УТВЕРЖДАЮ
Министр социальной политики и труда
Удмуртской Республики

_____ Т. Ю. Чуракова
«____» _____ 2021 г.

ПРАВИЛА
соблюдения требований по информационной безопасности в государственной информационной системе Удмуртской Республики «Государственная информационная система социальной защиты и занятости населения Удмуртской Республики»

СОГЛАСОВАНО
Директор АУ УР «РИЦ»

_____ А. Н. Поскребышев
«____» _____ 2021 г.

г. Ижевск, 2021 г.

1. Общие положения

1.1. Настоящие Правила определяют требования по обеспечению информационной безопасности при работе в государственной информационной системе Удмуртской Республики «Государственная информационная система социальной защиты и занятости населения Удмуртской Республики» (далее – ГИС), а также описывают необходимые действия работников по их соблюдению.

1.2. Положения настоящих Правил являются обязательными для соблюдения всеми пользователями ГИС.

1.3. Ознакомление пользователей с настоящими Правилами осуществляется под роспись в установленном порядке.

2. Термины и определения

Информационный ресурс (ИР)	– любое системное или прикладное программное обеспечение, физические и виртуальные хранилища данных в электронном виде, средства чтения и записи электронных носителей информации
Мобильное устройство	– любое легко перемещаемое вычислительное устройство, предназначенное и используемое для создания, получения, хранения, обработки и передачи информации. К ним относятся **ноутбуки (в том числе планшетные портативные компьютеры)**, **карманные портативные компьютеры** (КПК), **смартфоны**, компьютерные записные книжки, сотовые телефоны.
Администратор информационной безопасности (далее - АИБ)	– работник, назначенный ответственным за обеспечение информационной безопасности и постоянный контроль за соблюдением требований безопасности информации, обрабатываемой на АРМ пользователей.
Носитель информации	– материальный предмет, на котором (или в котором) возможно разместить информацию в виде символов, образов, файлов и пр.
Съемный носитель информации	– электронный носитель информации, подключаемый к средствам компьютерной техники и используемый для хранения информации. К съемным носителям информации относятся дискеты, оптические (CD, DVD) диски, USB-носители, энергонезависимые карты памяти, фотоаппараты и т.п.

Устройство ввода-вывода информации	– выполненные как во внутреннем, так и во внешнем исполнении дисководы, приводы чтения и записи CD и DVD дисков, USB-порты и прочие переносные устройства, которые могут использоваться для выгрузки или загрузки информации в компьютер. Устройства ввода-вывода также являются информационными ресурсами.

3. Работа с информацией ограниченного доступа

3.1. Доступ к информации ограниченного доступа и ее передача

3.1.1. Пользователи **обязаны не разглашать информацию ограниченного доступа** в течение всего времени работы, а также обязаны соблюдать требования законодательства РФ и внутренних нормативных документов, регулирующих порядок предоставления информации, лицам, не являющимся пользователями. Фактом разглашения информации ограниченного доступа является несанкционированное предоставление данной информации, лицам, не имеющим прав на доступ к данной информации. Пользователи **несут ответственность** за несанкционированное разглашение им информации ограниченного доступа в соответствии с действующим законодательством Российской Федерации.

3.1.2. Разовое (единовременное) предоставление доступа к конфиденциальной информации либо ознакомление с ней пользователей, характер должностных обязанностей которых не связан с ее получением, использованием или обработкой, допускается **только** по согласованию с руководителем подразделения, имеющего право предоставления доступа к данной информации.

3.1.3. Предоставление постоянного (на постоянной основе) доступа и доступ к сетевым информационным ресурсам осуществляется в соответствии с разделом 5 настоящих Правил.

3.1.4. Передача документов на любых носителях, содержащих информацию ограниченного доступа, третьим лицам (клиентам, контрагентам и др.) без согласования с вышестоящим руководителем подразделения и АИБ **запрещается**. При передаче необходимо удостовериться, что с получателем заключено Соглашение о неразглашении и защите конфиденциальной информации.

3.1.5. При работе с носителями информации, содержащими конфиденциальную информацию, пользователь не должен оставлять данные носители без присмотра или должен убрать их в закрытое на ключ место хранения. Общие правила пользования, учета и хранения ключей от шкафов, тумбочек и прочих запирающихся устройств описаны в Приложении № 1 к настоящим Правилам.

3.1.6. Не допускается производить работу с **конфиденциальной** информацией в случае возможности ее просмотра посторонними лицами. Лица, не являющиеся пользователями, не должны видеть конфиденциальную информацию на экране компьютера. При необходимости пользователям

следует закрыть или свернуть все окна с конфиденциальной информацией или заблокировать компьютер. Бумажные конфиденциальные документы следует перевернуть текстом вниз или убрать со стола.

