МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ им. А. И. ГЕРЦЕНА»

П Р И К А З

03.10.2025 № 01-253/01

Санкт-Петербург

Об утверждении правил доступа сотрудников РГПУ им. А. И. Герцена к персональным данным и защищаемой информации

В целях обеспечения безопасности информации ограниченного доступа от уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении информации ограниченного доступа, обрабатываемой с использованием и/или без использования средств автоматизации,

ПРИКАЗЫВАЮ:

1. Утвердить Правила доступа сотрудников РГПУ им. А. И. Герцена в помещения, в которых размещены информационные системы персональных данных, ведется обработка информации ограниченного доступа, расположены и используются средства криптографической защиты информации (Приложение № 1).

2. Утвердить Правила регистрации событий безопасности в информационных системах РГПУ им. А. И. Герцена (Приложение № 2).

3. Утвердить Правила ограничения программной среды в информационных системах РГПУ им. А. И. Герцена (Приложение № 3).

4. Утвердить Правила защиты периметра информационных систем РГПУ им. А. И. Герцена при их взаимодействии с иными информационными системами и информационно–телекоммуникационными сетями (Приложение № 4).

5. Утвердить Правила идентификации и аутентификации субъектов доступа и объектов доступа в информационных системах РГПУ им. А. И. Герцена (Приложение № 5).

6. Утвердить Перечень программного обеспечения, разрешенного к использованию в информационных системах РГПУ им. А. И. Герцена (Приложение № 6).

7. Утвердить Перечень событий безопасности в информационных системах РГПУ им. А. И. Герцена, подлежащих регистрации (Приложение № 7).

8. Утвердить форму Перечня лиц, имеющих доступ в помещения, в которых размещены и используются средства криптографической защиты информации (технические средства), позволяющие осуществлять обработку информации ограниченного доступа, а также хранятся носители информации (Приложение № 8).

9. Руководителям структурных подразделений ознакомить сотрудников подразделений, работающих с персональными данными и защищаемой информацией, с нормативными актами РГПУ им. А.И. Герцена, указанными в пунктах 1-5 настоящего приказа, под подпись.

10. Контроль за исполнением приказа возложить на проректора по инновационной деятельности и цифровой трансформации Стрельцова А.Н.

Ректор С.В. Тарасов

Приложение № 1 к приказу
от 03.10.2025 № 01/01-253/01

ПРАВИЛА

доступа сотрудников РГПУ им. А. И. Герцена в помещения, в которых размещены информационные системы персональных данных, ведется обработка информации ограниченного доступа, расположены и используются средства криптографической защиты информации

1. Настоящие Правила доступа сотрудников РГПУ им. А. И. Герцена в помещения, в которых размещены информационные системы персональных данных и ведется обработка информации ограниченного доступа, и расположены и используются средства криптографической защиты информации (далее – Правила) разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119

«Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», иными нормативными правовыми актами Российской Федерации, локальными нормативными актами РГПУ им. А. И. Герцена.

2. Настоящие Правила устанавливают требования к доступу в помещения, в которых размещены и используются средства криптографической защиты информации (далее соответственно – помещения, СКЗИ).

3. Правила доступа в помещения установлены, в том числе, в целях обеспечения безопасности информации ограниченного доступа от уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении информации ограниченного доступа, обрабатываемой с использованием и/или без использования средств автоматизации.

4. Размещение информационных систем, в которых обрабатывается информация ограниченного доступа, размещены и используются средства криптографической защиты информации должно осуществляться в пределах контролируемой зоны, границами которой является периметр охраняемой территории зданий РГПУ им. А. И. Герцена, охраняемой части здания или помещения.

5. Для помещений, в которых обрабатывается информация ограниченного доступа и расположены и используются средства криптографической защиты информации организуется режим обеспечения безопасности, при котором обеспечивается сохранность

носителей информации и средств защиты информации, СКЗИ и ключевых документов к ним, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц и просмотра ведущихся там работ.

