

ПРИНЯТО

ученым советом ФГАОУ ВО РНИМУ
им. Н.И. Пирогова Минздрава России
(Пироговский Университет)
протокол от 16.02.2026
№ 6

УТВЕРЖДЕНО

приказом ФГАОУ ВО РНИМУ
им. Н.И. Пирогова Минздрава России
(Пироговский Университет)
от 06.03.2026
№ 267 рук

ПОЛОЖЕНИЕ
о порядке организации и проведения работ
по защите персональных данных

Определения

Безопасность информации, в том числе персональных данных – состояние защищенности информации, в том числе персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации, в том числе персональных данных, при ее обработке в информационных системах.

Блокирование информации, в том числе персональных данных – временное прекращение обработки информации, в том числе персональных данных (за исключением случаев, если обработка необходима для уточнения информации).

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на защищаемую информацию или ресурсы информационной системы.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе.

Информационная система – совокупность содержащихся в базах данных информации, в том числе персональных данных, и обеспечивающих ее обработку информационных технологий и технических средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Конфиденциальность информации, в том числе персональных данных – обязательное для соблюдения оператором или иным получившим доступ к информации (персональным данным) лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Нарушитель безопасности информации, в том числе персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации (персональных данных) при их обработке техническими средствами в информационных системах.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка информации (персональных данных) – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с информацией (персональными данными), включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение информации (персональных данных).

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющие обработку информации (персональных данных), а также определяющие цели обработки информации (персональных данных), состав информации (персональных данных), подлежащих обработке, действия (операции), совершаемые с информацией (персональными данными).

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

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

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства информационной системы – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

Угрозы безопасности информации (персональных данных) – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации (персональным данным), результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации (персональных данных), а также иных несанкционированных действий при их обработке в информационной системе.

Уничтожение информации (персональных данных) – действия, в результате которых невозможно восстановить содержание информации (персональных данных) в информационной системе или в результате которых уничтожаются материальные носители информации (персональных данных).

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Обозначения и сокращения

| | |
|----------------------------------|---|
| Университет, Оператор | – федеральное государственное автономное образовательное учреждение высшего образования «Российский национальный исследовательский медицинский университет имени Н.И. Пирогова» Министерства здравоохранения Российской Федерации, его филиалы и обособленные структурные подразделения |
| ЗИ | – защищаемая информация, в том числе, персональные данные, содержащаяся в базах данных |
| ИС | – информационные системы |
| ПДн | – персональные данные |
| ПО | – программное обеспечение |

1. Общие положения

1.1 Настоящее Положение о порядке организации и проведения работ по защите информации и персональных данных (далее – Положение) определяет порядок получения, хранения, обработки, защиты, комбинирования, передачи, обезличивания и любого другого использования персональных данных, обрабатываемых в ИС в соответствии с законодательством Российской Федерации.

1.2 Настоящее Положение разработано в соответствии с:

- Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Постановление Правительства Российской Федерации от 1 августа 2025 года № 1154 «Об утверждении требований к обезличиванию персональных данных, методов обезличивания персональных данных и Правил обезличивания персональных данных».

2. Получение, обработка и защита персональных данных

2.1 Порядок получения персональных данных.

2.1.1 Все персональные данные следует получать лично у субъекта персональных данных (далее – ПДн). Если персональные данные возможно получить только у третьей стороны, то субъект ПДн должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Оператор должен сообщить субъекту ПДн о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных и последствиях отказа субъекта ПДн дать письменное согласие на их получение.

2.1.2 Оператор вправе обрабатывать персональные данные субъектов ПДн только с их письменного разрешения.

2.1.3 Письменное согласие субъекта ПДн на обработку своих персональных данных должно включать в себя персональные данные, указанные в перечне ПДн, подлежащих защите в ИС.

2.1.4 Работники Оператора имеют право получать только те ПДн, которые необходимы им для выполнения своих служебных обязанностей.

2.1.5 Работники Оператора, получающие персональные данные субъекта ПДн, обязаны соблюдать режим конфиденциальности.

2.2 Порядок обработки персональных данных.

Обработка персональных данных осуществляется в рамках утвержденной Политики Университета в отношении обработки персональных данных.

