САНКТ-ПЕТЕРБУРГСКОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ ИНСТИТУТ ПСИХОЛОГИИ И СОЦИАЛЬНОЙ РАБОТЫ»
(СПбГИПСР)

ПРИНЯТО	УТВЕРЖДЕНО
Ученым советом СПбГИПСР	приказом ректора СПбГИПСР
(протокол от 22.02.2022 № 07)	от 22.02.2022 № 046

Положение

о разрешительной системе доступа к ресурсам абонентского пункта информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации» в институте

1. Общие положения

1.1. Положение о разрешительной системе доступа к ресурсам абонентского пункта информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации» в институте (далее – Положение) разработано в соответствии с законодательством Российской Федерации об информации ограниченного доступа (далее – ИОД) и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности ИОД при ее обработке в информационных системах.

1.2. Положение определяет методы управления доступом, типы доступа и правила разграничения доступа субъектов доступа к объектам доступа при работе с информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации» (далее – АП ФИС ГИА) в Санкт-Петербургском государственном институте психологии и социальной работы (далее – институт).

1.3. Основные термины и определения, используемые в Положении:

1.3.1. **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.

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

1.3.3. **Матрица доступа** – таблица, отображающая правила разграничения доступа.

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

1.3.5. **Правила разграничения доступ** – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

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

1.3.7. **Средство защиты информации** – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации. К средствам защиты информации, установленным на электронных вычислительных машинах относятся: антивирусные средства, средства защиты от несанкционированного доступа, криптографические средства и т.д.

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

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

1.4. Положение обязательно для исполнения всеми работниками института, непосредственно осуществляющими обработку и защиту ИОД.

Все работники, осуществляющие обработки и защиту ИОД, обрабатываемую на АП ФИС ГИА, обязаны ознакомиться с данным Положением под роспись.

Работники несут персональную ответственность за выполнение требований настоящего Положения

1.5. Положение подлежит пересмотру не реже одного раза в три года.

2. Субъекты и объекты доступа

2.1. К субъектам доступа на АП ФИС ГИА, относятся работники института, выполняющие свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств АП ФИС ГИА в соответствии с должностными инструкциями и которым на АП ФИС ГИА присвоены учетные записи.

2.2. К объектам доступа на АП ФИС ГИА относятся:

- основные конфигурационные файлы операционной системы (далее – ОС);
- средства настройки и управления ОС;
- основные конфигурационные файлы средств защиты информации (далее – СЗИ);
- средства настройки и управления СЗИ;
- прикладное программное обеспечение;
- периферийные устройства;
- съемные машинные носители ИОД;
- обрабатываемая, хранимая ИОД.

3. Методы управления доступом

3.1. Методы управления доступом реализованы в соответствии с особенностями функционирования АП ФИС ГИА и с учетом угроз безопасности ИОД и включают комбинацию следующих методов:

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

3.2. Реализация ролевого метода управления доступом на АП ФИС ГИА представлена в таблице 1.

Таблица 1

№ п/п	Роль субъекта доступа	Уровень доступа к объектам доступа
1	Администратор ИС	обладает полной информацией о конфигурации АП ФИС ГИА (структура, состав, места установки и параметры программного обеспечения и технических средств); обладает правами настройки и конфигурирования средств связи передачи данных; обладает правами настройки и конфигурирования ОС и прикладного программного обеспечения; обладает правами внесения изменений в программное обеспечение АП ФИС ГИА на стадии разработки, внедрения и сопровождения.
2	Ответственный за защиту информации в ИС	обладает полной информацией о конфигурации системы защиты информационных систем (структура, состав, места установки и параметры настройки СЗИ); обладает полной информацией о конфигурации АП ФИС ГИА (структура, состав, места установки и параметры программного обеспечения и технических средств); обладает правами настройки и конфигурирования СЗИ; обладает правами настройки и конфигурирования средств связи передачи данных; обладает правами настройки и конфигурирования ОС и прикладного программного обеспечения; обладает правами внесения изменений в программное обеспечение АП ФИС ГИА на стадии ее разработки, внедрения и сопровождения.
3	Пользователь АП ФИС ГИА	обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к обрабатываемой ИОД.

3.3. Дискреционный метод управления доступом на АП ФИС ГИА реализован с помощью «Матрицы доступа субъектов абонентского пункта информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации», форма которой приведена в Приложении №1 к Положению.

4. Типы доступа

4.1. На АП ФИС ГИА 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.

4.2. Разрешенные к выполнению, субъектами доступа при доступе к объектам доступа в информационной системе, типы доступа, определены в «Матрице доступа субъектов абонентского пункта информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации».

5. Правила разграничения доступа

5.1. На АП ФИС ГИА правила разграничения доступа реализованы совокупностью правил, регламентирующих порядок и условия доступа субъекта к объектам АП ФИС ГИА:

- разделение обязанностей и назначение минимально необходимых прав пользователям, администратору ИС и лицу, обеспечивающему функционирование системы защиты информации информационных систем (далее – СиЗИ);
- 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 ИС, а также между ИС;
- ограничение неуспешных попыток входа на АП ФИС ГИА (доступа к АП ФИС ГИА);
- 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 на АП ФИС ГИА технологий беспроводного доступа;
- контроль использования на АП ФИС ГИА мобильных технических средств;
- управление взаимодействием с ИС сторонних организаций (внешние информационные системы).

5.2. На АП ФИС ГИА реализовано разделение обязанностей и назначение минимально необходимых прав пользователям, администратору ИС и лицу, обеспечивающему функционирование СиЗИ, в соответствии с их должностными функциями.

5.3. Права и обязанности пользователей АП ФИС ГИА зафиксированы в «Инструкции по эксплуатации абонентского пункта информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации».