6. В помещения, в которых размещены и используются средства криптографической защиты информации (технические средства), позволяющие осуществлять обработку информации ограниченного доступа, а также, хранятся носители информации, допускаются только сотрудники РГПУ им. А. И. Герцена, включенные в перечень, утвержденный приказом ректора (уполномоченного ректором проректора).

7. При оборудовании помещений должны выполняться требования к размещению, монтажу, использованию средств криптографической защиты информации, а также другого оборудования, функционирующего с указанными средствами криптографической защиты информации.

8. Нахождение лиц в помещениях работников, не включенных в перечень лиц, имеющих доступ в помещения, возможно только в присутствии уполномоченного сотрудника РГПУ им. А. И. Герцена. Время нахождения в помещениях ограничивается временем решения вопросов, в рамках которого возникла необходимость пребывания в помещении.

9. Сотрудники РГПУ им. А. И. Герцена, допущенные к обработке информации ограниченного доступа, не должны покидать помещение, не убедившись, что доступ посторонних лиц к информации невозможен. Запрещается оставлять материальные носители с информацией без присмотра в незапертом помещении.

10. Перед открытием помещения, работники, имеющие право доступа в помещения, должны произвести внешний осмотр помещения с целью установления целостности двери и замка, открыть дверь, осмотреть помещения, проверить наличие целостности имеющихся печатей (пломб).

11. После окончания рабочего дня дверь каждого помещения, в котором ведется обработка информации ограниченного доступа, закрывается на ключ. Ответственный сдает/получает ключ дежурному сотруднику охраны под подпись в журнале, после чего помещения ставятся под охрану в установленном в РГПУ им. А. И. Герцена порядке.

12. Помещения РГПУ им. А. И. Герцена, в которых ведется обработка информации ограниченного доступа и расположены и используются средства криптографической защиты информации, должны быть оснащены входными дверьми с замками. Кроме того, должно быть обеспечено постоянное закрытие дверей таких помещений на замок и их открытие только для санкционированного прохода, а также опечатывание помещений по окончании рабочего дня или оборудование помещений

соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

13. Помещения должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по Университету.

14. Для предотвращения просмотра извне окна помещений должны быть защищены шторами или жалюзи.

15. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, оборудуются металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в помещения.

16. Внутренний контроль за соблюдением порядка доступа в помещения, проводится в порядке, определенном в плане проведения внутреннего контроля соответствия требованиям по защите. Контроль и управление физическим доступом к информационным системам и средствам криптографической защиты должны предусматривать:

– определение лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены – поддерживание в актуальном состоянии перечня лиц, имеющих доступ в помещения;

– санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены – выдача ключей от помещений строго в соответствии с утвержденным перечнем лиц;

– учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены – выдача ключей от помещений под подпись в соответствующем журнале, проверка раз в месяц данного журнала.

17. При обнаружении повреждений замков или других признаков, указывающих на возможное проникновение посторонних лиц в помещения, в которых ведется обработка информации и расположены и используются средства криптографической защиты информации, эти помещения не вскрываются, составляется акт о случившемся. При этом немедленно ставятся в известность ректор (уполномоченный ректором проректор) и правоохранительные органы. Одновременно принимаются меры по охране места

происшествия и до прибытия работников правоохранительных органов в эти помещения никто не допускается.

18. В нештатных ситуациях, в случае необходимости принятия в рабочее время экстренных мер при срабатывании пожарной и (или) охранной сигнализации, авариях в системах энерго–, водо– и теплоснабжения помещения, иных аналогичных ситуациях, действия работников осуществляются в соответствии с установленными правилами пожарной безопасности и иными правилами обеспечения безопасности жизнедеятельности. При этом по возможности работниками, осуществляющими работу в данном помещении, осуществляется контроль доступа в данные помещения обслуживающего и иного персонала.

19. Ответственность за соблюдение настоящих Правил возлагается на руководителей структурных подразделений и работников, имеющих право доступа в помещения.

20. Общий контроль за соблюдением работниками настоящих Правил возлагается на проректора по инновационной деятельности и цифровой трансформации.

