МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«Вологодский государственный университет»

(ВоГУ)

ПРИКАЗ

«27» июля 2022 г. № 02.00-67/0426

г. Вологда

Об утверждении инструкций по работе с персональными данными

В целях обеспечения конфиденциальности при обработке персональных данных и в соответствии с требованиями Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных», приказываю:

1. Утвердить прилагаемые:

1.1. Инструкцию о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные (Приложение № 1).

1.2. Инструкцию пользователя информационной системы персональных данных федерального государственного бюджетного образовательного учреждения высшего образования «Вологодский государственный университет» (Приложение № 2).

2. Управлению информатизации (А.В. Елгаев) разместить настоящий приказ на официальном сайте Университета в сети Интернет.

3. Руководителям структурных подразделений, в которых осуществляется обработка персональных данных, ознакомить работников, осуществляющих обработку персональных данных, с утвержденными инструкциями под роспись и представить листы ознакомления в Управление правового и кадрового обеспечения в срок до 1 сентября 2022 года.

4. Контроль за исполнением приказа возложить на проректора по правовой, кадровой и организационной деятельности В.В. Дементьеву.

Ректор В.В. Приятелев

Приложение № 1

УТВЕРЖДЕНО
приказом ректора
от 27.07.22 №02.00-67/04

ИНСТРУКЦИЯ
о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные

1. Общие положения

1.1. Настоящая Инструкция устанавливает применяемые в федеральном государственном бюджетном образовательном учреждении высшего образования «Вологодский государственный университет» (далее - Университет) меры обеспечения безопасности при обработке персональных данных с целью соблюдения конфиденциальности сведений, содержащих персональные данные работников и обучающихся Университета.

1.2. Настоящая Инструкция разработана на основании Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлений Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" и иных нормативных правовых актов Российской Федерации.

2. Общие правила хранения и передачи персональных данных

2.1. Перечень персональных данных, хранимых и обрабатываемых в Университете, приведен в Положении о порядке обработки персональных данных, утвержденном приказом ректора от 05 мая 2022 года № 02.00-67/0269. Обработка и хранение конфиденциальных данных, не указанных в перечне запрещена.

2.2. Перечень сотрудников Университета, ответственных за хранение и обработку персональных данных, утвержден приказом ректора от 11 мая 2022 года № 02.00-67/0282 «Об утверждении перечня должностей работников по вопросам обработки персональных данных» (далее – Перечень). Обработка и хранение конфиденциальных данных лицами, не указанными в Перечне запрещена.

2.3. Университет предоставляет должностным лицам, обрабатывающим персональные данные, условия необходимые для обеспечения конфиденциальности и безопасности персональных данных.

2.4. Должностные лица Университета, работающие с персональными данными, обязаны использовать информацию о персональных данных исключительно для целей, связанных с выполнением своих трудовых обязанностей.

2.5. Передача персональных данных третьим лицам допускается только в случаях, установленных законодательством Российской Федерации, в соответствии с

настоящей Инструкцией, должностными инструкциями и иными локальными нормативными актами Университета.

2.6. Должностные лица Университета, работающие с персональными данными, обязаны немедленно сообщать своему непосредственному руководителю и администратору информационной безопасности обо всех ставших им известными фактах, либо попытках, получения третьими лицами несанкционированного доступа к персональным данным, об утрате носителей информации и других фактах, которые могут привести к несанкционированному доступу к персональным данным.

2.7. Должностные лица, осуществляющие обработку персональных данных, за невыполнение требований конфиденциальности, защиты персональных данных несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

2.8. Отсутствие контроля со стороны Университета за надлежащим исполнением работником своих обязанностей в области обеспечения конфиденциальности и безопасности персональных данных не освобождает работника от таких обязанностей и предусмотренной законодательством РФ ответственности.

2.9. Запрещается оставлять материальные носители с персональными данными без присмотра в незапертом помещении.

2.10. Сотрудникам, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью или письменным запросом установленного образца.

2.11. После подготовки и передачи документа в соответствии с резолюцией, файлы черновиков и вариантов документа переносятся, подготовившим их сотрудником, на маркированные носители, предназначенные для хранения персональных данных.

2.12. Без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов, записных книжек и др.), содержащих конфиденциальные данные, запрещается.

2.13. Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и настоящей инструкцией.

2.14. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах конфиденциальные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

3. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемой без использования средств автоматизации, в том числе условия хранения персональных данных

3.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных.

