
	<b>МИНОБРНАУКИ РОССИИ</b> Федеральное государственное бюджетное образовательное учреждение высшего образования «Ухтинский государственный технический университет» (ФГБОУ ВО «УГТУ»)	СК УГТУ -2020
	<b>Сектор по защите информации и антитеррору</b>	Лист 1 Всего листов 16
	Инструкция пользователя информационной системы персональных данных	Версия 1.0

Приложение № 5  
 к приказу от 06.04.2020 № 232

**ИНСТРУКЦИЯ**  
**пользователя информационной системы персональных данных**

Ухта  
 2020

	<b>МИНОБРНАУКИ РОССИИ</b> Федеральное государственное бюджетное образовательное учреждение высшего образования «Ухтинский государственный технический университет» (ФГБОУ ВО «УГТУ»)	СК УГТУ -2020
	<b>Сектор по защите информации и антитеррору</b>	Лист 2 Всего листов 16
	Инструкция пользователя информационной системы персональных данных	Версия 1.0

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция пользователя информационных систем персональных данных ФГБОУ ВО «Ухтинский государственный технический университет» (далее – Инструкция/Университет) определяет общие правила работы работников в информационных системах персональных данных Университета.

1.2. В настоящей Инструкции применяются следующие термины и определения:

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

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

1.2.3. **Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники.


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

1.2.5. **Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

1.2.6. **Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.2.7. **Несанкционированный доступ (НСД)** – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

1.2.8. **Посторонние лица** – лица, которые не имеют права самостоятельного доступа в помещение и (или) не имеют права

	<b>МИНОБРНАУКИ РОССИИ</b> Федеральное государственное бюджетное образовательное учреждение высшего образования «Ухтинский государственный технический университет» (ФГБОУ ВО «УГТУ»)	СК УГТУ -2020
	<b>Сектор по защите информации и антитеррору</b>	Лист 3 Всего листов 16
	Инструкция пользователя информационной системы персональных данных	Версия 1.0

самостоятельного доступа в информационные системы и (или) не имеют допуска к защищаемой информации.

**1.2.9. Средство защиты информации от несанкционированного доступа (СЗИ НСД)** – программное, техническое или программно-техническое средство, направленное на предотвращение или существенное затруднение несанкционированного доступа к информации.

**1.2.10. Пользователь ИСПДн (далее – Пользователь)** осуществляет обработку персональных данных в информационной системе персональных данных Университета.

**1.2.11. Администратор** - сотрудник, должностные обязанности которого подразумевают обеспечение штатной работы парка компьютерной техники, сети и программного обеспечения.

**1.2.12. Администратор ИСПДн** - лицо, выполняющее функции по обеспечению безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники ИСПДн в пределах своей зоны ответственности.

**1.3.** Пользователем является каждый работник Университета, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.


**1.4.** Пользователь в своей работе руководствуется настоящей Инструкцией, Положением об обработке персональных данных ФГБОУ ВО "Ухтинский государственный технический университет", утвержденным приказом ректора, руководящими и нормативными актами ФСТЭК России и ФСБ России и локальными нормативными актами Университета, регламентирующими обработку персональных данных.

**1.5.** Методическое руководство работой Пользователя осуществляет Администратор ИСПДн.

## **2. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ**

**2.1.** Знать и выполнять требования законодательных актов Российской Федерации, настоящей Инструкции и других внутренних документов Университета, регламентирующих порядок обработки персональных данных.

**2.2.** Выполнять на автоматизированном рабочем месте (персональный компьютер или терминал, далее - АРМ) только те процедуры обработки персональных данных, которые определены для него должностной инструкцией.

	<b>МИНОБРНАУКИ РОССИИ</b> Федеральное государственное бюджетное образовательное учреждение высшего образования <b>«Ухтинский государственный технический университет»</b> (ФГБОУ ВО «УГТУ»)	СК УГТУ -2020
	<b>Сектор по защите информации и антитеррору</b>	Лист 4 Всего листов 16
	Инструкция пользователя информационной системы персональных данных	Версия 1.0

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.

