бюджетное учреждение профессионального образования Ханты-Мансийского автономного округа - Югры «Няганский технологический колледж»
(БУ «Няганский технологический колледж»)

П Р И К А З

«12» 09 2017 г. № 290

Нягань

О разрешительной системе доступа

Во исполнение Федерального закона Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона №152-ФЗ от 27.07.2006 г. «О персональных данных» и прочих нормативных документов по защите информации,

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемое Положение о разрешительной системе доступа в информационных системах персональных данных БУ «Няганский технологический колледж» (далее - Положение).
2. Требования прилагаемого Положения довести до работников, непосредственно осуществляющих защиту персональных данных.
3. Контроль за исполнением приказа оставляю за собой.

И.о. директора О. В. Перминова

Приложение № 1 к приказу
от «12» 09 2017 г. № 250

ПОЛОЖЕНИЕ
о разрешительной системе доступа в информационных системах персональных данных БУ «Няганский технологический колледж»

Нягань
2017

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 БУ «Няганский технологический колледж», 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 генерального директора и действует бессрочно, до замены его новым Положением.

2.4 Все изменения в Положение вносятся приказом генерального директора.

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

3. Субъекты и объекты доступа

3.1 К субъектам доступа информационных системах персональных данных, относятся работники, 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:

- 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;
- средства настройки и управления операционной системой, средств связи и передачи данных и средств защиты информации;
- прикладное программное обеспечение;
- периферийные устройства;
- машинные носители информации;

- обрабатываемые, хранимые данные.

4. Правила разграничения доступа

4.1 Правила разграничения доступа к информационной системе реализуются в соответствии с особенностями функционирования информационной системы 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 конфигурации системы защиты персональных данных (структуру системы защиты персональных данных, состава, мест установки и параметров настройки средств защиты информации); - обладает полной информацией о конфигурации информационной системы (структуре информационной системы, состава, мест установки и параметров программного обеспечения и технических средств); - обладает правами настройки и конфигурирования средств защиты информации; - обладает правами настройки и конфигурирования средств связи передачи данных; - обладает правами настройки и конфигурирования операционных систем и прикладного программного обеспечения; - обладает правами внесения изменений в программное обеспечение информационной системы на стадии ее разработки, внедрения и сопровождения
2	Ответственный за обеспечение безопасности персональных данных в информационных системах	- обладает полной информацией о конфигурации информационной системы (структуре информационной системы, состава, мест установки и параметров программного обеспечения и технических средств); - обладает правами настройки и конфигурирования средств связи передачи данных; - обладает правами настройки и конфигурирования операционных систем и прикладного программного обеспечения; - обладает правами внесения изменений в программное обеспечение информационной системы на стадии ее разработки, внедрения и сопровождения
3	Пользователь	- обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к обрабатываемой информации.

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 (Приложение 1).

4.4 Администратор информационной системы определяет и назначает права доступа работников к объектам доступа информационной системы в соответствии с исполняемой ролью работника в информационной системе и Матрицей доступа.

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

4.6 В информационной системе исключено использование технологий беспроводного доступа.

5. Контроль выполнения правил разграничения доступа

5.1 Контроль выполнения работниками правил разграничения доступа в информационной системе осуществляется ответственным за обеспечение безопасности персональных данных в информационных системах.

Приложение 1
к Положению о разрешительной системе доступа
в БУ «Няганский технологический колледж»

Матрица доступа работников, к ресурсам информационных систем персональных данных БУ «Няганский технологический колледж»

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 обеспечение безопасности персональных данных в информационных системах	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.