3.2. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие

несанкционированный к ним доступ. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

3.3. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

3.4. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы.

3.5. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

3.6. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, исключающие одновременное копирование иных персональных данных, не подлежащих распространению и использованию.

3.7. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

3.7.1. Типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес Оператора, фамилия, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Оператором способов обработки персональных данных.

3.7.2. Типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, при необходимости получения письменного согласия на обработку персональных данных.

3.7.3. Типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.

3.7.4. Типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

3.8. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, то путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем

изготовления нового материального носителя с уточненными персональными данными.

3.9. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

4. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемой с использованием средств автоматизации, в том числе правила доступа, хранения и пересылки персональных данных

4.1. Обработка персональных данных с использованием средств автоматизации означает совершение операций с этими данными с помощью средств вычислительной техники в корпоративной вычислительной сети Университета.

4.2. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

4.3. Технические и программные средства защиты информации должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

4.4. Допуск лиц к обработке персональных данных в информационной системе осуществляется на основании приказа ректора Университета. Работа с персональными данными, осуществляется в соответствии с «Инструкцией пользователя информационной системы персональных данных ВоГУ», с которой работник, в должностные обязанности которого входит обработка персональных данных, знакомится под роспись.

4.5. Размещение средств вычислительной техники в помещениях, организация работы с персональными данными должны обеспечивать сохранность персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

4.6. Доступы к персональным данным для каждого пользователя должны быть защищены индивидуальными паролями доступа. Пароль должен быть не менее 7 символов и состоять из букв в верхнем и нижнем регистре, цифр и специальных символов. Запрещается использовать в качестве пароля своё имя и год своего рождения, последовательный ряд букв или цифр. Работа на компьютерах с персональными данными открытым доступом, или под чужими или общими паролями, запрещен.

4.7. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернета, запрещается.

4.8. При обработке персональных данных в информационных системах пользователи обязаны:

4.8.1. использовать только предназначенные для этого разделы (каталоги) автоматизированных рабочих мест, серверов или учтенные съемные носители;

4.8.2. не допускать применение на технические средства автоматизированной обработки персональных данных физического воздействия, в результате которого может быть нарушено их функционирование;

4.8.3. постоянно использовать антивирусное обеспечение для обнаружения зараженных файлов и незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие электронных вирусов;

4.8.4. не допускать несанкционированный вынос из помещений технических средств автоматизированной обработки персональных данных, подключения внештатного оборудования, а также удаления, инсталляции нового или настройки существующего программного обеспечения.

4.9. При обработке персональных данных в информационной системе разработчики и администраторы системы должны:

4.9.1. проводить обучение пользователей информационных систем, правилам работы со средства защиты информации;

4.9.2. вести учет лиц, допущенных к работе с персональными данными в информационной системе, их прав доступов;

4.9.3. вести учет применяемых средств защиты информации и эксплуатационной и технической документации к ним;

4.9.4. контролировать соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

4.10. Специфические требования по защите персональных данных в отдельных автоматизированных системах устанавливаются инструкциями по их использованию и эксплуатации.

4.11. В случае необходимости, восстановление данных из резервных копий производится в соответствии с документацией на используемое программное обеспечение с составлением акта (приложение № 1 к настоящей инструкции).

4.12. Ответственный за защиту информации и администраторы автоматизированных информационных систем обязаны вести «Журнал выдачи паролей и учёта пользователей», в котором указываются виды конкретных работ и возможности доступа персонально для каждого пользователя, а также отмечать в нем изменения в составе пользователей (приложение № 2 к настоящей Инструкции).

4.13. Новые пользователи назначаются руководителями подразделений через служебную записку на имя администратора автоматизированной информационной системы.

5. Порядок учета, хранения и обращения со съемными носителями персональных данных, твердыми копиями и их утилизации

5.1. Все находящиеся на хранении и обращении съемные носители с персональными данными подлежат учету.

5.2. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

5.3. Учет и выдачу съемных носителей персональных данных осуществляют сотрудники структурных подразделений согласно Порядку учета, хранения и использования съемных электронных носителей конфиденциальной информации, утвержденному приказом ректора от 24.03.2022 № 02.00-67/0178.

5.4. Сотрудники Университета получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок.

5.5. При получении учтенного съемного носителя делается соответствующая запись в журнале учета и движения электронных носителей конфиденциальной информации (далее – журнал учета).

