МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского»
(ННГУ)

ПРИКАЗ

22.06.2026 № 837-ОД

Нижний Новгород

О допуске к работе лиц,
прошедших обучение

Во исполнение Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и приказа от 18.02.2026 №180-ОД «О назначении ответственных за организацию обработки персональных данных» п р и к а з ы в а ю:

1. Допустить к работе уполномоченных работников, прошедших обучение 16.04.2026 по программе обучения «Правила обработки персональных данных», в обязанности которых входит обработка персональных данных.

2. Утвердить и ввести в действие Инструкцию ответственного за организацию обработки персональных данных, определяющую функциональные обязанности лиц, ответственных за организацию обработки персональных данных в информационных системах ННГУ. (Приложение № 1).

3.Утвердить и ввести в действие Инструкцию пользователя по общему порядку работы в информационных системах персональных данных, определяющую функциональные обязанности лиц, ответственных за обработку персональных данных. (Приложение № 2).

4. Руководителям структурных подразделений при трудоустройстве новых работников либо изменении должностных обязанностей уже работающих в ННГУ, в чьи обязанности входит обработка персональных данных, перед допуском к работе направлять их в управление информационной безопасности для прохождения обучения.

5. Контроль за исполнением приказа возложить на проректора по безопасности Малышева А.Е.

Ректор О.В. Трофимов

ННГУ – 352841

5

Приложение № 2
к приказу
от "22" 06.2026 г. № 837-ОД

Инструкция пользователя по общему порядку работы в информационных системах персональных данных

1. Общие положения

1.1. Настоящая Инструкция пользователю по общему порядку работы в информационных системах персональных данных (далее – Инструкция) определяет основные права и обязанности пользователя информационных систем персональных данных в федеральном государственном автономном образовательном учреждении высшего образования «Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского» (далее - Университет).

1.2. Пользователями информационных систем персональных данных являются работники Университета, допущенные к обработке персональных данных установленным порядком.

1.3. Для каждого пользователя информационных систем персональных данных (далее - ИСПДн) создается уникальная учетная запись для авторизации в сети и в информационной системе. Учетная запись пользователя – это его реквизиты в информационной системе, основными параметрами которой являются имя пользователя и его пароль.

1.4. К самостоятельной работе в информационных системах персональных данных допускаются пользователи, прошедшие обучение правилам обработки персональных данных.

1.5. Методическое руководство работой пользователя информационной системы персональных данных в области обеспечения защиты персональных данных осуществляет ответственный за обеспечение защиты информации в ходе эксплуатации информационной системы персональных данных и администратор безопасности ИСПДн, в части касающейся.

1.6. Инструкция корректируется и дополняется установленным порядком.

2. Должностные обязанности

Все пользователи, допущенные к работе в ИСПДн Университета, обязаны:

2.1. Знать и выполнять требования законодательства РФ, внутренних инструкций, распоряжений, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте только те процедуры обработки персональных данных, которые определены для него должностной инструкцией.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных.

2.4. Использовать для хранения персональных данных только определенные места хранения и учтенные носители персональных данных Университета.

2.5. Не разглашать персональные данные, которые будут доверены или станут известны в ходе рабочего процесса во время выполнения должностных (договорных) обязанностей.

2.6. Не сообщать устно или письменно, не передавать в каком-либо виде третьим лицам и не раскрывать публично персональные данные без соответствующего разрешения непосредственного руководителя.

ННГУ – 352848

2.7. Незамедлительно, в кратчайшие сроки, сообщать непосредственному руководителю об утрате или недостаче носителей информации, ключей от помещений, хранилищ, сейфов, личных печатей и о других фактах, которые могут привести к разглашению персональных данных.

2.8. Незамедлительно сообщать администратору безопасности ИСПДн о замеченных случаях нарушения компьютерной безопасности (несанкционированный доступ к оборудованию и информации, несанкционированное искажение или уничтожение информации).

2.9. При прекращении работ (трудовых отношений) все материальные носители, содержащие персональные данные, передать непосредственному руководителю.

2.10. Использовать информационные ресурсы Университета и переданные в распоряжение технические средства хранения, обработки и передачи информации исключительно для выполнения порученных работ, должностных (договорных) обязанностей.

2.11. Соблюдать требования парольной политики Университета.

2.12. Соблюдать требования антивирусной защиты в ИСПДн данных Университета.

2.13. Обо всех выявленных нарушениях, связанных с порядком обработки персональных данных, а также для получений консультаций по вопросам обработки персональных данных необходимо обращаться к ответственному за обеспечение защиты информации в ходе эксплуатации ИСПДн или администратору безопасности ИСПДн.