2.2.1 При определении объема и содержания, обрабатываемых персональных данных, Оператор должен руководствоваться Конституцией Российской Федерации, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и иными федеральными законами в области защиты персональных данных.

2.2.2 При принятии решений, затрагивающих интересы субъекта ПДн, Оператор не имеет права основываться на персональных данных субъекта ПДн, полученных исключительно в результате их автоматизированной обработки или электронно.

2.2.3 Переносные машинные носители информации (оптические диски, Flash-диски и другие переносные устройства хранения), на которые копируется конфиденциальная (защищаемая) информация, должны быть промаркированы в соответствии с Положением о порядке использования, учета, хранения и уничтожения носителей информации и учтены в журнале учета машинных носителей информации.

2.3 Порядок защиты персональных данных.

2.3.1 Защита персональных данных субъекта ПДн от неправомерного их использования или утраты должна быть обеспечена Оператором за счет его средств в порядке, установленном федеральными законами Российской Федерации в области защиты персональных данных.

2.3.2 Оператор обязан при обработке персональных данных субъектов персональных данных принимать необходимые организационные и технические меры для защиты персональных данных от несанкционированного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

2.3.3 Соблюдать порядок получения, учета и хранения персональных данных субъектов ПДн.

2.3.4 Применять технические средства охраны и сигнализации.

2.3.5 Подписать со всеми работниками, связанными с получением, обработкой и защитой персональных данных субъектов ПДн, Обязательство о неразглашении персональных данных.

2.3.6 Привлекать к дисциплинарной ответственности работников, виновных в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта ПДн.

2.3.7 Запретить допуск к персональным данным субъектов ПДн работников Оператора, не включенных в Перечень лиц, допущенных к обработке персональных данных, обрабатываемых в ИС.

2.3.8 Защита доступа к электронным базам данных, содержащим персональные данные субъектов ПДн, должна обеспечиваться путем использования сертифицированных программных и программно-аппаратных средств защиты информации, предотвращающих несанкционированный доступ третьих лиц к персональным данным субъектов ПДн.

2.3.9 Копировать и делать выписки персональных данных субъектов ПДн разрешается исключительно в служебных целях с письменного разрешения руководителя структурного подразделения.

2.3.10 Субъекты ПДн не должны отказываться от прав на сохранение и защиту своих персональных данных.

2.3.11 Оператор, субъекты ПДн и их представители должны совместно вырабатывать меры защиты персональных данных субъектов ПДн.

3. Хранение персональных данных

3.1 Сведения о субъектах ПДн на бумажных носителях должны храниться в специально оборудованных шкафах и сейфах, которые запираются и опечатываются. Ключи от шкафов и сейфов, в которых хранятся сведения о субъектах ПДн, находятся у ответственного за организацию обработки информации и персональных данных.

3.2 Обязанности по хранению сведений о субъектах ПДн, заполнению, хранению и выдаче документов, содержащих персональные данные, в ИС возлагаются на руководителя каждого структурного подразделения Университета, осуществляющего обработку ПДн - ответственного за организацию обработки информации и персональных данных, либо на иного работника структурного подразделения Университета, осуществляющего обработку ПДн и назначенного приказом по представлению руководителя этого подразделения.

3.3 В процессе хранения персональных данных субъектов ПДн необходимо обеспечивать контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

4. Передача персональных данных

4.1 При передаче персональных данных субъекта ПДн Оператор должен соблюдать следующие требования:

4.1.1 Предупреждать лиц, получающих персональные данные субъекта ПДн, о том, что эти данные могут быть использованы только в целях работы с ИС.

4.1.2 Осуществлять передачу персональных данных субъекта ПДн только в целях ведения баз данных ИС согласно действующему законодательству.

4.1.3 При передаче персональных данных субъекта ПДн использовать выделенную WAN (глобальную компьютерную сеть/сеть общего пользования) с применением сертифицированных средств криптографической защиты информации.

4.1.4 Передавать персональные данные субъекта ПДн представителю субъекта ПДн в порядке, установленном федеральными законами Российской Федерации.