5.6. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

5.7. О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений немедленно ставится в известность руководитель соответствующего структурного подразделения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журнал учета. Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется уполномоченной комиссией. По результатам уничтожения носителей составляется акт (приложение № 2 к Порядку учета, хранения и использования съемных электронных носителей конфиденциальной информации, утвержденному приказом ректора от 24.03.2022 № 02.00-67/0178).

5.8. Нельзя хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам.

5.9. Нельзя выносить съемные носители с персональными данными из служебных помещений.

5.10. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов с ограниченным правом пользования. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

6. Порядок ознакомления с Инструкцией

Работники подразделений Университета и лица, выполняющие работы по договорам и контрактам, имеющие отношение к работе с персональными данными, должны быть в обязательном порядке ознакомлены под роспись с настоящей Инструкцией согласно приложению № 3.

Приложение №1
к Инструкции о порядке обеспечения
конфиденциальности при обращении с информацией,
содержащей персональные данные,
утвержденной приказом ректора
от 27.07.2022 № 02.00-67/0426

АКТ

о восстановлении информационных ресурсов

Мною, _____

(Ф.И.О., должность администратора ресурса)

Дата выявления сбоя: _____

Проведена проверка _____

(вид ИР)

В результате чего выявлено: _____

(указывать вид и причины)

Способ восстановления: _____

Используемая документация: _____

Подпись
администратора АИС

Дата

Приложение №2
к Инструкции о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные, утвержденной приказом ректора
от 27.07.2022 № 02.00-67/0426

ЖУРНАЛ
выдачи паролей и учета пользователей

ФГБОУ ВО «Вологодский государственный университет»
(наименование учреждения)

Начат «___» _____ 20___ г.

Окончен «___» _____ 20___ г.

На _____листах

№ п/п	ФИО	Имя пользователя	Подразделение должность	Дата выдачи пароля	Перечень ресурсов в соответствии с разрешением	Права доступа	Дата регистрации пользователя	Изменение прав доступа	Подпись
1									
2									

Приложение № 3
к Инструкции о порядке обеспечения
конфиденциальности при обращении с информацией,
содержащей персональные данные,
утвержденной приказом ректора
от 27.04.2022 № 02.00-67/0426

ЛИСТ ОЗНАКОМЛЕНИЯ СОТРУДНИКОВ
С Инструкцией о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные

С инструкцией ознакомлен (ы):

№ п/п	Фамилия сотрудника	Дата ознакомления	Роспись в ознакомлении
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			

Приложение № 2

УТВЕРЖДЕНО
приказом ректора
от 27.07.22 №02.00-67/04

ИНСТРУКЦИЯ
пользователя информационной системы персональных данных федерального государственного бюджетного образовательного учреждения высшего образования «Вологодский государственный университет»

1. Общие положения

1.1. Настоящая инструкция определяет основные обязанности сотрудников федерального государственного бюджетного образовательного учреждения высшего образования «Вологодский государственный университет» (далее - университет), осуществляющих автоматизированную обработку персональных данных (ПДн) в информационных системах персональных данных (ИСПДн) университета.

1.2. Пользователям ИСПДн (далее – пользователь) является каждый сотрудник университета, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и средствам защиты ИСПДн.

1.3. Список пользователей, утвержден приказом ректора от 11 мая 2022 года № 02.00-67/0282 «Об утверждении перечня должностей работников по вопросам обработки персональных данных».

1.4. Пользователь несет персональную ответственность за свои действия.

1.5. Пользователь в своей работе руководствуется настоящей инструкцией и другими регламентирующими документами университета.

1.6. Методическое руководство работой пользователей в вопросах обеспечения безопасности ПДн осуществляет администратор безопасности ИСПДн.

2. Пользователь обязан:

2.1. Знать и выполнять требования настоящей инструкции и других документов университета, регламентирующих порядок действий по защите информации.

2.2. Выполнять на рабочем месте только те процедуры обработки ПДн, которые определены для него в должностной инструкции.

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

2.4. Соблюдать требования действующего Положения об организации парольной защиты доступа к сетевым ресурсам и автоматизированным системам ВоГУ.

2.5. Соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при их обработке.