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

2.8. При прекращении работ (трудовых отношений) все материальные носители, содержащие персональные данные (флэш-накопители, дискеты, компакт-диски, документы, черновики, распечатки на принтерах, кино- и фотоматериалы, модели, промышленные образцы и пр.), передать непосредственному руководителю.


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

2.10. Соблюдать требования парольной политики (раздел 3 настоящей Инструкции).

2.11. Соблюдать требования антивирусной защиты (раздел 4 настоящей Инструкции).

2.12. Пользователи, имеющие выход в Интернет, обязаны соблюдать правила при работе в сетях связи общего пользования и (или) сетях международного информационного обмена – Интернет (раздел 5 настоящей Инструкции).

2.13. Пользователи, работающие с электронной подписью или использующие шифрование, обязаны соблюдать Инструкцию по обращению с сертифицированными ФСБ (ФАПСИ) шифровальными средствами (СКЗИ) в ФГБОУ ВО "Ухтинский государственный технический университет",

	<b>МИНОБРНАУКИ РОССИИ</b> Федеральное государственное бюджетное образовательное учреждение высшего образования <b>«Ухтинский государственный технический университет»</b> (ФГБОУ ВО «УГТУ»)	СК УГТУ -2020
	<b>Сектор по защите информации и антитеррору</b>	Лист 5 Всего листов 16
	Инструкция пользователя информационной системы персональных данных	Версия 1.0

утвержденную приказом ректора.

2.14. Пользователи, работающие с персональными данными контрагентов организации, все наработанные файлы должны хранить на определенном Администратором сетевом диске/папке.

2.15. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.16. Обо всех выявленных нарушениях, связанных с порядком обработки персональных данных, а также для получения консультаций по вопросам обработки персональных данных необходимо обращаться к Администратору ИСПДн или ответственному за организацию обработки персональных данных.

2.17. Пользователям запрещается:

2.17.1. Нарушать установленные в Университете правила обработки персональных данных.

2.17.2. Использовать компоненты программного и аппаратного обеспечения Университета в неслужебных целях.

2.17.3. 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).


2.17.4. Оставлять без присмотра или неубранными в хранилища (шкаф, сейф) носители или документы, содержащие персональные данные.

2.17.5. Записывать и хранить конфиденциальную информацию (в том числе персональные данные) на неучтенных носителях информации (оптических (CD) дисках, гибких магнитных дисках, флеш-накопителях и т.п.).

2.17.6. Самовольно изменять состав и конфигурацию используемых программных, аппаратных, программно-аппаратных средств, самовольно устанавливать программное обеспечение, отключать/подключать оборудование или изменять режимы его работы.

2.17.7. Самовольно подключать компьютер к ЛВС Университета, изменять IP-адрес, MAC-адрес и иные настройки сети компьютера.

2.17.8. Производить действия, направленные на получение несанкционированного доступа к АРМ и серверам, равно как и любым другим

	<b>МИНОБРНАУКИ РОССИИ</b> Федеральное государственное бюджетное образовательное учреждение высшего образования <b>«Ухтинский государственный технический университет»</b> (ФГБОУ ВО «УГТУ»)	СК УГТУ -2020
	<b>Сектор по защите информации и антитеррору</b>	Лист 6 Всего листов 16
	Инструкция пользователя информационной системы персональных данных	Версия 1.0

узлам сети Интернет, в том числе:

- действия, направленные на нарушение нормального функционирования элементов сети (компьютеров, другого сетевого оборудования или программного обеспечения);
- установка программного обеспечения, осуществляющего перехват информации (информационных пакетов), адресованной другим пользователям;
- действия, направленные на получение несанкционированного доступа к информационным ресурсам, в последующем использовании такого доступа;
- уничтожение, модификация программного обеспечения или данных без согласования с непосредственным руководителем или владельцами этого ресурса;
- попытки подбора паролей к любым информационным ресурсам методом перебора всех возможных вариантов паролей, либо атак по словарю;
- 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;
- действия по сканированию локальной сети с целью определения ее внутренней структуры, списков открытых портов, наличия существующих сервисов и уязвимостей.