5. Обезличивание персональных данных

5.1 При обезличивании персональных данных Оператор должен обеспечить:

5.1.1 Соблюдение Правил обезличивания персональных данных и методов обезличивания персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 августа 2025 г. № 1154 «Об утверждении требований к обезличиванию персональных данных, методов обезличивания персональных данных и Правил обезличивания персональных данных».

5.1.2 Раздельное хранение персональных данных и обезличенных данных.

5.1.3 Принятие мер по обеспечению безопасности обезличенных данных.

5.1.4 Исключение из обезличенных данных информации, доступ к которой

ограничен федеральными законами.

5.1.5 Использование алгоритмов и программ для электронных вычислительных машин для обезличивания персональных данных без потери таких данных и (или) их изменения.

5.1.6 Возможность внесения изменений и дополнений в обезличенные данные, поддержку актуальности обезличенных данных и возможность повторного применения методов обезличивания персональных данных без возможности преобразования обезличенных данных к исходному виду, позволяющему определить их принадлежность конкретному субъекту персональных данных, а также целостность массива обезличенных данных и их соответствие требованию о предоставлении обезличенных данных.

5.2 Обезличивание персональных данных осуществляется в соответствии с Положением об обезличивании персональных данных Университета.

6. Уничтожение персональных данных

6.1 При необходимости уничтожения персональных данных Оператор должен руководствоваться следующими требованиями:

6.1.1 Уничтожение персональных данных в ИС осуществляется комиссией по классификации информационных систем либо иной комиссией, назначенной приказом.

6.1.2 Бумажные носители персональных данных должны уничтожаться при помощи специального оборудования (измельчителя бумаги).

6.1.3 Персональные данные, представленные в электронном виде, должны уничтожаться программным обеспечением, методом, гарантирующим предотвращение восстановления удаленных данных.

6.1.4 После окончания процедуры удаления персональных данных комиссией по проведению мероприятий по защите персональных данных должен быть составлен акт уничтожения персональных данных.

7. Внутренние проверки состояния защищенности

7.1 Проверка состояния защищенности ИС осуществляется комиссией по классификации информационных систем либо иной комиссией, назначенной приказом.

7.2 Проверка состояния защищенности ИС осуществляется с целью определения соответствия нормативных, организационных, практических и технических мероприятий, реализуемых Оператором, требованиям законов и иных нормативных правовых актов Российской Федерации в области информационной безопасности и защиты персональных данных.

7.3 Проверка состояния защищенности ИС включает в себя:

7.3.1 Определение характера циркулирующих персональных данных и установленных в ИС режимов их обработки.

7.3.2 Определение актуальности организационно-распорядительной документации, учитывающей конкретные условия функционирования средств

вычислительной техники различного уровня и назначения (рабочие станции пользователей, серверное и периферийное оборудование, технические средства защиты информации, в том числе средства криптографической защиты информации), порядок работы сотрудников организации при эксплуатации средств вычислительной техники.

7.3.3 Анализ принятых мер (программных, технических, организационных), обеспечивающих защиту средств вычислительной техники, информационной системы и баз данных от несанкционированного доступа, оценка продуктивности организационного процесса защиты информации. Достаточность технических средств обработки и защиты информации, наличие подтверждений соответствия по требованиям информационной безопасности (сертификатов соответствия).

7.3.4 Проведение анализа конфигураций активного сетевого оборудования, маршрутизаторов, коммутаторов, серверов с целью выявления уязвимых мест в системе защиты информации.

7.3.5 Проведение инструментального анализа сетевого и серверного оборудования локально-вычислительных сетей, информационных систем и баз данных с применением программно-аппаратных средств.

7.3.6 Проверка работоспособности используемых программных и программно-аппаратных средств обнаружения и предотвращения компьютерных атак.

7.3.7 Проверка наличия лицензионных средств защиты от вредоносных программ и вирусов или сертифицированных свободно распространяемых антивирусных средств защиты.

7.3.8 Проверка оснащения серверных и кроссовых помещений средствами контроля доступа и пожаротушения, обеспечения температурного режима, наличия регламента доступа к серверным и кроссовым помещениям.

7.3.9 Проверка состояния защищенности информационных ресурсов от сбоев в системе электропитания (система резервирования и автоматического ввода резерва).

