Министерство образования и молодежной политики Свердловской области

государственное автономное профессиональное образовательное учреждение
Свердловской области
«Уральский горнозаводской колледж имени Демидовых»

Рассмотрено
на заседании Совета
автономного учреждения
№ протокола 5
«03» 07 2020 г.

Введено в действие приказом
№ 144/2 от «03» 04 2020г.

ПОЛОЖЕНИЕ

О РАЗРЕШИТЕЛЬНОЙ СИСТЕМЕ ДОСТУПА К РЕСУРСАМ АБОНЕТСКОГО ПУНКТА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ «ФЕДЕРАЛЬНАЯ ИНФОРМАЦИОННАЯ СИСТЕМА ОБЕСПЕЧЕНИЯ ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ»

В ГАПОУ СО «УрГЗК»

Невьянск 2020

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.

- **Общие положения**
- Настоящее Положение о разрешительной системе доступа (далее - Положение) к ресурсам абонентского пункта автоматизированной системы "Федеральная информационная система обеспечения проведения

государственной итоговой аттестации" (далее - Информационная система), 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.»

- Настоящее Положение определяет методы управления доступом, типы доступа и правила разграничения доступа субъектов доступа к объектам доступа.
- Настоящее Положение вступает в силу с момента его утверждения директором ГАПОУ СО «УрГЗК» и действует бессрочно, до замены его новым Положением.
- Все изменения в Положение вносятся приказом директора ГАПОУ СО «УрГЗК».
- Положение обязательно для исполнения всеми работниками государственного автономного профессионального образовательного учреждения Свердловской области «Уральский горнозаводской колледж имени Демидовых» (далее - Организация), непосредственно осуществляющими защиту персональных данных.
- **Субъекты и объекты доступа**
- К субъектам доступа в информационной системе, относятся работники оператора, выполняющие свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств информационной системы в соответствии с должностными инструкциями и которым в информационной системе присвоены учетные записи.
- К объектам доступа в информационной системе, 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; обрабатываемые, хранимые данные.

- **Методы управления доступом**
- Методы управления доступом реализованы в соответствии с особенностями функционирования информационной системы и с учетом угроз безопасности информации и включают комбинацию следующих методов:

ролевой метод управления доступом; дискреционный метод управления доступом.

- Реализация ролевого метода управления доступом в информационной системе представлена в таблице 1.

Таблица 1

№ п/п	Роль субъекта доступа	Уровень доступа к объектам доступа
1	Администратор информационной системы	• обладает полной информацией о системном и прикладном программном обеспечении информационной системы; • обладает полной информацией о технических средствах и конфигурации информационной системы; • обладает правами конфигурирования и административной настройки технических средств информационной системы; • обладает правами внесения изменений в программное обеспечение информационной системы на стадии ее

		разработки, внедрения и сопровождения.
2	Ответственный за защиту информации	• обладает правами администратора информационной системы; • обладает полной информацией об используемых в информационной системе средствах защиты; • обладает правами конфигурирования средств Защиты используемых в информационной системе.
3	Пользователь	- обладает всеми необходимыми атрибутами и правами обеспечивающими доступ к обрабатываемой информации.

• Дискреционный метод управления доступом в информационной системе реализован с помощью "Матрицы доступа работников, к ресурсам абонентского пункта автоматизированной системы " Федеральная информационная система обеспечения проведения государственной итоговой аттестации " (Приложение 1).

• **Типы доступа**

• В информационной системе определены следующие типы доступа субъектов доступа к объектам доступа:

чтение (К.) - субъекту доступа разрешено просматривать содержимое объекта доступа; запись (\У) - субъекту доступа разрешено просматривать, записывать и создавать

новый объект доступа;

выполнение (Е) - субъекту доступа разрешено запускать/выполнять объект доступа; печать (Р) - субъекту доступа разрешена печать; полный (Р) - субъект доступа имеет полный доступ к объектам доступа.

- Разрешенные к выполнению, субъектами доступа при доступе к объектам доступа в информационной системе, типы доступа, определены в "Матрице доступа работников, к ресурсам абонентского пункта автоматизированной системы "Федеральная информационная система обеспечения проведения государственной итоговой аттестации".
- **Правила разграничения доступа**
- В информационной системе правила разграничения доступа реализованы совокупностью правил, регламентирующих порядок и условия доступа субъекта к объектам информационной системы:

разделение обязанностей и назначение минимально необходимых прав пользователям, администратору информационной системы и лицу, обеспечивающему функционирование системы защиты информационной системы;

управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей;

управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами;

ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);

разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;

реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;

контроль использования в информационной системе технологий беспроводного доступа;

контроль использования в информационной системе мобильных технических средств; управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).