2.17.9. Самовольно изменять параметры средств защиты информации (в том числе и средств антивирусной защиты), а также завершать их работу и (или) самостоятельно их устанавливать.


2.17.10. Самостоятельно разрабатывать или использовать нерегламентированные (без разрешения непосредственного руководителя, не относящиеся к производственному процессу) программы (например, игры; IM-клиенты, такие как Google Messenger, Microsoft Messenger, ICQ и т.п.; P2P-клиенты: Kazaa, eMule, Skype и т.п.).

2.17.11. Разрешать посторонним лицам работать под своей учетной записью на АРМ.

2.17.12. 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).

2.17.13. Получать доступ к сети Интернет любыми способами, кроме



	<b>МИНОБРНАУКИ РОССИИ</b> Федеральное государственное бюджетное образовательное учреждение высшего образования «Ухтинский государственный технический университет» (ФГБОУ ВО «УГТУ»)	СК УГТУ -2020
	<b>Сектор по защите информации и антитеррору</b>	Лист 7 Всего листов 16
	Инструкция пользователя информационной системы персональных данных	Версия 1.0

как установленными настоящей Инструкцией, например, при помощи несанкционированно установленных на АРМ модемов и т. п.

2.17.14. Самовольно создавать совместно используемые сетевые ресурсы (папки общего доступа) на своих компьютерах и файловых серверах, несанкционированно удалять или изменять права доступа к ним.

2.17.15. В случае возникновения любых механических неисправностей в оборудовании осуществлять самостоятельные попытки их устранения.

2.17.16. Препятствовать должностным лицам при проведении проверок и служебных расследований, связанных с обеспечением безопасности информации.

2.17.17. 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).

2.17.18. 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 сотрудников, ответственных за установку и (или) сопровождение программного обеспечения.

2.17.19. Подключать к ЛВС 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 системному администратору.

### 3. ПАРОЛЬНАЯ ПОЛИТИКА

3.1. Общие требования к паролям:


3.1.1. Минимальное требование: буквенно-цифровой пароль. Желательно использовать буквы в верхнем или нижнем регистрах, цифры или специальные символы (например, ~ ! @ # \$ % ^ & \* ( ) \_ - + = | \ ? / . , ; ' ] [ { } < > . и т.п.).

3.1.2. Минимальная длина пароля: не менее 8-ми (восьми) символов.

3.1.3. Максимальный срок действия пароля: 180 суток.

3.1.4. Запрет использования трех ранее использовавшихся паролей.

3.1.5. Пароль пользователя не должен включать в себя легко вычисляемые сочетания символов, общепринятые сокращения, имена,

	<b>МИНОБРНАУКИ РОССИИ</b> Федеральное государственное бюджетное образовательное учреждение высшего образования «Ухтинский государственный технический университет» (ФГБОУ ВО «УГТУ»)	СК УГТУ -2020
	<b>Сектор по защите информации и антитеррору</b>	Лист 8 Всего листов 16
	Инструкция пользователя информационной системы персональных данных	Версия 1.0

фамилии, должности, год рождения, номер паспорта, табельный номер, иную информацию о Пользователе, доступную другим лицам.

3.1.6. Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов.

3.1.7. Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567, qwerty и т.п.).

3.2. Правила использования паролей:

3.2.1. Хранить в тайне свой пароль, не сообщать его другим лицам.

3.2.2. Не давать доступ в информационные системы другим лицам под своей учетной записью и паролем.

3.2.3. Изменять свой пароль при первом требовании политики паролей операционной системы (информационной системы).