3.1.7. Делать копии, фотографировать или производить выписки из документов, содержащих конфиденциальную информацию, на любых видах носителей **не допускается**. Для осуществления данных действий необходимо получить **письменное** разрешение вышестоящего руководителя и разрешение АИБ.

4. Работа с персональным компьютером

4.1. Пользователю **запрещается** вскрывать персональный компьютер, который используется для работы (далее – компьютер), в том числе для самостоятельного устранения неисправностей, или **подключать к компьютеру любое оборудование**, не связанное непосредственно с его должностными обязанностями (модем, личные карманные персональные компьютеры (далее - КПК), смартфоны и сотовые телефоны и пр.).

4.2. При отсутствии пользователя на рабочем месте даже на незначительный период времени (более 5 минут) пользователь **обязан блокировать доступ к компьютеру**.

4.3. По окончанию рабочего дня пользователь должен выключать персональный компьютер. Исключением являются случаи, когда существует обоснованная в силу выполнения должностных обязанностей служебная необходимость не выключать компьютер.

4.4. Пользователю запрещается **самостоятельно устанавливать на компьютер программное обеспечение** (в том числе полученное в сообщениях электронной почты или из сети Интернет), изменять программную или аппаратную конфигурацию компьютера и настройки операционной системы. Список стандартного программного обеспечения и условия его установки для каждой категории пользователя определяются иными нормативными и распорядительными документами. В случае необходимости установки дополнительного ПО пользователю необходимо оформить соответствующую служебную записку в соответствии с утвержденной процедурой управления правами доступа.

4.5. Пользователю **запрещается отключать и/или удалять установленные средства защиты** (в том числе антивирусное программное обеспечение), а также изменять настройки данных средств.

4.6. Выполнение операций в ресурсах (прикладных системах), последствия которых пользователю не известны в силу отсутствия знаний по работе с данным ресурсом, использование компьютера для мошенничества и других видов противозаконной деятельности, а также использование каких-либо средств для осуществления несанкционированного доступа к ресурсам запрещается.

4.7. Самостоятельно осуществлять подключение, отключение, переключение и перенастройку сетевых элементов компьютера запрещается (подключение каких-либо сетевых карт, подключение компьютера в другую

сетевую розетку и пр.). Для проведения данных действий пользователю необходимо обратиться в подразделение, ответственное за сопровождение рабочих мест. Данный пункт не относится к пользователям, в обязанности которых входит перенастройка компьютеров.

5. Доступ к информационным ресурсам

5.1. Доступ к информационным ресурсам предоставляется пользователям **только** на основании соответствующих заявок, оформленных в соответствии с утвержденной процедурой управления правами доступа.

5.2. До начала работы в вычислительной сети пользователь обязан ознакомиться с настоящими Правилами**.**

5.3. Пользователь **обязан** периодически производить смену используемых им паролей. Срок действия паролей – 120 дней.

5.4. При создании пароля пользователь должны выбирать **сложные пароли**, состоящие не менее чем из **6**символов и **обязательно** содержащие как буквы, так и цифры, и, по возможности, специальные знаки (!»№;%:?*()_ и т. п.). Пароль не должен быть очевидными, то есть содержаться в каком-либо словаре. Не следует использовать в качестве пароля свою фамилию, даты рождений, имена детей номера своих телефонов, паспортов и других документов и т.п., а также любые всем известные и/или легко угадываемые сокращения. Запрещается использовать в качестве пароля имя пользователя.

5.5. При создании пароля пользователям **запрещается** использовать пароли, применяемые ими для доступа к домашним компьютерам, бесплатным службам электронной почты, web-сайтам сети Интернет и прочим сервисам не служебного характера.

5.6. **Запрещается** записывать пароли в доступных для визуального просмотра местах, а также хранить их в открытом виде на электронных носителях, за исключением ключевых носителей, к которым предъявляются отдельные требования (подробнее описано в разделе **Ошибка! Источник ссылки не найден.** настоящих Правил).

5.7. Пользователям **запрещается** передавать кому-либо (в том числе администраторам, непосредственному и вышестоящему руководителю) или разглашать свои аутентификационные данные (идентификатор доступа и пароль) для доступа к любому информационному ресурсу. Исключением могут быть случаи, когда отсутствие пользователя на рабочем месте (например, при болезни, вынужденном отсутствии и т.п.) может привести к приостановлению работы подразделения. В этом случае, возможен сброс пароля. После выхода на работу пользователь обязан сменить пароль, который был использован другим пользователем.