5.4. Права и обязанности администратора ИС зафиксированы в «Инструкции администратора информационных систем».

5.5. Права и обязанности лица, обеспечивающего функционирование СиЗИ зафиксированы в «Инструкции ответственного за защиту информации, обрабатываемой в информационных системах».

5.6. Управление (заведение, активацию, блокирование и уничтожение) учетными записями пользователей на АП ФИС ГИА, осуществляет администратор ИС.

5.7. Администратор ИС определяет и назначает права доступа субъектов к объектам доступа АП ФИС ГИА в соответствии с исполняемой ролью субъекта на АП ФИС ГИА и Матрицей доступа.

5.8. На АП ФИС ГИА 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 на АП ФИС ГИА;
- предоставление пользователям прав доступа к объектам доступа АП ФИС ГИА, основываясь на задачах, решаемых пользователями на АП ФИС ГИА и взаимодействующими с ней ИС.

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

5.10. На АП ФИС ГИА осуществляется автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования.

5.11. Администратор ИС ведет учет пользователей в «Журнале учета лиц, имеющих доступ к обработке информации ограниченного доступа на абонентском пункте информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации», форма которого приведена в Приложении №2 к настоящему Положению.

5.12. При передаче информации между устройствами, сегментами в рамках АП ФИС ГИА, осуществляется управление информационными потоками, включающее:

- фильтрацию информационных потоков в соответствии с правилами управления потоками;
- разрешение передачи информации на АП ФИС ГИА 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.

5.13. Управление информационными потоками обеспечивает разрешенный маршрут прохождения информации между пользователями, устройствами, сегментами в рамках АП ФИС ГИА, а также между ИС или при взаимодействии с сетью Интернет (или другими информационнотелекоммуникационными 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).

5.14. 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 информационной системы и (или) входящие в ИС.

5.15. На АП ФИС ГИА установлено и зафиксировано в "Инструкции по эксплуатации абонентского пункта информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации»:

- количество неуспешных попыток входа на АП ФИ ГИА (доступа к АП ФИС ГИА) за установленный период времени;
- блокирование сеанса доступа пользователя после установленного времени его бездействия (неактивности) на АП ФИС ГИА.

5.16. На АП ФИС ГИА обеспечивается блокирование сеанса доступа пользователя по запросу пользователя.

5.17. Блокирование сеанса доступа пользователя на АП ФИС ГИА обеспечивает временное приостановление работы пользователя со средством вычислительной техники, с которого осуществляется доступ к АП ФИС ГИА (без выхода из АП ФИС ГИА).

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

5.19. Администратору ИС и ответственному за защиту информации в ИС разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования АП ФИС ГИА в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

5.20. На АП ФИС ГИА исключен удаленный доступ субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети.

5.21. На АП ФИС ГИА исключено использование технологий беспроводного доступа.

5.22. На АП ФИС ГИА в качестве мобильных технических средств рассматриваются съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства).

5.23. Регламентация и контроль использования съемных машинных носителей ИОД, описаны в «Порядке обращения со съемными машинными носителями информации ограниченного доступа на абонентском пункте информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации».

5.24. На АП ФИС ГИА при взаимодействии с внешними ИС, взаимодействие с которыми необходимо для функционирования АП ФИС ГИА, предоставление доступа к АП ФИС ГИА осуществляется только авторизованным (уполномоченным) пользователям в соответствии с «Матрицей доступа субъектов абонентского пункта информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации».

Приложение №1 к Положению о разрешительной системе доступа к ресурсам абонентского пункта информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации» в институте

Форма матрицы доступа субъектов абонентского пункта информационной 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 конфигурационные файлы средств защиты информации	Средства настройки и управления средств защиты информации	Прикладное программное обеспечение	Периферийные устройства	Съемные машинные носители информации	Обрабатываемые, хранимые данные	Доступ к BIOS (в т.ч. настройкам загрузки ЭВМ)
Администратор ИС									
Ответственный за защиту информации в ИС									
Пользователь АП ФИС ГИА									

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 Положению о разрешительной системе доступа к ресурсам абонентского пункта информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации» в институте

Форма журнала учета лиц, имеющих доступ к обработке информации ограниченного доступа на абонентском пункте информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации»

Начат: "___" _____ 20__г.

Окончен: "___" _____ 20__г.

На _____ листах

Инв. № _____

№ п/п	Ф.И.О.	Должность	Сведения о предоставлении доступа		Сведения о прекращении доступа	
			Дата и подпись допущенного лица	Фамилия И.О., дата и подпись администратора ИС	Дата	Фамилия И.О. и подпись администратора ИС
1	2	3	4	5	6	7

Приложение №3 к Положению о разрешительной системе доступа к ресурсам абонентского пункта информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации» в институте

Матрица доступа субъектов абонентского пункта информационной системы «Федеральная информационная система обеспечения проведения государственной итоговой аттестации» СПб ГАОУ ВО «СПбГИПСР»

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.

Субъект доступа	**Объект доступа**								
	Основные конфигурационные файлы ОС	**Средства настройки и управления ОС**	**Основные конфигурационные файлы СЗИ**	**Средства настройки и управления СЗИ**	**Прикладное ПО**	**Периферийные устройства**	**Съемные машинные носители информации**	**Обрабатываемые, хранимые данные**	**Доступ к BIOS (в т.ч. настройкам загрузки ЭВМ)**
Администратор ИС	F	F	-	-	F	P/S	-	-	F
Ответственный за защиту информации в ИС	F	F	F	F	F	P/S	F	F	F
Пользователи АП ФИС ГИА	R-E	-	-	-	R-E	P/S	F	F	-