3.2.4. Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.2.5. Немедленно сообщить ответственному по парольной защите об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

3.2.6. Запрещается записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.

3.2.7. Запрещается хранить пароли в записанном виде на отдельных листах бумаги.


3.2.8. Смена, удаление личного пароля любого Пользователя производится в следующих случаях:

- в случае подозрения на компрометацию пароля;
- по окончании срока действия;
- в случае прекращения полномочий (увольнение, переход на другую работу внутри Университета) Пользователя после окончания последнего сеанса работы в информационных системах;
- по указанию Администратора ИСПДн.

3.2.9. При увольнении, переходе на новую должность работника, имеющего доступ помимо своей учетной записи к другим ресурсам (межсетевые экраны, маршрутизаторы, серверы, другие учетные записи и т.п.) также производится внеплановая смена паролей к таким ресурсам.

3.2.10. Для создания значений паролей могут применяться



	<b>МИНОБРНАУКИ РОССИИ</b> Федеральное государственное бюджетное образовательное учреждение высшего образования <b>«Ухтинский государственный технический университет»</b> (ФГБОУ ВО «УГТУ»)	СК УГТУ -2020
	<b>Сектор по защите информации и антитеррору</b>	Лист 9 Всего листов 16
	Инструкция пользователя информационной системы персональных данных	Версия 1.0

специальные программные средства (генераторы паролей).

#### **4. АНТИВИРУСНАЯ ЗАЩИТА**

4.1. В случае отсутствия штатных функций антивирусной программы, предусматривающих автоматическую проверку файлов, Пользователь обязан осуществлять проверку файлов, получаемых:

- по электронной почте;
- через сеть Интернет;
- на магнитном, оптическом диске, флэш–накопителе;
- ином съемном носителе информации;
- полученные иным способом.

4.2. Пользователю запрещается:

4.2.1. Осуществлять действия, направленные на выключение антивирусной программы;


4.2.2. Самостоятельно устанавливать на АРМ программное обеспечение;

4.2.3. Запускать файлы, полученные по сетям связи (электронной почте, Интернет), со съемных носителей, даже если они получены проверенного адресата, без предварительной их проверки антивирусной программой.

4.3. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) Пользователь самостоятельно или вместе с ответственным за антивирусную защиту должен провести внеочередной антивирусный контроль своего рабочего места.

4.4. В случае обнаружения при проведении антивирусной проверки вирусного заражения Пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения вирусного заражения ответственного за антивирусную защиту;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь ответственного за антивирусную защиту).

	<b>МИНОБРНАУКИ РОССИИ</b> Федеральное государственное бюджетное образовательное учреждение высшего образования «Ухтинский государственный технический университет» (ФГБОУ ВО «УГТУ»)	СК УГТУ -2020
	<b>Сектор по защите информации и антитеррору</b>	Лист 10 Всего листов 16
	Инструкция пользователя информационной системы персональных данных	Версия 1.0

## **5. ПОРЯДОК РАБОТЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И СЕТИ ИНТЕРНЕТ**

5.1. Подключение к информационным системам и сервисам сети Интернет.

5.1.1. Целью работы Пользователя в информационных системах и сети Интернет является сбор, обработка, хранение общедоступной и служебной информации, обмен электронными сообщениями в служебных целях.

5.1.2. Доступ к ресурсам информационных систем и сервисам сети Интернет предоставляется Пользователям только в том случае, если это не противоречит требованиям по защите информации (требованиям настоящей Инструкции и иных нормативных документов в области защиты информации).

5.1.3. Возможность получить доступ к ресурсам информационных систем и сервисам сети Интернет не является гарантией того, что запрошенный ресурс или сервис является разрешенным политиками Университета.

5.1.4. Основанием для подключения работника Университета к ресурсам информационных систем и сервисам сети Интернет является мотивированная заявка Администратору от непосредственного руководителя Пользователя с указанием полномочий доступа к таким ресурсам и сервисам.