21. В случае нарушения настоящих Правил сотрудники могут быть привлечены к дисциплинарной и/или иной ответственности в соответствии с законодательством Российской Федерации.

Приложение № 2 к приказу
от 03.10.25 № 01-253/01

ПРАВИЛА

регистрации событий безопасности в информационных системах
РГПУ им. А. И. Герцена

1. Общие положения

1.1. Настоящие правила регистрации событий безопасности информационных систем РГПУ им. А. И. Герцена (далее – Правила) регламентируют состав и содержание информации о событиях безопасности, подлежащих регистрации, правила и процедуры сбора, записи, хранения и защиты информации о событиях безопасности в информационной системе федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный педагогический университет им. А. И. Герцена» (далее – ИС).

2. Определение событий безопасности, подлежащих регистрации, и сроков хранения записей журналов

2.1. В ИС подлежат регистрации в текущий момент времени события безопасности, утвержденные «Перечнем событий безопасности информационных систем РГПУ им. А. И. Герцена, подлежащих регистрации».

2.2. Состав и содержание информации о событиях безопасности, подлежащих регистрации, определяются в соответствии с пунктом 3 настоящих Правил.

2.3. Сроки хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в ИС, в течение 3 (трех) месяцев.

3. Определение состава и содержания информации о событиях безопасности, подлежащих регистрации

3.1. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации событий безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события

безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

3.2. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации событий безопасности, приведены в «Перечне событий безопасности информационных систем РГПУ им. А. И. Герцена, подлежащих регистрации».

4. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения

4.1. Процедуры сбора, записи и хранения информации о событиях безопасности в течение установленного времени хранения предусматривают:

– возможность выбора администратором информационной безопасности событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности, определенных в соответствии с «Перечнем событий безопасности информационных систем РГПУ им. А. И. Герцена, подлежащих регистрации»;

– генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с «Перечнем событий безопасности информационных систем РГПУ им. А. И. Герцена, подлежащих регистрации», с составом и содержанием информации, установленными для соответствующего типа события;

– хранение информации о событиях безопасности в течение времени, установленного в соответствии с разделом 2 настоящих Правил.

4.2. Объем памяти для хранения информации о событиях безопасности рассчитывается и выделяется администратором информационной безопасности ИС с учетом типов событий безопасности, подлежащих регистрации в соответствии с «Перечнем событий безопасности информационных систем РГПУ им. А. И. Герцена, подлежащих регистрации», составом и содержанием информации о событиях безопасности, подлежащих регистрации, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

5. Реагирование на сбои при регистрации событий безопасности

5.1. В ИС реагирование на сбои при регистрации событий безопасности (в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти) должно предусматривать:

– предупреждение (сигнализация, индикация) администратора информационной безопасности о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;

– реагирование на сбои при регистрации событий безопасности путем изменения администратором информационной безопасности параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов ИС, запись поверх устаревших хранимых записей событий безопасности.

6. Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них

6.1. Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться администратором информационной безопасности не реже одного раза в неделю для всех событий, подлежащих регистрации в соответствии с «Перечнем событий безопасности информационных систем РГПУ им. А. И. Герцена, подлежащих регистрации», и обеспечивать своевременное выявление признаков инцидентов безопасности в ИС.

6.2. В случае выявления признаков инцидентов безопасности в ИС администратор информационной безопасности осуществляет планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности.

7. Генерирование временных меток и (или) синхронизация системного времени в информационной системе

7.1. В ИС осуществляется генерирование надежных меток времени и синхронизация системного времени.

7.2. Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в ИС достигается посредством применения внутренних системных часов информационной системы или путем синхронизации системного времени.

8. Защита информации о событиях безопасности

8.1. Защита информации о событиях безопасности (записях регистрации (аудита)) в ИС должна обеспечиваться применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в проектной и организационно-распорядительной документации по защите информации, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

8.2. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) предоставляется только администратору информационной безопасности.