- Разделение обязанностей и назначение минимально необходимых прав пользователям, администратору информационной системы и лицу, обеспечивающему функционирование системы защиты информационной системы.
- В информационной системе реализовано разделение обязанностей и назначение минимально необходимых прав пользователям, администратору информационной системы и лицу, обеспечивающему функционирование системы защиты информационной системы, в соответствии с их должностными функциями.
- Права и обязанности пользователей информационной системы зафиксированы в "Инструкции пользователя абонентского пункта автоматизированной системы "Федеральная информационная система обеспечения проведения государственной итоговой аттестации".
- Права и обязанности администратора информационной системы зафиксированы в "Инструкции администратора абонентского пункта автоматизированной системы "Федеральная информационная система обеспечения проведения государственной итоговой аттестации".
- Права и обязанности лица, обеспечивающего функционирование системы защиты информационной системы зафиксированы в "Инструкции ответственного за защиту информации в абонентском пункте автоматизированной системы "Федеральная информационная система обеспечения проведения государственной итоговой аттестации".
- Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей.
- Управление (заведение, активацию, блокирование и уничтожение) учетными записями пользователей в информационной системе, осуществляет администратор информационной системы.

• В информационной системе реализованы следующие функции управления учетными записями пользователей:

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;

пересмотр и корректировка учетных записей пользователей;

порядок заведения и контроля использования временных учетных записей пользователей;

оповещение администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;

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

предоставление пользователям прав доступа к объектам доступа информационной системы, основываясь на задачах, решаемых пользователями в информационной системе и взаимодействующими с ней информационными системами.

• 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).

• В информационной системе осуществляется автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования.

• Администратор информационной системы ведет учет пользователей в "Журнале учета пользователей абонентского пункта автоматизированной системы "Федеральная информационная система

обеспечения проведения государственной итоговой аттестации" (Приложение 2).

- Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами.
- При передаче информации между устройствами, сегментами в рамках информационной системы, 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.

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

• Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе).

• В информационной системе установлено и зафиксировано в "Инструкции по организации парольной защиты в абонентском пункте автоматизированной системы " Федеральная информационная система обеспечения проведения государственной итоговой аттестации": количество неуспешных попыток входа в информационную систему (доступа к

информационной системе) за установленный период времени; блокирование сеанса доступа пользователя после установленного времени его

бездействия (неактивности) в информационной системе.

• В информационной системе обеспечивается блокирование сеанса доступа пользователя по запросу пользователя.

• Блокирование сеанса доступа пользователя в информационную систему обеспечивает временное приостановление работы пользователя со средством вычислительной техники, с которого осуществляется доступ к информационной системе (без выхода из информационной системы).

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

• Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации.

• Администратору информационной системы и ответственный за защиту информации в информационной системе 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).

- Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети.
- В информационной системе исключен удаленный доступ субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети.
- Контроль использования в информационной системе технологий беспроводного доступа.
- В информационной системе исключено использование технологий беспроводного доступа.
- Контроль использования в информационной системе мобильных технических средств.
- В информационной системе в качестве мобильных технических средств рассматриваются съемные машинные носители информации (флэш- накопители, внешние накопители на жестких дисках и иные устройства).
- Регламентация и контроль использования съемных машинных носителей информации, описаны в "Порядке обращения со съемными машинными носителями персональных данных в абонентском пункте автоматизированной системы "Федеральная информационная система обеспечения проведения государственной итоговой аттестации".
- Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).
- В информационной системе при взаимодействии с внешними информационными системами, взаимодействие с которыми необходимо для функционирования информационной системы, предоставление доступа к информационной системе осуществляется только авторизованным (уполномоченным) пользователям в соответствии с

"Матрицей доступа работников, к ресурсам абонентского пункта автоматизированной системы " Федеральная информационная система обеспечения проведения государственной итоговой аттестации".

Матрица доступа к ресурсам абонентского пункта автоматизированной системы "Федеральная информационная система обеспечения проведения государственной итоговой аттестации"

Субъект доступа	Объект доступа						
	Основные конфигурационные файлы операционной системы	Средства настройки и управления операционной системой	Основные ко нфигу рационные файлы средств защиты информации	Средства настройки и управления средств защиты информации	Прикладное программное обеспечение	Периферийные устройства	Обрабатываем ые, хранимые данные 1.»
Администратор информационной системы							
Ответственный за защиту информации							
Пользователь							

Типы доступа:

• чтение (К.) - субъекту доступа разрешено просматривать содержимое объекта доступа;

• запись (\У) - субъекту доступа разрешено просматривать, записывать и создавать новый объект доступа;

• выполнение (Е) - субъекту доступа разрешено запускать/выполнять объект доступа;

• печать (Р) - субъекту доступа разрешена печать;

• полный (Р) - субъект доступа имеет полный доступ к объектам доступа.

Журнал учета пользователей абонентского пункта автоматизированной системы "Федеральная информационная система обеспечения проведения государственной итоговой аттестации"

№ 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