При проведении очередных проверок техники уполномоченными пользователь должен **самостоятельно** вводить свой пароль. **В случае поступления запроса по телефону или электронной почте с просьбой сообщить аутентификационные данные, немедленно сообщить об этом непосредственному руководителю.**

5.8. Запрещается осуществлять доступ с использованием чужого идентификатора доступа (имя пользователя) и пароля (за исключением случаев,

описанных в п. 5.7 настоящих Правил).

5.9. В случае увольнения пользователя или изменения его должностных обязанностей непосредственный руководитель **обязан** своевременно инициировать процедуру отключения (изменения) прав доступа данных пользователей.

6. Работа с сетью интернет

6.1. Доступ пользователей к сети Интернет предоставляется **только** в связи с необходимостью осуществления ими своих непосредственных должностных обязанностей.

6.2. Запрещается указывать аутентификационные данные (идентификатор доступа и пароль) для регистрации на web-сайтах, не имеющих непосредственного отношения к исполнению пользователей должностных обязанностей (например, сайты знакомств, Интернет-магазинов и пр.) и/или на которых указанная информация будет доступна другим пользователям сайта (например, форумы).

6.3. Пользователями **запрещается** пользоваться службами мгновенных сообщений (ICQ, Skype, MSN Messenger Connect for Enterprises и т.п.), посещать сервисы бесплатной электронной почты, а также сайты не имеющие отношения к выполнению должностных обязанностей.

6.4. Все действия пользователей при работе в сети Интернет (посещаемые сайты, объем отправленной и принятой информации и т.п.) сохраняются в специальных электронных журналах, которые периодически анализируются администратором информационной безопасности.

6.5. С целью недопущения заражения сети компьютерными вирусами, пользователям **запрещается** самостоятельно загружать из сети Интернет какое-либо программное обеспечение и исполняемые файлы.

7. Работа с устройствами ввода-вывода и съемными носителями информации

7.1. **Устройства ввода-вывода**

7.1.1. Устройства ввода-вывода, имеющие функции записи информации на носители, устанавливаются (подключаются) на рабочие компьютеры пользователей **в исключительных случаях**, если работа с такими устройствами вызвана необходимостью осуществления ими своих непосредственных должностных обязанностей. Для установки и подключения данных устройств оформляется Заявка, оформленная в соответствии с Регламентом управления правами доступа к информационным ресурсам и содержащая подробное обоснование необходимости такого доступа. Формулировки общего характера, такие как: «в связи с производственной необходимостью» в качестве обоснования не принимаются.

7.1.2. Пользователь, имеющий подключенное устройство ввода-вывода с функциями записи, **несет персональную ответственность** за его использование **только** для целей, указанных в Заявке.

7.2. **Съемные носители информации**

7.2.1. Подключение съемных носителей должно осуществляться только для непосредственной работы с ними. В случае отсутствия пользователя на рабочем месте, все съемные носители информации должны быть извлечены и/или отсоединены пользователем от компьютера. Оставлять указанные носители в не присоединенном/неподключенном состоянии в местах открытого доступа и на столах без присмотра **запрещено**. Пользователь должен убирать съемные носители в закрываемое на ключ место хранения или забирать с собой.

7.2.2. Пользователи, допущенные к работе со съемными носителями информации, **обязаны** предъявлять их по требованию АИБ для проверки. Если съемный носитель не используется, подлежит замене (для ремонта) или подлежит сдаче, пользователю необходимо также обратиться к администратору информационной безопасности для удаления всей информации, хранящейся на носителях. При увольнении или изменении должностных обязанностей, исполнение которых не требует использования съемных носителей информации, пользователь обязан сдать съемный носитель пользователю, осуществляющем выдачу носителей.

7.2.3. Самостоятельное приобретение съемного носителя для служебных целей возможно при разрешении вышестоящего руководителя и АИБа. Пользователь должен **зарегистрировать** приобретенный съемный носитель у АИБа перед его использованием. Использование незарегистрированных в установленном порядке у АИБа съемных носителей информации **запрещено**.

7.2.4. Пользователю запрещается передавать используемые съемные носители информации посторонним лицам или другим пользователям без согласования непосредственного руководителя.

8. Работа с мобильными устройствами

8.1. **Общие правила работы с мобильными устройствами**

8.1.1. Пользователям **запрещается** подключение к локальной сети (компьютеру) личных мобильных устройств и их использование для работы с информацией ограниченного доступа.