Приложение № 3 к приказу
от 03.10.2025 № 01-55/01

ПРАВИЛА

ограничения программной среды в информационных системах РГПУ им. А. И. Герцена

1. Общие положения

1.1. Настоящие правила ограничения программной среды информационных систем РГПУ им. А. И. Герцена (далее – Правила) регламентируют контроль использования в информационной системе федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный педагогический университет им. А. И. Герцена» (далее – ИС) программного обеспечения, разрешенного к использованию, и возможности восстановления программного обеспечения при возникновении внештатных ситуаций.

2. Установка (инсталляция) разрешенного к использованию программного обеспечения и его компонентов

2.1. Установка (инсталляция) в ИС программного обеспечения (вида, типа, класса программного обеспечения) и (или) его компонентов осуществляется с учетом Перечня программного обеспечения, разрешенного к использованию в ИС.

2.2. Установка (инсталляция) в ИС программного обеспечения и (или) его компонентов осуществляется администратором ИС при контроле выполнения требований безопасности информации администратором ИБ.

2.3. Администраторами информационных систем РГПУ им. А. И. Герцена обеспечивается не реже одного раза в три месяца контроль установленного (инсталлированного) в ИС программного обеспечения на предмет соответствия его Перечню программного обеспечения, разрешенного к использованию, а также на предмет отсутствия программного обеспечения, запрещенного в ИС к установке.

2.4. Пересмотр Перечня программного обеспечения, разрешенного к использованию, может осуществляться по заявке пользователя, согласованной с

непосредственным руководителем пользователя и администратором информационной безопасности.

3. Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций

3.1. Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций предусматривает:

– восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения – выполняется администраторами в рамках возложенных на них функций;

– восстановление и проверку работоспособности системы защиты информации, обеспечивающей необходимый уровень защищенности информации, - выполняется администратором информационной безопасности;

– возврат ИС в начальное состояние (до возникновения нештатной ситуации), обеспечивающее их штатное функционирование, или восстановление отдельных функциональных возможностей ИС, позволяющих решать задачи по обработке информации – выполняется администраторами в рамках возложенных на них функций.

3.2. В случае, когда восстановление работоспособности системы защиты информации невозможно, администратором информационной безопасности, должны применяться компенсирующие меры защиты информации.

Приложение № 4 к приказу
от 03.10.2025 № 01-253/01

ПРАВИЛА

защиты периметра информационных систем РГПУ им. А. И. Герцена при их взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями

1. В информационных системах РГПУ им. А. И. Герцена (далее – ИС) осуществляется защита периметра (физических и (или) логических границ) при их взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, предусматривающая:

— управление (контроль) входящими в ИС и исходящими из ИС информационными потоками на физической и (или) логической границе ИС;

— обеспечение взаимодействия ИС с иными информационными системами и сетями только через сетевые интерфейсы, которые обеспечивают управление (контроль) информационными потоками с использованием средств защиты информации (управляемые (контролируемые) сетевые интерфейсы), установленных на физическом и (или) логическом периметре ИС (маршрутизаторов, межсетевых экранов, коммутаторов, прокси-серверов, шлюзов безопасности, средств построения виртуальных частных сетей и иных средств защиты информации).

2. Количество точек доступа в ИС определяется администратором информационной безопасности с учетом функций ИС, при этом количество точек должно быть минимальным и должен обеспечиваться постоянный и всесторонний контроль входящих и исходящих информационных потоков.

3. В ИС для каждого внешнего телекоммуникационного сервиса применяется отдельный физический управляемый (контролируемый) сетевой интерфейс.

4. В ИС для каждого физического управляемого (контролируемого) сетевого интерфейса устанавливаются правила управления информационными потоками.

5. В ИС исключен выход (вход) через управляемые (контролируемые) сетевые интерфейсы информационных потоков по умолчанию (реализация принципа «запрещено все, что не разрешено»).

