ПРИЛОЖЕНИЕ № 3
к приказу Министерства природных ресурсов и
экологии Новосибирской области
от «18» декабря 2024 г. № 1604-ПА

ИНСТРУКЦИЯ
пользователя информационных систем Министерства природных ресурсов и экологии Новосибирской области

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Инструкция пользователя информационных систем Министерства природных ресурсов и экологии Новосибирской области (далее – Инструкция) определяет функциональные обязанности, права и ответственность пользователей информационных систем (далее – ИС) Министерства природных ресурсов и экологии Новосибирской области (далее – МПР НСО).

1.2. Пользователями ИС МПР НСО (далее - Пользователь) являются уполномоченные сотрудники МПР НСО, осуществляющие обработку информации, содержащейся в ИС МПР НСО, или использующие результаты функционирования ИС МПР НСО согласно Перечню информационных систем Министерства природных ресурсов и экологии Новосибирской области.

1.3. Настоящая Инструкция подготовлена с учетом требований нормативно-методических документов Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России) и Федеральной службы безопасности Российской Федерации (далее – ФСБ России) по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – защищаемая информация), обрабатываемой с использованием средств автоматизации.

1.4. Пользователь в своей работе руководствуется настоящей Инструкцией, нормативными правовыми актами и методическими документами ФСТЭК России, ФСБ России и внутренними документами МПР НСО, регламентирующими вопросы обработки и защиты информации.

1.5. В настоящей Инструкции используются следующие понятия и определения:

1.5.1. Автоматизированное рабочее место – объект вычислительной техники, созданный на базе автономных средств вычислительной техники с необходимым для решения конкретных задач периферийным оборудованием.

1.5.2. Инцидент информационной безопасности – непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (может привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).

1.5.3. Компрометация пароля – утрата доверия к тому, что используемый пароль обеспечивает безопасность информации. К событиям, приводящим к компрометации пароля, относятся следующие события (включая, но не ограничиваясь) – несанкционированное сообщение пароля другому лицу; утрата бумажного или машинного

носителя информации, на котором был записан пароль; запись пароля на бумажном, машинном, ином носителе информации, доступ к которому не контролируется.

1.5.4. Конфиденциальность информации – обязательное для соблюдения лицом, получившим доступ к информации, требование не допускать ее распространение без наличия иного законного основания.

1.5.5. Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

1.5.6. Несанкционированный доступ к информации – доступ к информации с нарушением установленных прав доступа, приводящий к нарушению конфиденциальности информации, к утечке, искажению, подделке, уничтожению, блокированию доступа к информации.

1.5.7. Средство защиты информации – программные, программно-аппаратные, аппаратные средства, предназначенные и используемые для защиты информации в ИС.

1.5.8. Пользователь ИС – лицо, которому разрешено выполнять определенные действия (операции) по обработке информации в ИС или использующее результаты ее функционирования.

2. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

2.1. Пользователь ИС МПР НСО обязан:

2.1.1. Знать и выполнять требования:

– настоящей Инструкции;

– положения локальных актов МПР НСО;

– нормативных правовых актов действующего законодательства Российской Федерации в области обработки и защиты информации, к которой он допущен в рамках выполнения своих должностных обязанностей при работе в ИС.

2.1.2. Добросовестно и в срок исполнять свои функциональные обязанности, в отведенное время решать поставленные задачи в соответствии с предоставленными полномочиями доступа к ресурсам ИС.

2.1.3. Выполнять при работе в ИС только те процедуры, которые необходимы для исполнения его должностных обязанностей.

2.1.4. Использовать для выполнения должностных обязанностей только предоставленное ему в служебных целях автоматизированное рабочее место (далее – АРМ).

2.1.5. Располагать средства отображения (монитор (экран) АРМ, принтер/многофункциональное устройство и т.п.), используемые для работы с защищаемой информацией, таким образом, чтобы исключить возможность визуального просмотра выводимой защищаемой информации посторонними лицами. Осуществлять вывод на печать обрабатываемой защищаемой информации исключительно в целях исполнения должностных обязанностей.

