

Приложение № 2 к приказу «Об
обеспечении безопасности
персональных данных в ГБОУВО
РК КИПУ имени Февзи Якубова»
от 05.09.2023, г. № 449

ПРАВИЛА

обработки персональных данных без использования средств автоматизации в ГБОУВО РК КИПУ имени Февзи Якубова

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила обработки персональных данных без использования средств автоматизации в ГБОУВО РК КИПУ имени Февзи Якубова (далее соответственно – Правила, Университет) разработаны в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без средств автоматизации» и определяет правила работы с персональными данными (далее – ПДн) и их материальными носителями без использования средств автоматизации (далее – СА).

1.2. Обработка ПДн считается осуществленной без использования СА (неавтоматизированной), если такие действия с ПДн, как использование, уточнение, распространение, уничтожение ПДн в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека, при этом ПДн могут быть, как извлеченными из информационной системы персональных данных (далее – ИСПДн), так и не связанными с ИСПДн.

1.3. Все вопросы, связанные с обработкой ПДн, не урегулированные настоящими Правилами, разрешаются действующим законодательством Российской Федерации.

2. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

2.1. ПДн при их обработке, осуществляемой без использования СА, должны обособляться от иной информации, в частности, путем фиксации их на отдельных материальных носителях персональных данных (далее –

материальные носители), в специальных разделах или на полях форм (бланков).

2.2. При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы. Для обработки различных категорий ПДн, осуществляемой без использования СА, для каждой категории ПДн должен использоваться отдельный материальный носитель.

2.3. Лица, осуществляющие обработку ПДн без использования СА, должны быть проинформированы о факте обработки ими ПДн, обработка которых осуществляется без использования СА.

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

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки ПДн, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых способов обработки ПДн;

б) типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования СА, – при необходимости получения письменного согласия на обработку ПДн;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;

г) типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

2.5. При ведении журналов, содержащих ПДн, необходимые для однократного пропуска субъекта ПДн на территорию (объекты) Университета, делается запись в журнал не более одного раза в каждом случае пропуска субъекта ПДн.

2.6. При несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, должны быть приняты меры по обеспечению отдельной обработки ПДн, в частности:

а) при необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн;

б) при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

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

2.8. Правила, предусмотренные п.п. 2.6 и 2.7 настоящих Правил, применяются также в случае, если необходимо обеспечить отдельную обработку зафиксированных на одном материальном носителе ПДн и информации, не являющейся ПДн.

2.9. Уточнение ПДн при осуществлении их обработки без использования СА 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 ПДн.

3. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

3.1. Обработка ПДн, осуществляемая без использования СА, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

3.2. Необходимо обеспечивать отдельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

3.3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключаящие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются Университетом.

4. СРОКИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Общий срок обработки ПДн определяется периодом времени, в течение которого Университет осуществляет действия (операции) в отношении ПДн, обусловленные заявленными целями их обработки, в том числе хранение ПДн.

4.2. Обработка ПДн начинается с момента их получения Университетом и заканчивается:

- по достижении заранее заявленных целей обработки;
- по факту утраты необходимости в достижении заранее заявленных целей обработки.

4.3. Университет осуществляет хранение ПДн в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки.

4.4. Все работники Университета, допущенные к обработке ПДн без использования СА, несут административную, материальную, уголовную ответственность в соответствии с действующим законодательством Российской Федерации за обеспечение сохранности и соблюдение правил работы с ПДн.

4.5. Работники Университета, работающие с ПДн, обязаны использовать информацию о ПДн исключительно для целей, связанных с выполнением своих трудовых обязанностей.

4.6. Работники Университета, работающие с ПДн, обязаны немедленно сообщать своему непосредственному руководителю и(или) руководству Университета обо всех ставших им известными фактах получения третьими лицами несанкционированного доступа либо попытки получения доступа к ПДн, об утрате или недостатке носителей информации, содержащих ПДн, удостоверений, пропусков, ключей от сейфов (хранилищ), личных печатей, электронных ключей и других фактах, которые могут привести к несанкционированному доступу к ПДн, а также о причинах и условиях возможной утечки этих сведений.

