**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КУРСКОЙ ОБЛАСТИ**

**ОБЛАСТНОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «КУРСКИЙ АВТОТЕХНИЧЕСКИЙ КОЛЛЕДЖ» (ОБПОУ «КАТК»)**

# ПРИКАЗ

«17» 06 2025 г. № 1-359

## О разрешительной системе доступа

Во исполнение требований Федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных», приказа ФСТЭК России №21 от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»,

ПРИКАЗЫВАЮ:

1. С даты подписания настоящего Приказа утвердить и ввести в действие:

- Положение о разрешительной системе доступа в информационных системах персональных данных ОБПОУ «КАТК» (далее – Положение, Приложение 1 к настоящему Приказу).
- Матрицу доступа работников к ресурсам информационных систем персональных данных ОБПОУ «КАТК» (Приложение 2 к настоящему Приказу).

2. Администратору информационной системы персональных данных ОБПОУ «КАТК» своевременно осуществлять подготовку предложений по внесению изменений в Матрицу доступа работников к ресурсам информационных систем персональных данных ОБПОУ «КАТК».

3. Заместителю директора по ИТ Матвееву А.И. довести настоящий Приказ и Положение до работников, осуществляющих обработку и защиту персональных данных в информационных системах ОБПОУ «КАТК».

4. Ответственность за исполнение настоящего Приказа возложить на лиц, указанных в настоящем Приказе в части, их касающейся.

5. Контроль за исполнением настоящего Приказа возложить на Заместителя директора по ИТ Матвеева А.И.

Директор А.В. Салтанов

Приложение 1
к приказу ОБПОУ «КАТК»
от «17» 06 2025 г. №1-353

# ПОЛОЖЕНИЕ
## о разрешительной системе доступа в информационных системах персональных данных ОБПОУ «КАТК»

### 1. Термины и определения

1.1. 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.

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

1.3. Матрица доступа – таблица, отображающая правила разграничения доступа.

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

1.5. Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

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

1.7. Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

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

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

### 2. Общие положения

2.1. Настоящее Положение о разрешительной системе доступа в информационных системах персональных данных ОБПОУ «КАТК» (далее – Положение), разработано в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативно-методическими документами федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).

2.2. Настоящее Положение определяет методы управления доступом, типы доступа и правила разграничения доступа субъектов доступа к объектам доступа в ИСПДн.

2.3. Положение обязательно для исполнения всеми работниками ОБПОУ «КАТК» (далее – Учреждение), непосредственно осуществляющими обработку и защиту ПДн.

### 3. Субъекты и объекты доступа

3.1. К субъектам доступа ИСПДн, относятся работники, выполняющие свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств ИСПДн в соответствии с должностными инструкциями и которым в ИСПДн присвоены учетные записи.

3.2. К объектам доступа в ИСПДн, относятся:

- средства вычислительной техники;
- средства связи и передачи данных;
- средства обеспечения бесперебойной работы средств вычислительной техники и средств связи и передачи данных;
- основные конфигурационные файлы операционных систем, средств связи и передачи данных и средств защиты информации (далее – СЗИ);
- средства настройки и управления операционной системой, средств связи и передачи данных и СЗИ;
- прикладное программное обеспечение;
- периферийные устройства;
- машинные носители информации;
- обрабатываемые, хранимые данные.

## 4. Методы разграничения доступа

4.1. Методы разграничения доступа к ИСПДн реализуются в соответствии с особенностями функционирования ИСПДн и включают комбинацию следующих методов:

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

4.2. Реализация ролевого метода управления доступом в ИСПДн представлена в таблице 1.

Таблица 1

| № п/п | Роль субъекта доступа | Уровень доступа к объектам доступа |
|---|---|---|
| 1 | Администратор безопасности | - обладает полной информацией о конфигурации системы защиты ПДн (структуре системы защиты ПДн, составе, местах установки и параметров настройки СЗИ);<br>- обладает полной информацией о конфигурации ИСПДн (структуре ИСПДн, состава, мест установки и параметров программного обеспечения и технических средств);<br>- обладает правами настройки и конфигурирования СЗИ;<br>- обладает правами настройки и конфигурирования средств связи передачи данных;<br>- обладает правами настройки и конфигурирования операционных систем и прикладного программного обеспечения;<br>- обладает правами внесения изменений в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения. |
| 2 | Пользователь | - обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к ИСПДн. |

4.3. Реализация дискреционного метода управления доступом достигается путем назначения прав доступа для каждой пары «Роль субъекта доступа» – «Объект доступа» явного и недвусмысленного перечисления допустимых типов доступа в соответствии с Матрицей доступа работников к ресурсам информационных систем персональных данных (далее – Матрица доступа), форма которой установлена в Приложении к настоящему Положению.

## 5. Типы доступа

5.1. В ИСПДн 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.

5.2. Разрешенные к выполнению, субъектами доступа при доступе к объектам доступа в ИСПДн, типы доступа, определены в Матрице доступа.

## 6. Правила разграничения доступа

6.1. В ИСПДн правила разграничения доступа реализованы совокупностью правил, регламентирующих порядок и условия доступа субъекта к объектам доступа в ИСПДн:

- разделение обязанностей и назначение минимально необходимых прав пользователям и администраторам;
- управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей ИСПДн;
- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками в ИСПДн;
- ограничение неуспешных попыток доступа в ИСПДн;
- разрешение (запрет) действий пользователей ИСПДн, разрешенных до идентификации и аутентификации;
- реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;
- контроль использования в ИСПДн технологий беспроводного доступа;
- контроль использования в ИСПДн мобильных технических средств;
- управление взаимодействием с ИСПДн организаций (внешние информационные системы).

