УТВЕРЖДЕНО
приказом от «__» _____ 2018г. №_____

Инструкция
пользователя информационной системы персональных данных

1. Общие положения

Настоящая Инструкция устанавливает обязанности пользователя информационной системы персональных данных (далее – СПДн) ГБОУ РК ЦДК (далее – ОУ) по обеспечению безопасности обрабатываемых в ней персональных данных, запреты на действия пользователя в ИСПДн, а также его права и ответственность.

Доступ пользователя к ИСПДн осуществляется в соответствии с перечнем сотрудников, допущенных к обработке персональных данных.

Контроль за выполнением настоящей Инструкции возлагается на ответственного за обеспечение безопасности персональных данных.

Каждый сотрудник подразделения ОУ, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным (в дальнейшем именуемый пользователь), несёт персональную ответственность за свои действия при работе с информационными ресурсами ИСПДн.

2. Обязанности пользователя ИСПДн

Пользователь обязан:

2.1. При работе с документами, содержащими персональные данные, руководствоваться требованиями организационно-распорядительных документов ИСПДн. Строго соблюдать установленные правила обеспечения безопасности персональных данных при работе с программными и техническими средствами ИСПДн.

2.2. Использовать ИСПДн для выполнения служебных задач в соответствии с должностной инструкцией.

2.3. Использовать для доступа к ИСПДн собственную уникальную учетную запись (логин) и пароль.

2.4. Хранить в тайне пароли и PIN-коды, обеспечивать физическую сохранность ключевого носителя доступа к ИСПДн.

2.5. Не допускать при работе с ИСПДн просмотр посторонними лицами персональных данных, отображаемых на дисплее АРМ.

2.6. Блокировать экран дисплея АРМ парольной заставкой при оставлении рабочего места.

2.7. По всем вопросам, связанным с обеспечением защиты персональных данных, содержащихся в базах данных, и работе со средствами защиты информации, возникающими при работе в ИСПДн, обращаться к администратору информационной безопасности.

2.8. Немедленно прекращать обработку персональных данных и ставить в известность администратора информационной безопасности при подозрении компрометации пароля, а также при обнаружении:

- нарушений целостности пломб, наклеек на ПЭВМ (персональные электронно-вычислительные машины), при наличии таковых, или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД);
- несанкционированных изменений в конфигурации программных или аппаратных средств АРМ;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования АРМ;

– непредусмотренных конфигурацией АРМ отводов кабелей и подключенных устройств.

2.9. Немедленно информировать ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн в случае обнаружения попыток несанкционированного доступа к ИСПДн.

2.10. Немедленно информировать сотрудников, осуществляющих сетевое администрирование ОУ, при появлении сообщений от программного обеспечения антивирусной защиты о возможном вирусном заражении АРМ или возникновении неисправностей (сбоев) в работе сервисов и информационных ресурсов ОУ.

3. Действия, запрещенные пользователю ИСПДн

Пользователю ИСПДн запрещается:

3.1. Предоставлять доступ к информации, содержащей персональные данные, лицам, не допущенным к их обработке.

3.2. Записывать пароль на любые носители, в том числе бумажные.

3.3. Сообщать (или передавать) посторонним лицам личные ключи или атрибуты доступа к ресурсам ИСПДн.

3.4. Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

3.5. Работать с персональными данными в присутствии посторонних (не допущенных к данной информации) лиц.

3.6. Самостоятельно изменять конфигурацию аппаратно-программных средств ИСПДн.

3.7. Осуществлять действия по преодолению установленных ограничений на доступ к ИСПДн.

3.8. Отключать или изменять конфигурацию средств защиты информации ИСПДн.

3.9. Устанавливать на АРМ программное обеспечение, не связанное с исполнением служебных обязанностей.

4. Права пользователя ИСПДн

Пользователь ИСПДн имеет право:

4.1. Получать помощь по вопросам эксплуатации ИСПДн от ответственного за систему защиты информации (далее – СЗИ) ИСПДн.

4.2. Обращаться к сотрудникам, осуществляющим сетевое администрирование ОУ, по вопросам дооснащения АРМ техническими и программными средствами, не входящими в штатную конфигурацию АРМ и ИСПДн, необходимыми для автоматизации деятельности в соответствии с возложенными на него должностными обязанностями.

4.3. Подавать сотрудникам, осуществляющим сетевое администрирование ОУ, предложения по совершенствованию функционирования ИСПДн.

5. Ответственность пользователя ИСПДн

Пользователь ИСПДн несет ответственность за:

5.1. Обеспечение безопасности персональных данных при их обработке в ИСПДн.

5.2. Нарушение работоспособности или вывод из строя системы защиты ИСПДн.

5.3. Преднамеренные действия, повлекшие модификацию или уничтожение персональных данных в ИСПДн, и несанкционированный доступ к персональным данным в ИСПДн.

5.4. Разглашение персональных данных.

5.5. Пользователь, имеющий расширенные права «Опытный пользователь» или «Администратор», несет ответственность за корректное функционирование прикладного программного обеспечения ИСПДн.

5.6. За нарушение настоящей Инструкции к пользователю могут применяться меры дисциплинарного воздействия.

6. Правила работы в информационно-телекоммуникационных сетях международного информационного обмена

6.1. Работа в информационно-телекоммуникационных сетях международного информационного обмена – сети Интернет и других (далее – Сеть) на элементах ИСПДн должна проводиться только при служебной необходимости.

6.2. При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирусных и других);
- передавать по Сети защищаемую информацию без использования средств шифрования;
- скачивать из Сети программное обеспечение и другие файлы в неслужебных целях;
- посещать сайты сомнительной репутации (сайты, содержащие нелегально распространяемое программное обеспечение (ПО), сайты знакомств, онлайн игры и другие).

7. Перечень нормативных документов, использованных при разработке данного порядка

7.1. Регламент по проведению контрольных мероприятий и реагированию на инциденты информационной безопасности (Инструкция пользователя на случай возникновения внештатных ситуаций).

7.2. Инструкция администратора информационной безопасности.

7.3. Разрешительная система доступа к персональным данным, содержащимся в базах данных ИСПДн.

7.4. Инструкция по использованию паролей.

7.5. Порядок резервирования и восстановления работоспособности технических средств (ТС) и программного обеспечения (ПО), баз данных и системы защиты информации (СЗИ).