4.7. При прекращении выполнения трудовой функции, связанной с обработкой ПДн, все носители информации, содержащие ПДн (оригиналы и

копии документов, машинные и бумажные носители и пр.), которые находились в распоряжении работника в связи с выполнением должностных обязанностей, данный работник должен передать своему непосредственному руководителю.

5. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

5.1. Доступ к ПДн работников, лиц, претендующих на трудоустройство, лиц, ранее состоящих в трудовых отношениях с Университетом, родственников работников Университета, в том числе бывших, обучающихся (студенты, аспиранты), родителей (законных представителей) обучающихся, поступающих (абитуриентов), слушателей (учащихся довузовской подготовки), а также лиц, состоящих в договорных и иных гражданско-правовых отношениях с Университетом имеют следующие работники Университета, непосредственно использующие эти данные в рамках выполнения своих должностных обязанностей:

- ректор Университета;
- проректора Университета;
- помощники ректора и первого проректора;
- начальник и работники управления кадров;
- начальник и работники учебно-методического управления;
- начальник и работники управления документооборота и контроля;
- главный бухгалтер и работники финансово-экономического управления;
- начальник и работники юридического отдела;
- директор и работники научно-технической библиотеки;
- директор и работники центра дополнительного профессионального обучения;
- работники отдела научно-исследовательской деятельности и инновационного развития;
- начальник и работники отдела по международным связям;
- работники приемной комиссии;
- начальник и работники управления информатизации;
- начальник и работники редакционно-издательского отдела;
- работники отдела по воспитательной и социальной работе;
- начальник и работники отдела комплексной безопасности;
- деканы факультетов, их заместители, руководители иных образовательных подразделений, осуществляющих работу с обучающимися;

- методисты и секретари факультетов;
- заведующие кафедрами и специалисты по учебно-методической работе кафедр;
- директор, заместители директора и учебно-вспомогательный персонал Инженерно-педагогического колледжа КИПУ имени Февзи Якубова;
- директор и учебно-вспомогательный персонал Керченского филиала КИПУ имени Февзи Якубова;
- директор и секретарь Научно-исследовательского института крымскотатарской филологии, истории и культуры этносов Крыма;
- непосредственно субъект ПДн.

5.2. Внешний доступ к ПДн разрешается только при наличии заявления запросившего их лица с указанием перечня необходимой информации, целей для которых она будет использована, с письменного согласия субъекта ПДн которого затребованы.

5.3. Сообщение сведений о ПДн субъекта его родственникам, членам семьи, иным близким ему людям также производится только при получении письменного согласия субъекта ПДн.

5.4. При передаче ПДн третьим лицам, в том числе представителям работников, обучающихся, в порядке, установленном нормативными правовыми актами Российской Федерации и настоящими Правилами, передаваемая информация ограничивается только теми ПДн, которые необходимы для выполнения третьими лицами их функций.

5.5. Запрещается передача ПДн в коммерческих целях без согласия субъекта ПДн, а также иное использование ПДн в неслужебных целях.

6. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. ПДн относятся к конфиденциальной информации. Работники Университета, уполномоченные на обработку ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

6.2. Обработка ПДн осуществляется в охраняемых помещениях. Возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц исключена.

6.3. При хранении носителей ПДн должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный доступ к ним.

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

6.5. Университет при обработке ПДн принимает необходимые организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий.

6.6. В помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн, а также хранятся носители ПДн, допускаются только работники, уполномоченные на обработку ПДн приказом ректора Университета.

6.7. Нахождение в помещениях, предназначенных для обработки ПДн, лиц, не являющихся уполномоченными на обработку ПДн, возможно только в сопровождении работника, уполномоченного на обработку ПДн на время, обусловленное производственной необходимостью.

6.8. Ответственными за организацию доступа в помещения, в которых ведется обработка ПДн, являются руководители структурных подразделений.