6.2. Права и обязанности пользователей зафиксированы в «Инструкции пользователя информационных систем персональных данных ОБПОУ «КАТК».

6.3. Права и обязанности администратора зафиксированы в «Инструкции администратора информационных систем персональных данных ОБПОУ «КАТК».

6.4. Права и обязанности администратора безопасности зафиксированы в «Инструкции ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных ОБПОУ «КАТК».

6.5. Управление (заведение, активацию, блокирование и уничтожение) учетными записями пользователей ИСПДн, осуществляет администратор ИСПДн.

6.6. Администратор ИСПДн определяет и назначает права доступа субъектов к объектам доступа в ИСПДн в соответствии с исполняемой ролью субъекта в ИСПДн и Матрицей доступа.

6.7. В ИСПДн реализованы следующие функции управления учетными записями пользователей ИСПДн:

- определение типа учетной записи (пользователь, администратор, системная);

- объединение учетных записей в группы (пользователи, администраторы);
- верификация пользователя при заведении учетной записи пользователя;
- заведение, активация, блокирование и уничтожение учетных записей пользователей ИСПДн;
- пересмотр и корректировка учетных записей пользователей ИСПДн;
- порядок заведения и контроля использования временных учетных записей Пользователей ИСПДн;
- оповещение администратора ИСПДн, осуществляющего управление учетными записями пользователей ИСПДн, об изменении сведений о пользователях ИСПДн, их ролях, обязанностях, полномочиях, ограничениях;
- уничтожение временных учетных записей пользователей ИСПДн, предоставленных для однократного (ограниченного по времени) выполнения задач в ИСПДн;
- предоставление пользователям ИСПДн прав доступа к объектам доступа ИСПДн, основываясь на задачах, решаемых пользователями ИСПДн.

6.8. При передаче информации между устройствами, сегментами в рамках ИСПДн, осуществляется управление информационными потоками, включающее:

- фильтрацию информационных потоков в соответствии с правилами управления потоками;
- разрешение передачи информации в ИСПДн 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.

6.9. Управление информационными потоками обеспечивает разрешенный маршрут прохождения информации между пользователями ИСПДн, устройствами, сегментами в рамках ИСПДн, а также при взаимодействии с сетью Интернет (или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными потоками, включающих контроль конфигурации ИСПДн, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации).

6.10. Управление информационными потоками блокирует передачу защищаемой информации через сеть Интернет (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, не санкционированно исходящие из ИСПДн и (или) входящие в ИСПДн.

6.11. В ИСПДн установлено и зафиксировано в «Инструкции по парольной защите информации в ОБПОУ «КАТК»:

- количество неуспешных попыток входа (доступа) ИСПДн за установленный период времени;
- блокирование сеанса доступа пользователя ИСПДн после установленного времени его бездействия (неактивности).

6.12. В ИСПДн обеспечивается блокирование сеанса доступа пользователя ИСПДн по запросу.

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

6.14. Администратору ИСПДн и ответственному за обеспечение безопасности ПДн в ИСПДн разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования ИСПДн в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

6.15. Регламентация и контроль использования съемных машинных носителей ПДн, описаны в «Порядке обращения со съемными машинными носителями персональных данных в ОБПОУ «КАТК».

6.16. В ИСПДн при взаимодействии с внешними информационными системами, взаимодействие с которыми необходимо для функционирования ИСПДн, предоставление доступа к ИСПДн осуществляется только авторизованным (уполномоченным) пользователям ИСПДн в соответствии с Матрицей доступа.

## 7. Ответственность

7.1. Все работники Учреждения, осуществляющие обработку и защиту ПДн обязаны ознакомиться с данным Положением под подпись.

7.2. Работники Учреждения несут персональную ответственность за выполнение требований настоящего Положения.

7.3. Контроль выполнения работниками Учреждения правил разграничения доступа в ИСПДн осуществляется Ответственным за обеспечение безопасности ПДн в ИСПДн.

## 8. Срок действия и порядок внесения изменений

8.1. Настоящее Положение вступает в силу с момента его утверждения и действует бессрочно.

8.2. Настоящее Положение подлежит пересмотру не реже одного раза в три года.

8.3. Изменения и дополнения в настоящее Положение вносятся приказом Директора Учреждения.

Приложение
к Положению о разрешительной системе
доступа в информационных системах
персональных данных ОБПОУ «КАТК»

# ФОРМА

## Матрица доступа работников к ресурсам информационных систем персональных данных ОБПОУ «КАТК»

| 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 | Настройки BIOS / UEFI |
| Администратор безопасности | | | | | | | | | |
| Пользователь | | | | | | | | | |

**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.

Приложение 2
к приказу ОБПОУ «КАТК»
от «17» 06 2025 г. №1-359

# Матрица доступа
## субъектов к ресурсам информационных систем персональных данных
## ОБПОУ «КАТК»

| 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 | Настройки BIOS / UEFI |
| Администратор безопасности | F | F | F | F | F | P/S | F | 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.