5.1.5. Администратор, либо работник, выполняющий его функции, организует подключение к сервисам сети Интернет Пользователей в установленном порядке, осуществляет контроль над использованием ресурсов сети Интернет.


5.1.6. После выполнения задания Администратор сообщает Пользователю о выполнении заявки.

5.1.7. Основанием для отключения АРМ Пользователя от информационных систем и сервисов сети Интернет являются следующие события:

- нарушение инструкций и иных локальных нормативных актов в области защиты информации Университета;
- в случае нарушения Пользователем действующего законодательства в сфере компьютерной информации;
- увольнение Пользователя, либо перевод его в другое подразделение.

5.2. Порядок работы в сети Интернет.

5.2.1. Использование сотрудниками Университета сети Интернет должно осуществляться исключительно для выполнения должностных обязанностей.

	<b>МИНОБРНАУКИ РОССИИ</b> Федеральное государственное бюджетное образовательное учреждение высшего образования <b>«Ухтинский государственный технический университет»</b> (ФГБОУ ВО «УГТУ»)	СК УГТУ -2020
	<b>Сектор по защите информации и антитеррору</b>	Лист 11 Всего листов 16
	Инструкция пользователя информационной системы персональных данных	Версия 1.0

5.2.2. Информация, образованная (образующаяся) в процессе трудовой деятельности работника, является собственностью Университета и не подлежит использованию, в том числе использованию в сети Интернет или с помощью сети Интернет в личных целях и (или) в корыстных интересах других лиц (организаций).

5.2.3. При проведении технических работ, связанных с настройкой оборудования (коммуникационное оборудование, прокси-сервера, маршрутизаторы и т.п.); в случае обнаружения попыток несанкционированного доступа к Интернет-шлюзу, АРМ Пользователей может проводиться временное отключение Пользователей от сервисов сети Интернет (в случае планового отключения Пользователи уведомляются об этом заблаговременно).

5.2.4. Вся информация о ресурсах, посещаемых работниками Университета, протоколируется и, при необходимости, может быть предоставлена руководителям подразделений, а также руководству Университета для детального изучения и принятия решения о мерах дисциплинарной ответственности.


5.2.5. При работе в сети Интернет Пользователям запрещается:

- умышленное распространение и получение материалов в/из сети Интернет, противоречащих законодательству Российской Федерации, в том числе материалов, пропагандирующих насилие или экстремизм; разжигающих расовую, национальную или религиозную вражду; разъясняющих порядок изготовления и/или применения наркотиков, взрывчатых веществ, оружия и т. п.; материалов порнографического характера; компьютерных вирусов и других вредоносных программ;

- передавать в сеть Интернет информацию, к которой в соответствии с законодательством ограничен доступ (персональные данные, коммерческая тайна) без соответствующего разрешения;

- фальсифицировать IP-адрес, MAC-адрес, иные адреса, используемые в сетевых протоколах, а также прочую служебную информацию при передаче данных через сеть Интернет.

- предоставлять доступ в сеть Интернет со своей рабочей станции кому-либо, в том числе программно-техническими способами через локальную вычислительную сеть Управления (например, путем несанкционированной установки локального Интернет-шлюза на рабочую станцию);

	<b>МИНОБРНАУКИ РОССИИ</b> Федеральное государственное бюджетное образовательное учреждение высшего образования «Ухтинский государственный технический университет» (ФГБОУ ВО «УГТУ»)	СК УГТУ -2020
	<b>Сектор по защите информации и антитеррору</b>	Лист 12 Всего листов 16
	Инструкция пользователя информационной системы персональных данных	Версия 1.0

– получать доступ к сети Интернет любыми способами, не предусмотренными действующими локальными нормативными актами Университета (инструкциями, положениями, регламентами);

– осуществлять несанкционированный доступ к ресурсам и сервисам сети Интернет.