7.3.10 Проверка состояния линейно-кабельного оборудования локально-вычислительных сетей (наличие запирающих и опечатывающих устройств, оборудования распределительных шкафов).

7.4 Внутренняя проверка комиссией по классификации информационных систем либо иной комиссией, назначенной приказом, завершается подведением итогов (обобщением) результатов проверки и составлением акта о результате проверки состояния защищенности ИС.

7.5 Акт должен содержать:

7.5.1 Дата, время и место составления акта.

7.5.2 Дата и место проведения проверки.

7.5.3 Сведения о результатах проверки, в том числе о выявленных нарушениях и их характере.

7.5.4 Достоверное и обоснованное изложение состояния защищенности информационной системы и ресурсов, выявленных недостатков и нарушений со ссылками на соответствующие документы и факты, выводы и предложения по их устранению с указанием конкретных сроков.

8. Обязанности субъекта персональных данных и Оператора

8.1 В целях обеспечения достоверности персональных данных субъект ПДн обязан:

8.1.1 Предоставлять полные и достоверные данные о себе.

8.1.2 В случае изменения своих персональных данных сообщать данную информацию Оператору.

8.2 Оператор обязан:

8.2.1 Осуществлять защиту персональных данных субъекта ПДн.

8.2.2 Вести Журнал учета запросов (обращений) субъектов персональных данных в ИС (Приложение).

8.2.3 Обрабатывать запросы запросов (обращения) субъектов персональных данных или их представителей в соответствии с утвержденными Правилами рассмотрения запросов субъектов персональных данных или их представителей в Университете.

8.2.4 Обеспечивать хранение документации, содержащей персональные данные субъектов ПДн, при этом персональные данные не должны храниться дольше, чем это оправдано выполнением задач, для которых они собирались, или дольше, чем это требуется в интересах лиц, о которых собраны данные.

9. Права субъекта ПДн в целях защиты персональных данных

9.1 Субъект персональных данных вправе требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

9.2 Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Оператором способы обработки персональных данных;
- сроки обработки персональных данных, в том числе сроки их хранения;

9.3 Субъект персональных данных имеет право на определение представителей для защиты своих персональных данных.

9.4 Субъект персональных данных имеет право требовать исключить или исправить неверные или неполные персональные данные, а также данные, обрабатываемые с нарушением требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

9.5 Субъект персональных данных имеет право требовать об извещении Оператором всех лиц, которым ранее были сообщены неверные или неполные

персональные данные субъекта ПДн, обо всех произведенных в них исключениях, исправлениях или дополнениях.

9.6 Субъект персональных данных имеет право на обжалование в судебном порядке любых неправомерных действий или бездействия Оператора при обработке и защите его персональных данных.

10. Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъекта ПДн

10.1 Лица, виновные в нарушении требований федеральных законов Российской Федерации, несут предусмотренную законодательством Российской Федерации ответственность.

10.2 Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных федеральными законами, а также нарушения требований к защите персональных данных подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

ПРИЛОЖЕНИЕ
к Положению о порядке организации и проведения работ
по защите персональных данных

ЖУРНАЛ

**учета запросов (обращений) субъектов персональных данных или их
представителей**

| № п/ п | Дата и рег. номер запроса (обраще ния) | Сведения о запрашиваю щем лице (ФИО, паспортные данные, доверенност ь и ФИО субъекта в случае представите ля) | Краткое содержан ие обращени я | Отметка о предостав лении (или отказе в предостав лении) информа ции | Дата и рег. номер ответа на запро с | Подпись запрашиваю щего лица о получении ответа (отметка об отправке письма) | Подпись ответств енного лица |
|--------------|---|--|--|---|---|---|---------------------------------------|
| 1 | | | | | | | |
| 2 | | | | | | | |
| 3 | | | | | | | |
| 4 | | | | | | | |
| 5 | | | | | | | |
| 6 | | | | | | | |
| 7 | | | | | | | |
| 8 | | | | | | | |
| 9 | | | | | | | |
| 10 | | | | | | | |
| 11 | | | | | | | |
| 12 | | | | | | | |
| 13 | | | | | | | |
| 14 | | | | | | | |
| 15 | | | | | | | |
| 16 | | | | | | | |
| 17 | | | | | | | |