6.9. Персональные данные, содержащиеся на бумажных носителях, хранятся в запираемых шкафах с соблюдением установленных требований пожарной безопасности. В помещении(ях) научно-технической библиотеки и финансово-экономического управления допускается хранить ПДн в не запираемых стеллажах (шкафах) при условии пребывания в данных помещениях посторонних лиц, в том числе проведения уборки помещений, в присутствии работника(ов) соответствующего подразделения и запираания дверей на ключ при покидании помещения(ий) работником(ами) подразделения.

6.10. Выдача ключей от сейфа производится руководителем структурного подразделения, в функции которого входит обработка определенных ПДн (а на период его временного отсутствия – болезнь, отпуск и т.п. – лицом, исполняющим его обязанности), только работникам данного структурного подразделения, либо иным лицам, которые в соответствии с локальными нормативными актами Университета осуществляют обработку ПДн. Сдача ключа осуществляется лично руководителю или лицу, исполняющему его обязанности, после закрытия сейфа или несгораемого шкафа.

6.11. ПДн, содержащиеся на бумажных носителях, сдаются в архив Университета после истечения срока хранения, установленного номенклатурой дел Университета.

7. ПОРЯДОК ОХРАНЫ И ДОПУСКА ПОСТОРОННИХ ЛИЦ В ЗАЩИЩАЕМЫЕ ПОМЕЩЕНИЯ

7.1. Вскрытие и закрытие помещений с ПДн осуществляется работниками, работающими в данных помещениях. Перечень уполномоченных лиц Университета, которым предоставлен доступ к ПДн, имеющих право вскрывать (сдавать под охрану) и опечатывать помещения, утверждается приказом ректора Университета.

7.2. При отсутствии работников, ответственных за вскрытие помещений, данные помещения могут быть вскрыты комиссией, созданной на основании приказа. Комиссией составляется акт вскрытия.

7.3. При закрытии помещений работники, ответственные за помещения, проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и носители информации, на которых содержится конфиденциальная информация, убирают для хранения в специальные шкафы и/или сейфы, предусмотренные для хранения ПДн.

7.4. Постановка и снятие помещений под охрану производится охранником после окончания и перед началом рабочего дня соответственно.

8. ОСУЩЕСТВЛЕНИЕ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ.

8.1. Полученные в ходе внутреннего контроля результаты обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер защиты информации и выявления нарушений. При обнаружении нарушений норм и требований по защите информации ответственный за обеспечение безопасности ПДн докладывает о несоответствиях руководству Университета для принятия решения о прекращении обработки информации и проведения соответствующих организационных и технических мер по устранению нарушения(ий). Результаты контроля защиты информации оформляются предписанием, содержащим протокол или в соответствующих журналах учета результатов контроля.

9. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Ответственность за организацию защиты ПДн, обрабатываемых без использования СА, несут руководители соответствующих структурных подразделений. Ответственность за непосредственное исполнение требований по защите ПДн и надлежащего порядка проводимых работ возлагается на работников подразделений, в которых производится обработка ПДн.

9.2. Работники Университета, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн субъекта ПДн, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

9.3. Разглашение ПДн субъекта ПДн (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих ПДн субъекта ПДн, а также иные нарушения обязанностей по их защите и обработке, установленных настоящими Правилами, локальными нормативно-правовыми актами (приказами) Университета, влечет наложение на работника, имеющего доступ к ПДн, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник Университета, имеющий доступ к ПДн субъекта ПДн и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Университету (в соответствии с п. 7 ст. 243 Трудового кодекса РФ).

9.4. В отдельных случаях при разглашении ПДн работник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

9.5. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни) предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

10.1. С положениями настоящих Правил должны быть ознакомлены под роспись все работники структурных подразделений Университета и лица, выполняющие работы по договорам и контрактам, имеющие отношение к обработке ПДн работников, лиц, претендующих на трудоустройство, лиц, ранее состоящих в трудовых отношениях с Университетом, родственников работников Университета, в том числе

бывших, обучающихся (студенты, аспиранты), родителей (законных представителей) обучающихся, поступающих (абитуриентов), слушателей (учащихся довузовской подготовки), а также лиц, состоящих в договорных и иных гражданско-правовых отношениях с Университетом.