– выполнять действия (взлом, DoS (отказ в обслуживании), ARP-spoofing атаки, сканирование локальной вычислительной сети) направленные на нарушение функционирования элементов сети Интернет (коммуникационного оборудования, серверов, рабочих станций, программного обеспечения).

5.3. Правила работы Пользователей с электронной почтой:

5.3.1. Пользователи обязаны использовать электронную почту только для выполнения служебных обязанностей.

5.3.2. Запрещается отправлять файлы, содержащие персональные данные в открытом виде (незашифрованные).

5.3.3. Запрещается массовая рассылка почтовых сообщений (более 10) внешним адресатам без согласования с руководством (спама).

5.3.4. Запрещается использовать не свой обратный адрес при отправке электронной почты.

5.3.5. Запрещается отправлять по электронной почте исполняемые файлы (обычно имеют расширения exe, com, bat). В случае необходимости отправки таких файлов, помещать их в архив.

5.3.6. Присоединяемые файлы рекомендуется упаковывать в архив при помощи программ-архиваторов.

5.3.7. Корпоративные рекомендации использования электронной почты:

– Вы должны оказывать то же уважение, что и при устном общении;


– Вы должны проверять правописание, грамматику и дважды перечитывать свое сообщение перед отправлением;

– Вы не должны участвовать в рассылке посланий, пересылаемых по цепочке (чаще всего это письма религиозно-мистического, развлекательного содержания, спам);

– Вы не должны по собственной инициативе пересылать по произвольным адресам незатребованную информацию;

– Вы не должны рассылать сообщения, которые являются зловредными, раздражающими или содержащими угрозы другим пользователям;

– Вы не должны отправлять никаких сообщений противозаконного или неэтичного содержания;

	<b>МИНОБРНАУКИ РОССИИ</b> Федеральное государственное бюджетное образовательное учреждение высшего образования <b>«Ухтинский государственный технический университет»</b> (ФГБОУ ВО «УГТУ»)	СК УГТУ -2020
	<b>Сектор по защите информации и антитеррору</b>	Лист 13 Всего листов 16
	Инструкция пользователя информационной системы персональных данных	Версия 1.0

– Вы должны помнить, что электронное послание является эквивалентом почтовой открытки и не должно использоваться для пересылки конфиденциальной информации без использования средств защиты (шифрование);

– Вы не должны использовать широкоэмитательные возможности электронной почты за исключением выпуска уместных объявлений;

– Вы должны свести к минимуму количество электронных посланий личного характера;

– Вы должны неукоснительно соблюдать правила и инструкции и помогать администраторам бороться с нарушителями правил.

## **6. ПОРЯДОК РАБОТЫ С НОСИТЕЛЯМИ ИНФОРМАЦИИ**

6.1. Под использованием носителей информации в информационных системах Университета понимается их подключение к инфраструктуре информационных систем с целью обработки, приема/передачи информации между информационными системами и носителями информации.

6.2. Допускается использование только учтенных носителей информации, которые являются собственностью Университета и подвергаются регулярной ревизии и контролю.

6.3. Учет и выдачу съемных носителей информации осуществляет администратор. Факт выдачи носителя фиксируется в журнале учета съемных носителей информации, форма которого утверждается приказом ректора.

6.4. Возможность подключения носителей информации, а также получение учтенных носителей информации предоставляются Пользователям по инициативе руководителей структурных подразделений в случаях:

– необходимости выполнения вновь принятым работником своих должностных обязанностей;

– возникновения у Пользователя производственной необходимости.

6.5. При использовании носителей информации необходимо:


– использовать носители информации исключительно для выполнения своих служебных обязанностей;

– бережно относиться к носителям конфиденциальной информации;

– обеспечивать физическую безопасность носителей информации всеми разумными способами;

– извещать администраторов о фактах утраты (кражи) носителей информации.