Приложение № 5 к приказу
от 03.10.2025 № 001-2591

ПРАВИЛА

идентификации и аутентификации субъектов доступа и объектов доступа в информационных системах РГПУ им. А. И. Герцена

1. Общие положения

1.1. Данные правила идентификации и аутентификации субъектов доступа и объектов доступа в информационных системах РГПУ им. А. И. Герцена (далее – Правила) регламентируют порядок и процедуры присвоения субъектам и объектам доступа уникального признака (идентификатора), сравнения предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверки принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности), а также организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационной системе РГПУ им. А. И. Герцена (далее – ИС) и контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

2. Идентификация и аутентификация пользователей, являющихся внутренними пользователями

2.1. При доступе в ИС осуществляется идентификация и аутентификация пользователей, являющихся сотрудниками РГПУ им. А. И. Герцена (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей. К внутренним пользователям относятся должностные лица РГПУ им. А. И. Герцена:

- администратор ИС;
- администратор информационной безопасности (ИБ);
- ответственные сотрудники по работе с ИС, выполняющие свои должностные обязанности (функции) в соответствии с должностными регламентами (инструкциями),

утвержденными в установленном в РГПУ им. А. И. Герцена порядке, и которым в ИС присвоены учетные записи.

В качестве внутренних пользователей дополнительно рассматриваются должностные лица обладателя информации, заказчика, уполномоченного лица и (или) оператора иной информационной системы, а также лица, привлекаемые на договорной основе для обеспечения функционирования ИС (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с организационно-распорядительными документами РГПУ им. А. И. Герцена. Для каждого внутреннего пользователя в ИС должны быть заведены учетные записи.

2.2. Пользователи ИС однозначно идентифицируются и аутентифицируются для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации в соответствии с Правилами доступа сотрудников РГПУ им. А. И. Герцена в помещения, в которых размещены информационные системы персональных данных и ведется обработка информации ограниченного доступа, и расположены и используются средства криптографической защиты информации.

2.3. Аутентификация пользователя в ИС осуществляется с использованием паролей. Также на усмотрение администратора ИБ могут применяться аппаратные средства в случае многофакторной (двухфакторной) аутентификации.

2.4. В ИС обеспечивается возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

3. Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов

3.1. В ИС устанавливаются и реализуются следующие функции управления идентификаторами пользователей и устройств:

- формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;
- присвоение идентификатора пользователю и (или) устройству;
- предотвращение повторного использования идентификатора пользователя и (или) устройства в течение одного года;
- блокирование идентификатора пользователя после 90 (девяноста) дней неиспользования.

3.2. В качестве ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств определен Администратор ИБ, назначаемый в установленном в РГПУ им. А. И. Герцена порядке.

4. Управление средствами аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации

4.1. В ИС устанавливаются и реализуются следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств:

- изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты ИС;
- выдача средств аутентификации пользователям;
- генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации);
- установление характеристик пароля: длина пароля не менее 6 (шести) символов, алфавит пароля не менее 60 (шестидесяти) символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки – 5 (пять) попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации – 10 (десять) минут, смена паролей не более чем через 120 (сто двадцать) дней;
- блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации;
- назначение необходимых характеристик средств аутентификации (в том числе механизма пароля);
- обновление аутентификационной информации (замена средств аутентификации) с периодичностью не более, чем через 120 (сто двадцать) дней;
- защита аутентификационной информации от неправомерных доступа к ней и модифицирования.

4.2. В случае компрометации личного пароля пользователя ИС должны быть немедленно предприняты меры в зависимости от полномочий владельца скомпрометированного пароля:

- Внеплановая смена личного пароля или удаление учетной записи пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу внутри

организации и т.п.) должна производиться Администратором ИБ немедленно после окончания последнего сеанса работы данного пользователя с системой.

– Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации и другие обстоятельства) Администратора ИБ и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС.

4.3. В качестве ответственного за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации устройств определен Администратор ИБ.

5. Защита обратной связи при вводе аутентификационной информации

5.1. В ИС осуществляется защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

5.2. Защита обратной связи «система – субъект доступа» в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками «*», «•» или иными знаками.

6. Ответственность при организации идентификации и аутентификации

6.1. Ответственность за реализацию правил идентификации и аутентификации субъектов доступа и объектов доступа в соответствии с требованиями настоящих Правил возлагается на Администратора ИБ.