2.6. Соблюдать правила при работе в сетях общего доступа и международного обмена:

2.6.1. подключение рабочих мест ИСПДн к сетям общего доступа и международного обмена возможно только в случае необходимости этого для выполнения процедур обработки ПДн;

2.6.2. запрещено нецелевое использование ресурса сетей общего доступа и международного обмена;

2.6.3. рабочие места ИСПДн, имеющие подключение к сетям общего доступа и международного обмена, должны быть оснащены штатными средствами защиты информации (антивирусное программное обеспечение, межсетевые экраны, средства защиты от несанкционированного доступа);

2.6.4. запрещена работа в сетях общего доступа и международного обмена с отключенными средствами защиты информации;

2.6.5. передача защищаемых данных по сетям общего доступа и международного обмена возможна только с использованием средств шифрования.

2.7. При работе с персональными данными не допускать присутствие в помещении, где расположены средства вычислительной техники, лиц, не допущенных к обрабатываемой информации.

2.8. Соблюдать требования к расположению устройств вывода информации (мониторы, принтеры), исключающему возможность несанкционированного ознакомления посторонними лицами с отображаемой на них информацией.

2.9. Во время кратковременных отлучений от рабочего места производить блокировку персонального компьютера средствами операционной системы.

После окончания обработки персональных данных произвести завершение работы средствами обработки ПДн, убрать, если применяются, электронный ключ и съемные носители информации в сейф.

2.10. При возникновении подозрения на наличие на автоматизированном рабочем месте компьютерного вируса, пользователь должен провести внеочередной антивирусный контроль своей рабочей станции.

2.11. В случае обнаружения при проведении антивирусной проверки компьютерного вируса пользователь обязан приостановить работу и немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного начальника и администратора ИСПДн..

2.12. Обо всех выявленных нарушениях, связанных с информационной безопасностью университета, нештатной работой программного обеспечения необходимо уведомить непосредственного начальника и администратора безопасности ИСПДн.

2.13. По вопросам работы и настройки элементов ИСПДн необходимо обращаться к администратору ИСПДн.

3. Пользователю запрещено:

3.1. Записывать и хранить персональные данные на неучтенных установленным порядком машинных носителях информации.

3.2. Удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности.

3.3. Самостоятельно подключать к персональному компьютеру какие-либо устройства и вносить изменения в состав, конфигурацию, размещение персонального компьютера.

3.4. Самостоятельно устанавливать и/или запускать (выполнять) на персональном компьютере любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей.

3.5. Осуществлять обработку персональных данных в условиях, позволяющих осуществлять их просмотр лицами, не имеющими к ним допуска, а также при несоблюдении требований по эксплуатации персонального компьютера.

3.6. Сообщить кому-либо, кроме руководителя подразделения, устно или письменно личные атрибуты доступа к ресурсам персонального компьютера.

3.7. Отключать (блокировать) средства защиты информации.

3.8. Производить какие-либо изменения в подключении и размещении технических средств.

3.9. Производить иные действия, ограничения, на исполнение которых предусмотрены утвержденные регламенты и инструкции.

3.10. Оставлять бесконтрольно персональный компьютер с загруженными персональными данными.

4. Пользователь имеет право:

4.1. Обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать и пр.) информацию, содержащую персональные данные и иную конфиденциальную информацию, в пределах, определенных должностными полномочиями данного пользователя.

4.2. Обращаться к обслуживающему персоналу объектов вычислительной техники (далее - ОВТ) с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным на ОВТ, а также со средствами защиты информации.

5. Ответственность пользователей

5.1. Пользователь в соответствии с законодательством несет ответственность за:

5.1.1. неисполнение и ненадлежащее исполнение требований настоящей Инструкции;

5.1.2. несоблюдение требований инструкций и иных локальных нормативных актов, определяющих порядок обработки конфиденциальной информации на ОВТ и использования информационных ресурсов Университета.

6. Порядок ознакомления с Инструкцией

6.1. Работники подразделений ВоГУ и лица, выполняющие работы по договорам и контрактам, имеющие отношение к работе с персональными данными, должны быть в обязательном порядке ознакомлены под роспись с настоящей Инструкцией согласно приложению.

Приложение
к Инструкции пользователя,
информационной системы
персональных данных ВоГУ,
утвержденной приказом ректора
от 27.07.2022 № 02.00-67/0426

ЛИСТ ОЗНАКОМЛЕНИЯ СОТРУДНИКОВ
С Инструкцией пользователя информационной системы персональных данных ВоГУ

С инструкцией ознакомлен (ы):

№ п/п	Фамилия И.О. сотрудника	Дата ознакомления	Подпись об ознакомлении
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			