ПРИЛОЖЕНИЕ № 6
к распоряжению Межрайонного управления № 2
от « 2 » мая 2023 г. № 27/ру-о

**Инструкция пользователя информационные системы Межрайонного управления № 2**

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Пользователем информационная система (далее – Пользователь) является уполномоченный сотрудник Межрайонного управления № 2 (далее – Управление).

1.2. Пользователь должен знать нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну (далее – защищаемая информация).

1.3. В своей деятельности, связанной с обработкой защищаемой информации, Пользователь руководствуется Политикой в отношении обработки персональных данных в Межрайонном управлении № 2 и настоящей Инструкцией.

1.4. Пользователи, участвующие в рамках своих функциональных обязанностей в процессах автоматизированной обработки защищаемой информации и имеющие доступ к аппаратным средствам, программному обеспечению и обрабатываемой защищаемой информации, несут персональную ответственность за свои действия.

## 2. ОБЯЗАННОСТИ И ПРАВА ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

2.1. Пользователь обязан:

– соблюдать требования Политики в отношении обработки персональных данных в Межрайонном управлении № 2 и иных локальных актов Управления, устанавливающих порядок работы с защищаемой информацией;

– выполнять в информационные системы (далее – ИС) только те процедуры, которые необходимы для исполнения его должностных обязанностей;

– использовать для выполнения должностных обязанностей только предоставленное ему автоматизированное рабочее место (далее – АРМ) на базе персонального компьютера;

– пользоваться только зарегистрированными в установленном порядке съемными (отчуждаемыми) машинными носителями информации;

– обеспечивать безопасное хранение вышеуказанных материальных носителей информации, исключающее несанкционированный доступ к ним;

– немедленно сообщать руководителю структурного подразделения и (или) ответственному за защиту информации, не содержащей сведения, составляющие государственную тайну, в информационные системы Межрайонного управления № 2 (далее – Ответственный) о нештатных ситуациях, фактах и попытках несанкционированного доступа к обрабатываемой информации, о блокировании, исчезновении (искажении) защищаемой информации;

– перед началом обработки в ИС файлов, хранящихся на съемных машинных

носителях информации, осуществлять проверку файлов на наличие компьютерных вирусов;

– располагать экран монитора в помещении во время работы так, чтобы исключалась возможность ознакомления с отображаемой на нем информацией посторонними лицами;

– соблюдать установленный режим разграничения доступа к информационным ресурсам: получать пароль, надежно его запоминать и хранить в тайне.

2.2. Пользователям ИС запрещается:

– записывать и хранить защищаемую информацию на неучтенных материальных носителях информации;

– оставлять во время работы материальные носители информации без присмотра, несанкционированно передавать материальные носители информации другим лицам и выносить их за пределы помещения, в котором производится обработка защищаемой информации;

– отключать средства антивирусной защиты;

– отключать (блокировать) средства защиты информации;

– производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;

– самостоятельно устанавливать, тиражировать или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

– обрабатывать в ИС информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам ИС;

– сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам в ИС;

– работать в ИС при обнаружении каких-либо неисправностей;

– хранить на учтенных носителях информации программы и данные, не относящиеся к рабочей информации;

– вводить в ИС защищаемую информацию под диктовку или с микрофона;

– привлекать посторонних лиц для производства ремонта технических средств ИС без согласования с Ответственным.

2.3. Пользователь имеет право знакомиться с внутренними документами Управления, регламентирующими его обязанности по занимаемой должности.

## 3. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ ПО ПАРОЛЬНОЙ ЗАЩИТЕ

3.1. Пользователям запрещается:

– записывать свои пароли в очевидных местах, таких как внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.;

– хранить пароли в записанном виде на отдельных листах бумаги;

– сообщать свои пароли посторонним лицам, а также сведения о применяемых средствах защиты от несанкционированного доступа.

3.2. Плановую смену паролей Пользователь осуществляет при истечении максимального срок действия пароля или заблаговременно до наступления окончания срока действия пароля.

3.3. При обнаружении фактов утраты, компрометации (подозрении на компрометацию) ключевой, парольной и аутентифицирующей информации Пользователь обязан незамедлительно сообщить об этом Ответственному.

3.4. Внеплановая смена личного пароля Пользователем должна производиться в следующих случаях:

– компрометации (подозрении на компрометацию) пароля;

– по инициативе Пользователя;

– по инициативе Ответственного.

## 4. ТЕХНОЛОГИЯ ОБРАБОТКИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

4.1. При первичном допуске к работе с ИС Пользователь:

– проходит инструктаж по использованию ИС;

– знакомится с требованиями локальных актов, регламентирующих обработку и обеспечение безопасности защищаемой информации;

– получает у сотрудник, выполняющего функции по управлению (администрированию) системой защиты информации, идентификатор и начальную аутентификационную информацию (пароль) для входа в ИС.

4.2. Перед началом работы Пользователь визуально проверяет целостность пломб, убеждается в отсутствии посторонних технических средств, включает необходимые средства вычислительной техники.

4.3. Авторизацию в ИС (ввод личного идентификатора и пароля) Пользователь осуществляет при отсутствии в помещении посторонних лиц.

4.4. В процессе работы на АРМ ИС Пользователь использует технические средства и установленное Ответственным программное обеспечение согласно Техническому паспорту ИС.

4.5. Копирование защищаемой информации на машинные носители информации осуществляется только при наличии производственной необходимости и только на учтенные машинные носители информации.

4.6. При необходимости создания на АРМ Пользователя дополнительных электронных документов, содержащих защищаемую информацию, Пользователь создает и хранит такие документы в строго отведенном для этого месте.

4.7. Печать документов, содержащих защищаемую информацию, осуществляется только при наличии производственной необходимости на принтер, подключенный Ответственным к АРМ Пользователя. Распечатанные черновые бумажные варианты вновь создаваемых документов, содержащих защищаемую информацию, уничтожаются с применением уничтожителей бумаги незамедлительно после подписания (утверждения) окончательного варианта документа.

4.8. В случае возникновения необходимости временно покинуть рабочее помещение во время работы в ИС, Пользователь обязан выключить компьютер либо заблокировать его. Разблокирование компьютера производится набором пароля разблокировки, который был создан при настройке системы блокировки АРМ. При отсутствии в покидаемом помещении других служащих Управления, Пользователь обязан закрыть дверь помещения на ключ или другой используемый ограничитель доступа.

4.9. Покидая рабочее помещение в конце рабочего дня, Пользователь обязан выключить все необходимые средства вычислительной техники и закрыть дверь помещения на ключ.