6.2. Ответственность за поддержание установленного порядка и соблюдение требований настоящих Правил возлагается на Администратора ИБ и пользователей ИС.

6.3. Периодический контроль за выполнением всех требований настоящих Правил осуществляется постоянно действующей комиссии по классификации информационных систем обработки персональных данных РГПУ им. А. И. Герцена, подлежащих защите.

Приложение № 6 к приказу
от 03.10.2025 № 01-253/01

ПЕРЕЧЕНЬ

программного обеспечения, разрешенного к использованию в информационных системах РГПУ им. А. И. Герцена

№ п/п	Наименование программных средств	Версия	Разработчик
1	1С: Предприятие 8	8.3.24.1548 8.3.27.1644	1С-Софт
2	7-Zip	24.01	Igor Pavlov
3	Adobe Acrobat Reader DC - Russian	2025.001.20672	Adobe Systems Incorporated
4	Google Chrome	140.0.7339.81	Google LLC
5	IdecoAgent	13.0.78.0	ООО «Айдеко»
6	Jinn-Client	1.0.3050.0	Security Code
7	Kaspersky Endpoint Security для Windows	12.9.0.384	АО "Лаборатория Касперского"
8	Microsoft Edge	140.0.3485.54	Корпорация Майкрософт
9	Microsoft Office профессиональный плюс 2016 - ru-ru	16.0.17932.20286	Microsoft Corporation
10	Microsoft OneDrive	25.130.0706.0004	Microsoft Corporation
11	Microsoft Store	22507.1401.7.0	Microsoft Corporation
12	Microsoft Update Health Tools	3.74.0.0	Microsoft Corporation
13	Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148	9.0.30729.4148	Microsoft Corporation
14	Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148	9.0.30729.4148	Microsoft Corporation
15	Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219	10.0.40219	Microsoft Corporation
16	Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219	10.0.40219	Microsoft Corporation
17	Microsoft Visual C++ 2012 Redistributable (x64) - 11.0.61030	11.0.61030.0	Microsoft Corporation
18	Microsoft Visual C++ 2012 Redistributable (x86) - 11.0.61030	11.0.61030.0	Microsoft Corporation
19	Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.40660	12.0.40660.0	Microsoft Corporation
20	ИС ММИС	4.5.74	Лаборатория ММИС
21	Яндекс браузер	25.8.0.1913 corp	ООО «ЯНДЕКС»
22	Chromium Ghost	140.0.7339.80	Chromium-Gost Community
23	Firebird	3.0.11	Firebird Foundation
24	PDF24	10.0.12	geek Software GmbH
25	NAPS	7.1.2	NAPS2 Software

26	КриптоПРО CSP	4.0.9963 5.0	ООО «КРИПТО-ПРО»
27	КриптоАРМ	5.4.1.160	«Цифровые технологии»
28	КриптоПРО PDF	2.0	ООО «КРИПТО-ПРО»
29	Континент TLS-Клиент	2.0	«Код Безопасности»
30	SecretNET	8.10	«Код Безопасности»
31	VIPNET Client	4.5.3.65117	ИнфоТеКС
32	Компас-3D	V23 учебная версия	ООО «АСКОН - Системы проектирования»
33	FileZilla	3.67.0	Tim Kosse
34	Microsoft Outlook	1.2025.828.402	Microsoft Corporation
35	Консультант Плюс	4016.00.12	«КонсультантПлюс»
36	Яндекс.Телемост	2.17.0.6668	ООО «ЯНДЕКС»
37	Сферум	2.21	ООО «Цифровое образование»
38	Рутокен	4.8.7.0	«Актив»
39	VLC media player	3.0.20	VideoLAN
40	OBS Studio	29.1.3	OBS Project

Приложение № 7 к приказу
от 03.10.2025 № 01-253/01

ПЕРЕЧЕНЬ

событий безопасности в информационных системах РГПУ им. А. И. Герцена, подлежащих регистрации