2.14. Пользователям запрещается:

– нарушать установленные в Университете правила обработки персональных данных;

– использовать компоненты программного и аппаратного обеспечения Университета в неслужебных целях;

– оставлять свое рабочее место без присмотра, предварительно не заблокировав (штатными средствами операционной системы Windows или Linux – комбинацией клавиш [WIN] + [L] или [CTRL] + [ALT] + [DEL] с дальнейшим нажатием кнопки "Блокировка" появившегося меню, либо при помощи штатных средств защиты информации от несанкционированного доступа при их наличии);

– оставлять без присмотра или неубранными в хранилища (шкаф, сейф) носители или документы, содержащие персональные данные;

– записывать и хранить конфиденциальную информацию (в том числе персональные данные) на неучтенных носителях информации (оптических (CD) дисках, флеш-накопителях и т.п.);

– самовольно изменять состав и конфигурацию используемых программных, аппаратных, программно-аппаратных средств, самовольно устанавливать программное обеспечение, отключать/подключать оборудование (в том числе смартфоны) или изменять режимы его работы;

– самовольно подключать компьютер к локальной вычислительной сети, ИСПДн Университета, изменять IP-адрес, MAC-адрес и иные настройки сети компьютера;

– производить действия, направленные на получение несанкционированного доступа к автоматизированным рабочим местам и серверам, равно как и любым другим узлам сети Интернет, в том числе:

а) действия, направленные на нарушение нормального функционирования элементов сети (компьютеров, другого сетевого оборудования или программного обеспечения);

б) установка программного обеспечения, осуществляющего перехват информации (информационных пакетов), адресованной другим пользователям;

ННГУ – 352848

в) действия, направленные на получение несанкционированного доступа к информационным ресурсам, в последующем использовании такого доступа;

г) уничтожение, модификация программного обеспечения или данных без согласования с непосредственным руководителем или владельцами этого ресурса;

д) попытки подбора паролей к любым информационным ресурсам методом перебора всех возможных вариантов паролей, либо атак по словарю;

е) умышленные действия по созданию, использованию и распространению вредоносных программ, в том числе направленных на получение несанкционированного доступа к любым информационным и служебным ресурсам (как внутри Университета, так и вне), либо на нарушение целостности и работоспособности этих систем;

ж) действия по сканированию локальной сети с целью определения ее внутренней структуры, списков открытых портов, наличия существующих сервисов и уязвимостей;

– самовольно изменять параметры средств защиты информации (в том числе и средств антивирусной защиты), а также завершать их работу и (или) самостоятельно их устанавливать;

– самостоятельно разрабатывать или использовать нерегламентированные (без разрешения непосредственного руководителя) программы (например, игры; IM-клиенты, такие как Google Messenger, Microsoft Messenger, ICQ и т.п.; P2P- клиенты: Kazaa, eMule и т.п.);

– разрешать посторонним лицам работать под своей учетной записью на автоматизированном рабочем месте;

– пересылать конфиденциальную информацию, в том числе персональные данные, по каналам связи в открытом виде, в том числе Интернет, по телефону, факсу, электронной почте и т.п. (без использования средств шифрования или шифрования и электронной подписи);

– получать доступ к сети Интернет любыми способами, кроме как установленными в Университете, например, при помощи несанкционированно установленных на автоматизированные рабочие места модемов и т.п.;

– в случае возникновения любых механических неисправностей в оборудовании осуществлять самостоятельные попытки их устранения;

– препятствовать должностным лицам при проведении проверок и служебных расследований, связанных с обеспечением безопасности информации;

– удалять или искажать программы и файлы с конфиденциальной информацией, в том числе персональных данных, и иной важной информацией (например, системной, необходимой для функционирования информационных систем персональных данных);

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению внештатной ситуации. Об обнаружении такого рода ошибок – ставить в известность руководителя своего подразделения и работников, ответственных за установку и (или) сопровождение программного обеспечения;

– подключать к локальной вычислительной сети, ИСПДн Университета личные средства вычислительной техники: ноутбуки, карманные компьютеры, смартфоны и т.п., а также личные носители и накопители информации. В случае необходимости переноса информации с личных носителей информации обращаться к администратору безопасности ИСПДн.

3. Права

Все пользователи, допущенные к работе в ИСПДн Университета, имеют право:

3.1. Использовать ИСПДн Университета для выполнения служебных обязанностей.

ННГУ – 352848

3.2. Обращаться к ответственному за организацию обработки персональных данных, ответственному за обеспечение защиты информации в ходе эксплуатации ИСПДн, системному администратору, администратору безопасности и администратору ИСПДн для консультаций по поводу использования программного обеспечения и автоматизированного рабочего места, вопросам обработки персональных данных.

3.3. Направлять предложения по установке новых версий существующего программного обеспечения (с обоснованием необходимости замены старых версий на новые).

3.4. Направлять предложения по модернизации программного обеспечения, разрабатываемого в Университете.

3.5. Направлять предложения по установке нового (а также дополнительного) программного обеспечения (с указанием цели использования, преимуществ перед существующими аналогами).

3.6. Направлять предложения по модернизации автоматизированных рабочих мест (замены на новые аналоги), входящих в ИСПДн (с обязательным обоснованием замены и указанием преимуществ перед существующими аналогами).

3.7. Требовать от руководства прекращения работ в рамках ИСПДн при обнаружении обстоятельств, создающих предпосылки утечки информации ограниченного доступа, обрабатываемой в рамках данной ИСПДн.

3.8. Получать консультации и разъяснения по работе с компьютерным оборудованием и программным обеспечением, по вопросам компьютерной безопасности.

4. Ответственность

4.1. Пользователь ИСПДн несет персональную ответственность за свои действия или бездействие, которые повлекут за собой разглашение персональных данных, а также за нарушение нормального функционирования ИСПДн или ее отдельных компонентов, несанкционированный доступ к информации в соответствии с законодательством Российской Федерации и локальными нормативными актами Университета.

ННГУ – 352848