2.1.6. Использовать для хранения и передачи защищаемой информации только зарегистрированные в установленном порядке съемные (отчуждаемые) машинные носители информации.

2.1.7. Обеспечивать безопасное хранение вышеуказанных материальных носителей информации, исключающее несанкционированный доступ к ним.

2.1.8. Перед началом обработки в ИС файлов, полученных из внешних источников (съемных машинных носителей информации, загруженных из сетей общего пользования и других внешних источников), осуществлять проверку файлов на наличие компьютерных вирусов.

2.1.9. Соблюдать конфиденциальность защищаемой информации, ставшей ему известной во время выполнения служебных (трудовых) обязанностей или иным путем. Не предоставлять защищаемую информацию третьим лицам и не распространять защищаемую информацию, если иное не предусмотрено федеральным законом. Пресекать действия других лиц, которые могут привести к нарушению конфиденциальности защищаемой информации.

2.1.10. Для предотвращения несанкционированного доступа к защищаемой информации и во избежание несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных средств ИС МПР НСО осуществлять блокировку (либо выключение) рабочей станции по окончании сеанса работы или во время перерыва в работе (при отсутствии визуального контроля за рабочей станцией).

2.1.11. При отсутствии в покидаемом помещении, в котором осуществляется обработка защищаемой информации, других сотрудников МПР НСО, обеспечить закрытие помещения на ключ или другой используемый ограничитель доступа.

2.1.12. Соблюдать правила при работе в сетях связи общего пользования, в том числе сетях международного информационного обмена (сети Интернет) (далее – сеть):

– запрещается передавать по сети защищаемую информацию без использования средств криптографической защиты информации;

– запрещается осуществлять нецелевое использование сети в корыстных и/или преступных целях.

2.1.13. Знать и соблюдать правила работы со средствами защиты информации, используемыми в ИС в соответствии с технической и эксплуатационной документацией на применяемые средства защиты информации.

2.1.14. Хранить в тайне персональные пароли доступа в ИС МПР НСО, а также информацию о системе защиты, реализованной в ИС МПР НСО.

2.1.15. Обеспечивать процессы генерации, использования и смены личного пароля с учетом следующих требований:

– длина пароля должна быть не менее восьми символов;

– в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);

– символы паролей должны вводиться в режиме латинской раскладки клавиатуры;

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения и другие данные, которые могут быть подобраны злоумышленником путем анализа информации;

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.

2.1.16. Немедленно ставить в известность лиц, ответственных за защиту информации, в случае:

– утраты носителя с защищаемой информацией и/или при подозрении компрометации паролей доступа;

– нештатных ситуаций, фактах, попытках, причинах или условиях несанкционированного доступа к обрабатываемой информации;

– блокирования, исчезновения (искажения) обрабатываемой информации;

– нарушения целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения попыток несанкционированного доступа к ИС МПР НСО;

– несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИС МПР НСО.

2.1.17. В случае выявления отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), некорректного функционирования установленных в ИС МПР НСО программных и (или) программно-аппаратных средств защиты информации ставить в известность лиц, ответственных за обеспечение функционирования ИС (системных администраторов), и (или) ответственного за защиту информации в МПР НСО в пределах их компетенции в зависимости от характера возникших неполадок.

2.1.18. В случае выявления инцидента информационной безопасности, при возникновении нештатных и аварийных ситуаций принимать меры по реагированию с целью ликвидации их последствий, в пределах своих полномочий, оказывать содействие при проведении работ по восстановлению работоспособности программных и программно-аппаратных средств ИС.

2.1.19. В случае увольнения вернуть все документы и материалы на бумажных и машинных носителях информации, программные и программно-аппаратные средства (в том числе средства защиты информации), относящиеся к ИС МПР НСО, в том числе: отчеты, инструкции, служебную переписку, списки сотрудников, а также все прочие материалы и копии названных материалов, полученные в течение всего периода работы в МПР НСО.

2.1.20. Соблюдать установленный порядок доступа в помещения, в которых размещены ИС МПР НСО и ведется обработка защищаемой информации, контролировать действия лиц, не имеющих права самостоятельного доступа в помещения, в которых размещены ИС МПР НСО и ведется обработка защищаемой информации, расположены технические средства, средства защиты информации и средства обеспечения функционирования ИС.

