуществляется автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования.

5.8 Администратор информационной системы персональных данных ведет учет пользователей в "Журнале учета пользователей" (Приложение 2).

5.9 При передаче информации между устройствами, сегментами в рамках информационной системы персональных данных, осуществляется управление информационными потоками, включающее:

- фильтрацию информационных потоков в соответствии с правилами управления потоками;
- разрешение передачи информации в информационной системе только по установленному маршруту;
- изменение (перенаправление) маршрута передачи информации только в установленных случаях;
- запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи в установленных случаях.

5.10 Количество неуспешных попыток входа в информационную систему персональных данных (доступа к информационной системе персональных данных) за установленный период времени зафиксировано в «Инструкции по организации парольной защиты в информационных системах персональных данных Федерального государственного бюджетного научного учреждения «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук»»;

5.11 В информационных системах персональных данных обеспечивается блокирование сеанса доступа пользователя по запросу пользователя, а также после установленного времени его бездействия (неактивности) в информационной системе персональных данных. Параметры блокировки сеанса пользователя зафиксированы в «Инструкции по организации парольной защиты в информационных системах персональных данных Федерального государственного бюджетного научного учреждения «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук»

5.12 Администратору информационной системы персональных данных и ответственному за защиту информации разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования информационной системы персональных данных в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

5.13 В информационной системе персональных данных исключено использование технологий беспроводного доступа.

5.14 Регламентация и контроль использования съемных машинных носителей персональных данных, описаны в «Порядке обращения со съемными машинными носителями персональных данных в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук».

Приложение 1
к Положению о разрешительной системе доступа в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук»

Матрица доступа к ресурсам информационной системы персональных данных

Субъект доступа	Объект доступа							
	Основные конфигурационные файлы операционной системы	Средства настройки и управления операционной системой	Основные конфигурационные файлы средств защиты информации	Средства настройки и управления средств защиты информации	Прикладное программное обеспечение	Периферийные устройства	Съемные машинные носители информации	Обрабатываемые, хранимые данные
Администратор информационной системы	F	F	-	-	F	P/S	-	-
Ответственный за защиту информации	F	F	F	F	F	P/S	F	F
Пользователь	R-E	-	-	-	R-E	P/S	F	F

Типы доступа:
- чтение (R) – субъекту доступа разрешено просматривать содержимое объекта доступа;
- запись (W) – субъекту доступа разрешено просматривать, записывать и создавать новый объект доступа;
- выполнение (E) - субъекту доступа разрешено запускать/выполнять объект доступа;
- печать (P) – субъекту доступа разрешена печать;
- сканирование (S) - субъекту доступа разрешено сканирование;
- полный (F) - субъект доступа имеет полный доступ к объектам доступа.

к Положению о разрешительной системе доступа в Федеральном государственном бюджетном научном учреждении «Федеральный исследовательский центр Институт прикладной физики им. А.В. Гапонова-Грехова Российской академии наук»

Журнал учета пользователей

Начат: "___" _____ 20__г.

Окончен: "___" _____ 20__г.

На _____ листах

Инв. № _____

№ п/п	Фамилия имя отчество	Должность	Имя компьютера (или домен)/ учетная запись	Типовая роль	Создан/ Удален	Дата создания/ удаления	Подпись администратора
1	2	3	4	5	6	7	8