№	События безопасности, подлежащие регистрации	Состав и содержание информации о событиях безопасности
1.	Вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы	Дата и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа
2.	Подключение машинных носителей информации и вывод информации на носители информации	Дата и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации
3.	Запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации	Дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный)
4.	Попытки доступа программных средств к защищаемым объектам доступа	Дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа

№	События безопасности, подлежащие регистрации	Состав и содержание информации о событиях безопасности
		(устройства), спецификацию защищаемого файла (логическое имя, тип)

Лист регистрации изменений

Изм.	Номера пунктов				Всего пунктов в докум.	№ докум.	Вх. № докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					

Приложение № 8 к приказу
от 03.10.2025 № 01-01-253/01

ФОРМА

ПЕРЕЧЕНЬ

лиц, имеющих доступ в помещения, в которых размещены и используются средства криптографической защиты информации (технические средства), позволяющие осуществлять обработку информации ограниченного доступа, а также, хранятся носители информации

№ п/п	ФИО	Должность и подразделение	Номер помещения	Допуск к информации ограниченного доступа (Наименование ИС/без доступа)	Обработка персональных данных без использования средств автоматизации (да/нет)	Примечание
1	...	*Начальник управления...*	*корп. 13, № 235*	*ИС БД Герцена*	*Да*	-
2						
3						
4						

Лист ознакомления

с Порядком доступа сотрудников в помещения, в которых ведется обработка информации ограниченного доступа и расположены средства криптографической защиты информации к Приложению № 1 Приказа «Об утверждении правил доступа сотрудников РГПУ им. А. И. Герцена к персональным данным и защищаемой информации» от 03.10.2025 № 0101-253/01

№ п/п	ФИО	Должность	Дата ознакомления	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				

Лист ознакомления

с Правилами регистрации событий безопасности информационных систем

РГПУ им. А. И. Герцена

к Приложению № 2 Приказа «Об утверждении правил доступа сотрудников

РГПУ им. А. И. Герцена к персональным данным

и защищаемой информации» от _____ № _____

№ п/п	ФИО	Должность	Дата ознакомления	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				

Лист ознакомления

с Правилами ограничения программной среды информационных систем

РГПУ им. А. И. Герцена

к Приложению № 3 Приказа «Об утверждении правил доступа сотрудников

РГПУ им. А. И. Герцена к персональным данным

и защищаемой информации» от 03.11.2015 № 0101-253/01

№ п/п	ФИО	Должность	Дата ознакомления	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				

Лист ознакомления

с Правилами защиты периметра информационных систем

РГПУ им. А. И. Герцена при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями

к Приложению № 4 Приказа «Об утверждении правил доступа сотрудников

РГПУ им. А. И. Герцена к персональным данным

и защищаемой информации» от 03.10.2025 № 0101-253/01

№ п/п	Дата ознакомления	ФИО сотрудника	Подпись сотрудника
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			

Лист ознакомления

с Правилами идентификации и аутентификации субъектов доступа и объектов доступа в информационной системе РГПУ им. А. И. Герцена

к Приложению № 5 Приказа «Об утверждении правил доступа сотрудников РГПУ им. А. И. Герцена к персональным данным и защищаемой информации» от 03.10.2025 № 0101-253/01

№ п/п	ФИО	Должность	Дата ознакомления	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				

Список рассылки Приказа «Об утверждении правил доступа сотрудников РГПУ им. А. И. Герцена к персональным данным и защищаемой информации»:

1. Гусаков Александр Александрович, проректор по безопасности;
2. Кобрина Лариса Михайловна, проректор по образовательной деятельности;
3. Микляева Анастасия Владимировна, проректор по научной работе;
4. Осипов Василий Викторович, проректор по развитию имущественного комплекса и административно-хозяйственной работе;
5. Рыборецкая Татьяна Геннадьевна, проректор по общим вопросам;
6. Соколов Роман Александрович, проректор по воспитательной деятельности и молодежной политике;
7. Стрельцов Александр Николаевич, проректор по инновационной деятельности и цифровой трансформации;
8. Юрик Анна Васильевна, проректор по финансово–экономической деятельности.