|  |  |
| --- | --- |
|  | Приложение 9  УТВЕРЖДЕНО  приказом Контрольно-счетной палаты Республика Карелия  от 27.06.2025 № 61 од |

|  |  |  |
| --- | --- | --- |
|  | **ИНСТРУКЦИЯ**  **пользователя, допущенного к обработке персональных** **данных в информационных системах**  **Контрольно-счетной** **палаты Республики Карелия** |  |

1. Общие положения

Настоящая Инструкция пользователя, допущенного к обработке персональных данных в информационных системах Контрольно-счетной палаты Республики Карелия (далее – Инструкция), разработана на основе приказа Федеральной службы по техническому и экспортному контролю Российской Федерации от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Настоящая Инструкция определяет основные обязанности, права и ответственность пользователей, допущенных к обработке персональных данных в информационных системах Контрольно-счетной палаты Республики Карелия (далее – Контрольно-счетная палата).

Все термины и определения, используемые в настоящих Правилах, соответствуют терминологии принятой в законодательных актах Российской Федерации в сфере защиты персональных данных и в правовых актах Контрольно-счетной палаты Республики Карелия, регламентирующих правила обработки персональных данных субъектов персональных данных в Контрольно-счетной палате Республики Карелия.

Допуск пользователей к обработке персональных данных в информационных системах определяется приказом Председателя Контрольно-счетной палаты.

Пользователь информационной системы руководствуется положениями федеральных законов и нормативных правовых актов органов государственной власти, локальных правовых актов Контрольно-счетной палаты, настоящей Инструкцией.

Контроль за выполнением требований настоящей Инструкции осуществляет ответственный за обработку персональных данных в Контрольно-счетной палате.

2. Обязанности пользователя

При выполнении работ в информационной системе пользователь обязан:

1) строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами информационной системы, правила работы и порядок регистрации в информационной системе, доступа к информационным ресурсам информационной системы;

2) знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте (далее – АРМ);

3) хранить в тайне свои идентификационные данные (имена, пароли и т. д.);

4) осуществлять вход на АРМ только под своими идентификационными данными;

5) хранить в установленным порядком свое индивидуальное устройство идентификации и другие реквизиты разграничения доступа;

6)  немедленно сообщать ответственному за техническое обслуживание информационных систем персональных данных Контрольно-счетной палаты и Председателю Контрольно-счетной палаты о случаях утери индивидуального устройства идентификации или при подозрении о компрометации, личных ключей и паролей, а также при обнаружении нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищённой АРМ, несанкционированных (произведённых с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ, некорректного функционирования установленных на АРМ технических средств защиты, непредусмотренных отводов кабелей и подключённых устройств;

7) присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закреплённого за ним АРМ, ставить в известность ответственного за техническое обслуживание информационных систем персональных данных Контрольно-счетной палаты при необходимости внесения изменения в состав аппаратных и программных средств АРМ;

8) работать в информационной системе только в разрешенный период времени;

9) ставить в известность ответственного за техническое обслуживание информационных систем персональных данных Контрольно-счетной палаты в случае появления сведений или подозрений о фактах несанкционированного доступа к информации, своей или чужой, а также отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств, а также перебоев в системе электроснабжения;

10) осуществлять установленным порядком уничтожение информации, содержащей сведения конфиденциального характера с машинных носителей информации;

Пользователю запрещается:

1) использовать компоненты программного и аппаратного обеспечения АРМ, в том числе и информационных систем в неслужебных целях;

2) самовольно вносить какие-либо изменения в состав, размещение, конфигурацию аппаратно-программных средств информационных систем (в том числе АРМ) или устанавливать дополнительно любые программные и аппаратные средства;

3) осуществлять обработку информации, содержащей сведения конфиденциального характера, в присутствии посторонних (не допущенных к данной информации) лиц;

4) записывать и хранить конфиденциальную информацию на неучтённых носителях информации, в том числе для временного хранения;

5) оставлять включенное без присмотра АРМ, не активизировав временную блокировку экрана и клавиатуры;

6) передавать кому-либо своё индивидуальное устройство идентификации, делать неучтённые копии ключевого носителя, и вносить какие-либо изменения в файлы ключевого устройства идентификации;

7) оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения конфиденциального характера);

8) умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках информационных систем (в том числе средств защиты), которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность ответственного за техническое обслуживание информационных систем персональных данных Контрольно-счетной палаты;

9) осуществлять попытки несанкционированного доступа к ресурсам системы и других пользователей информационной системы, проводить рассылку ложных, беспокоящих или угрожающих сообщений (писем);

10) фиксировать свои учётные данные (пароли, имена, идентификаторы, ключи) на материальных носителях;

11) разглашать ставшую известной в ходе выполнения своих обязанностей информацию, содержащую сведения конфиденциального характера;

12) вносить изменения в файлы, принадлежащие другим пользователям информационной системы.

4. Права пользователя

Пользователь информационной системы имеет право:

1) присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закреплённого за ним АРМ;

2) участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов информационной системы, если данное нарушение произошло под его идентификационными данными;

3) своевременно получать доступ к информационным ресурсам информационных систем, необходимым ему для выполнения своих должностных (функциональных) обязанностей;

4) требовать от ответственного за техническое обслуживание информационных систем персональных данных Контрольно-счетной палаты смены идентификационных данных в случае появления сведений или подозрений на то, что эти данные стали известны третьим лицам.

5. Правила работы в сетях общего доступа

Работа в сетях общего доступа и (или) международного обмена (сети Интернет) (далее – Сеть) на элементах информационных систем, должна производиться при служебной необходимости.

При работе в Сети запрещается:

1) осуществлять работу при отключённых средствах защиты (антивирусной защиты, средств от несанкционированного доступа и т. д.);

2) запрещается загружать из Сети программное обеспечение;

3) запрещается посещение сайтов сомнительной репутации (аморального содержания, содержащие нелегально распространяемое программное обеспечение или иной контент);

4) запрещается нецелевое использование подключения к Сети.

6. Ответственность

Пользователь информационных систем несет персональную ответственность за:

1) ненадлежащее исполнение своих должностных (функциональных) обязанностей, а также сохранность комплекта АРМ, съемных носителей информации, индивидуального средства идентификации и целостность установленного программного обеспечения;

2) разглашение сведений, отнесенных к сведениям конфиденциального характера, и сведений ограниченного распространения, ставших известными ему по роду работы.

Ответственность за нарушение функционирования информационных систем, уничтожение, блокирование, копирование, фальсификацию информации несет пользователь информационных систем, под чьими идентификационными данными было совершено нарушение.

Пользователи информационных систем, виновные в нарушениях, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством Российской Федерации.