8.1.2. Смартфоны и мобильные телефоны запрещается использовать для работы с конфиденциальной информацией.

8.1.3. **Запрещается** включать порты мобильного устройства, работающие на основе технологий беспроводной связи (IrDA, Wi-Fi, Bluetooth и WiMAX), подключать мобильные устройства к сетям сторонних юридических лиц и сетям общего пользования (в том числе Интернет). Запрещается оставлять персональные компьютеры (КПК), сотовые телефоны и другие мобильные устройства на столах и прочих местах открытого доступа без присмотра.

9. Ответственность за нарушение требований информационной безопасности

9.1. Контроль и мониторинг соблюдения настоящих Правил и требований информационной безопасности осуществляется АИБом в соответствии с установленными процедурами. АИБ имеет право проверять

выполнение и требовать соблюдения пользователями настоящих Правил.

9.2. **По всем фактам** нарушения пользователями настоящих Правил и требований информационной безопасности АИБ **проводится детальное служебное расследование**, результаты которого доводятся до непосредственного руководителя пользователя, а также до вышестоящего руководителя. По результатам расследования может быть принято решение о привлечении пользователя, допустившего нарушение, к ответственности в соответствии с Правилами внутреннего трудового распорядка и Трудовым кодексом Российской Федерации. Порядок принятия такого решения определяется Трудовым кодексом РФ и внутренними нормативными актами.

Приложение № 1

Общие правила пользования, учета и хранения ключей от шкафов, тумбочек и прочих запирающихся устройств

1. Все устройства хранения (шкафы, тумбочки, сейфы и пр.) должны быть закрыты на ключ по завершении рабочего дня. Устройства хранения конфиденциальной информации должны быть закрыты на ключ и открываться только для получения или помещения на хранения документов.

2. Руководителем подразделения назначаются ответственные (не менее двух пользователей (основной, дублер)) за хранение ключей от общих устройств хранения (шкафы, сейфы), а также за хранение запасных (дубликатов) ключей от индивидуальных устройств хранения (тумбочки) пользователей подразделения. Пользователи, являющиеся материальными ответственными, уведомляются о назначении ответственных пользователей служебной запиской с темой: «О пользователях, ответственных за учет и хранение дубликатов ключей от общих и индивидуальных устройств хранения».

3. Запасные экземпляры ключей должны храниться в запечатанных конвертах в закрытом на ключ шкафу или, что предпочтительно, сейфе. Ответственные пользователи ведут журнал учета ключей, фиксируют события получения ключей от пользователей, являющихся материальными ответственными, выдачи пользователям и сдачи пользователями (при переходе, увольнении), утери и т.д. Ключ от шкафа хранения запасных ключей может быть передан только дублеру в период отсутствия ответственного. При получении нового устройства хранения, ключи передаются пользователям под роспись, а дубликаты размещаются в шкафу хранения в установленном порядке.

4. Основные экземпляры ключей для индивидуального устройства (устройств) хранения выдаются пользователю под роспись ответственным пользователей. Ключ должен всегда находиться у владельца, и не может быть передан другому пользователю.

5. Оставлять ключ в местах общего доступа запрещается.

6. Если пользователь забыл основный экземпляр ключа, то ответственный пользователь, получив сообщение о необходимости предоставления запасного ключа, предоставляет ключ пользователю, удостоверив его личность. При этом запасной ключ не может быть оставлен у пользователя, а должен быть возвращен им на место хранения. В случае если последовательно в течение трех рабочих дней пользователь инициирует процедуру запроса запасного ключа, то ключ считается утерянным.

7. В случае потери ключа пользователь, потерявший ключ или ключ которого считается утерянным, оформляет объяснительную записку с указанием причины утери ключа. После получения объяснительной записки об утере ключа, материально ответственный пользователь должен в течение двух недель заменить замок (в любом случае, даже при наличии дубликата). Новые

два ключа (основной ключ и дубликат) выдаются ответственному пользователю на учет и хранение ключей, после чего основной экземпляр ключа для индивидуального устройства (устройств) хранения выдается пользователю в установленном порядке.

8. Руководитель пользователя должен сразу при получении информации об утере ключа установить, хранится ли в данном устройстве конфиденциальная информация. В случае положительного ответа обеспечить перенос конфиденциальной информации в другое устройство хранения.

9. В случае перехода пользователя внутри организации или при увольнении, ключи от персональных устройств хранения должны быть сданы ответственному пользователю.

Лист ознакомления
с Правилами соблюдения требований по информационной безопасности в ГИС

Должность	И. О. Фамилия	Подпись	Дата