2.2. Пользователю запрещается:

– передавать кому бы то ни было, устно или письменно, защищаемую информацию, а также атрибуты доступа к ресурсам ИС МПР НСО, открыто осуществлять ввод персонального пароля в присутствии других лиц;

– использовать защищаемую информацию при подготовке открытых публикаций, докладов, научных работ и т.д. (в случае отсутствия законных оснований);

– выполнять работы с документами, содержащими защищаемую информацию, за пределами служебных помещений, выносить их из служебных помещений за пределы контролируемой зоны, снимать копии с документов и других носителей защищаемой информации или производить выписки из таких документов без разрешения ответственного за организацию обработки персональных данных и/или ответственного за защиту информации в МПР НСО, равно как использовать различные технические средства (фото-, видео- и звукозаписывающую аппаратуру) для фиксации сведений, содержащих защищаемую информацию, в целях, не относящихся к исполнению служебных обязанностей;

– оставлять в рабочее время без присмотра материальные носители, содержащие защищаемую информацию, а также оставлять незапертыми хранилища с материальными носителями, содержащими защищаемую информацию, и(или) помещения, в которых осуществляется обработка защищаемой информации, в случае отсутствия в них других сотрудников МПР НСО;

– несанкционированно передавать материальные носители, содержащие защищаемую информацию, другим лицам;

– использовать компоненты программного и аппаратного обеспечения ИС МПР НСО, сети связи в неслужебных целях;

– самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств АРМ или устанавливать программные и аппаратные средства;

– самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств (в том числе отключать (блокировать) средства защиты информации);

– осуществлять обработку защищаемой информации в присутствии посторонних (не допущенных к данной информации) лиц;

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

– хранить на учтенных носителях информации данные, не относящиеся к выполнению служебных (должностных) обязанностей;

– оставлять рабочее место, не активизировав временную блокировку сеанса доступа;

– привлекать посторонних лиц для проведения ремонта или настройки программно-аппаратных средств ИС МПР НСО, не уполномоченных на осуществление указанных действий в соответствии с заключенными соглашениями, договорами, контрактами;

– умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению инцидента информационной безопасности. При обнаружении такого рода ошибок – ставить в известность ответственного за защиту информации в МПР НСО.

3. ПРАВА ПОЛЬЗОВАТЕЛЯ

3.1. Пользователь имеет право:

3.1.1. Требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения своих функциональных обязанностей.

3.1.2. Получать доступ к информации, материалам, техническим средствам, помещениям, необходимым для надлежащего исполнения своих обязанностей.

3.1.3. Вносить своему непосредственному руководителю предложения, касающиеся организации технологического процесса обработки и защиты информации.

3.1.4. Знакомиться с внутренними документами МПР НСО, регламентирующими его обязанности по занимаемой должности.

3.1.5. Для получения консультаций по вопросам обработки защищаемой информации обращаться к ответственному за организацию обработки персональных данных и (или) ответственному за защиту информации в МПР НСО.

3.1.6. Получать разъяснения по вопросам функционирования входящих в состав ИС МПР НСО программных и технических средств общего назначения, а также по вопросам информационной безопасности и использованию средств защиты информации.

4. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЯ

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

4.2. Пользователь несет предусмотренную законодательством Российской Федерации ответственность за:

– неисполнение либо ненадлежащее исполнение должностных обязанностей;

– нарушения в работе ИС МПР НСО, вызванные его неправомерными действиями или неправильным использованием предоставленных прав, предусмотренных настоящей Инструкцией;

– нарушение законодательства Российской Федерации, локальных актов МПР НСО в сфере обработки и обеспечения безопасности информации;

– превышение должностных полномочий и злоупотребление ими;

– применение к МПР НСО штрафных санкций по вине Пользователя;

– совершение противоправных действий (уничтожение, изменение, блокирование, копирование, предоставление, распространение, а также иных неправомерных действий) в отношении информации, к которой он допущен в рамках выполнения своих должностных (функциональных) обязанностей.