6.6. При использовании носителей конфиденциальной информации

	<b>МИНОБНАУКИ РОССИИ</b> Федеральное государственное бюджетное образовательное учреждение высшего образования <b>«Ухтинский государственный технический университет»</b> (ФГБОУ ВО «УГТУ»)	СК УГТУ -2020
	<b>Сектор по защите информации и антитеррору</b>	Лист 14 Всего листов 16
	Инструкция пользователя информационной системы персональных данных	Версия 1.0

запрещено:

- использовать носители конфиденциальной информации в личных целях;
- передавать носители конфиденциальной информации другим лицам (за исключением администраторов);
- хранить съемные носители с конфиденциальной информацией (персональными данными) на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
- выносить съемные носители с конфиденциальной информацией (персональными данными) из служебных помещений для работы с ними на дому и т. д.

6.7. Любое взаимодействие (обработка, прием/передача информации), инициированное Пользователем между информационной системой и неучтенными (личными) носителями информации, рассматривается как несанкционированное (за исключением случаев, оговоренных с администраторами заранее). Администратор оставляет за собой право заблокировать или ограничивать использование носителей информации.

6.8. Информация об использовании Пользователями носителей информации в информационных системах протоколируется и, при необходимости, может быть предоставлена руководителям структурных подразделений, а также руководителям Университета.


6.9. В случае выявления фактов несанкционированного и/или нецелевого использования носителей информации инициируется служебная проверка, проводимая комиссией, состав которой определяется ответственным за организацию обработки персональных данных и утверждается Ректором Университета. По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю структурного подразделения для принятия мер согласно локальным нормативным актам Университета и действующему законодательству Российской Федерации.

6.10. При отправке или передаче конфиденциальной информации (персональных данных) адресатам на съемные носители записываются только предназначенные адресатам данные.

6.11. Вынос съемных носителей конфиденциальной информации (персональных данных) для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

6.12. Съемные носители конфиденциальной информации



	<b>МИНОБНАУКИ РОССИИ</b> Федеральное государственное бюджетное образовательное учреждение высшего образования «Ухтинский государственный технический университет» (ФГБОУ ВО «УГТУ»)	СК УГТУ -2020
	<b>Сектор по защите информации и антитеррору</b>	Лист 15 Всего листов 16
	Инструкция пользователя информационной системы персональных данных	Версия 1.0

(персональных данных), пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется комиссией, состав которой определяется ответственным за организацию обработки персональных данных. По результатам уничтожения носителей составляется акт.

6.13. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители конфиденциальной информации изымаются и делаются соответствующие пометки в журнале учета носителей.

## **7. ПРАВА ПОЛЬЗОВАТЕЛЯ**

7.1. Использовать информационные системы Университета для выполнения служебных обязанностей.

7.2. Обращаться к системному администратору, Администратору ИСПДн, ответственному за организацию обработки персональных данных для консультаций по поводу использования программного обеспечения и АРМ, вопросам обработки персональных данных.

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

7.4. Направлять предложения по модернизации программного обеспечения, разрабатываемого в Университете или по заказу Университета.


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

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

7.7. Получать консультации и разъяснения по нормативным документам, регламентирующим работу с персональными данными в Университета.

## **8. ОТВЕТСТВЕННОСТЬ**

8.1. Пользователь несет персональную ответственность за свои действия или бездействие, которые повлекут за собой разглашение персональных данных, а также за нарушение нормального функционирования

	<p align="center"><b>МИНОБРНАУКИ РОССИИ</b>          Федеральное государственное бюджетное          образовательное учреждение высшего образования  <b>«Ухтинский государственный технический университет»</b>          (ФГБОУ ВО «УГТУ»)</p>	СК УГТУ -2020
	<p align="center"><b>Сектор по защите информации и антитеррору</b></p>	Лист 16 Всего листов 16
	<p align="center">Инструкция пользователя информационной системы персональных          данных</p>	Версия 1.0

информационных систем или ее отдельных компонентов, несанкционированный доступ к информации в соответствии с законодательством Российской Федерации и локальными нормативными актами Университета.