Приложение № 13

к приказу Управления финансов Администрации

муниципального района «Заполярный район»

от 20.05.2016 № 15

**Положение об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных**

I. Общие положения

1. Настоящее Положение об организации и проведении работ в Управлении финансов Администрации Заполярного района (далее – Управление) по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее - Положение) принято в целях обеспечения безопасности персональных данных (далее - ПДн) при их обработке в информационных системах персональных данных (далее - ИСПДн).

ИСПДн, которые используются в Управлении, утверждаются в Перечне информационных систем персональных данных в Управлении финансов Администрации Заполярного района. В указанном акте определяются структурные подразделения, работники которых имеют право доступа к ИСПДн.

2. Безопасность персональных данных при их обработке в ИСПДн Управлении обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

3. Самостоятельное подключение средств вычислительной техники, применяемых для хранения, обработки или передачи ПД, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к информационно-телекоммуникационной сети Интернет, не допускается.

II. Порядок работы персонала ИСПДн в части

обеспечения безопасности ПДн при их обработке в ИСПДн

4. Настоящий порядок работы определяет действия персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

5. Допуск пользователей для работы на персональной электронной вычислительной машине (далее - ПЭВМ), на которой установлена ИСПДн, осуществляется отделом информатизации, автоматизации и технического обслуживания Администрации Заполярного района исходя из Перечня информационных систем персональных данных в Управлении финансов.

6. Вход пользователя в ИСПДн должен осуществляться по персональному паролю (проходить процедуру идентификации и аутентификации).

7. Все магнитные, оптические и другие машинные носители ПДн подлежат обязательному учету.

Все автоматизированные рабочие места (ПЭВМ сотрудников Управления), на которых установлены ИСПДн, включаются только с использованием персонального пароля.

8. При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на ПЭВМ. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование.

9. Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

- хранить в тайне свой пароль (пароли);

- хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу).

10. Каждый сотрудник Управления обязан немедленно известить начальника Управления и начальника отдела информатизации, автоматизации технического обслуживания Администрации Заполярного района в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;

- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ПЭВМ, выхода из строя или неустойчивого функционирования узлов ПЭВМ или периферийных устройств, а также перебоев в системе электроснабжения;

- некорректного функционирования установленных на ПЭВМ технических средств защиты;

- непредусмотренных отводов кабелей и подключенных устройств.

11. Пользователю ПЭВМ категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения ПЭВМ в неслужебных целях;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения ПЭВМ;

- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;

- записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных электронных носителях информации;

- оставлять включенной без присмотра ПЭВМ, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);

- оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, электронные носители и распечатки, содержащие защищаемую информацию;

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

- размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации.

III. Порядок обучения персонала практике работы в ИСПДн

12. Обучение практике и методике работы в ИСПДн должно быть непрерывным, систематическим.

13. Обучение по методике делятся:

- на обучающие занятия;

- методическую помощь и практические занятия на месте.

14. Обучающие занятия по работе в ИСПДн проводятся сотрудниками отдела информатизации, автоматизации и технического обслуживания Администрации Заполярного района с пользователями ИСПДн при поступлении на работу сотрудника в соответствующий отдел Управления, где происходит обработка персональных данных в ИСПДн.

Обучающие занятия по работе в ИСПДн могут проводится сотрудниками организации, по лицензионному договору с которой Управление использует ИСПДн, без доступа к персональным данным, содержащимся в ИСПДн сотрудников такой организации.

15. При возникновении проблем, вопросов по работе в ИСПДн пользователи ПЭВМ обращаются только к сотрудникам отдела информатизации, автоматизации и технического обслуживания Администрации Заполярного района.

IV. Правила антивирусной защиты

16. К использованию на ПЭВМ допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств, сертифицированные ФСТЭК России.

17. Установка и начальная настройка средств антивирусного контроля на ПЭВМ осуществляется сотрудниками отдела информатизации, автоматизации и технического обслуживания Администрации Заполярного района.

18. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, CD-ROM, другие). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

19. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

20. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках) пользователь обращается к сотрудникам отдела информатизации, автоматизации и технического обслуживания Администрации Заполярного района для проведения проверки на наличие вирусов.

21. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить обработку данных в ИСПДн;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности, специалиста по защите информации, владельца зараженных файлов, а также смежные отделы, использующие эти файлы в работе;

- совместно с владельцем провести анализ зараженных вирусом файлов и выявить возможность дальнейшего их использования;

- провести лечение или уничтожение зараженных файлов.

22. Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями настоящего Положения возлагается на начальника отдела информатизации, автоматизации и технического обслуживания Администрации Заполярного района.

V. Обмен персональными данными

21. Обмен персональными данными при их обработке в ИСПДн осуществляется по каналам связи, защита которых обеспечивается путем реализации организационных мер и путем применения программных и технических средств.

22. Обмен ПД при их обработке в ИСПДн возможен с лицом, которое в силу закона либо согласия субъекта ПД, вправе обрабатывать такие данные.

VI. Правила допуска и доступа к персональным данным третьих лиц

23. Допуск к Пд, в том числе содержащимся в ИСПДн сторонних организаций, деятельность которых не связана с исполнением функций Управлением, регламентируется законодательством Российской Федерации, контрактами (договорами, соглашениями) и другими нормативными правовыми актами Российской Федерации.

24. Доступ к техническим (программно-техническим) средствам ИСПДн Управления предоставляется сторонним организациям, выполняющим работы на договорной основе.

Порядок допуска указанных организаций определяется в муниципальном контракте на выполнение работ (оказание услуг). Решением о допуске является подписанный в установленном порядке муниципальный контракт на выполнение работ (оказание услуг).

25. Доступ к ПД сторонних организаций осуществляется на основании письменных запросов или письменных соглашений (договоров) сторон об обмене информацией.

В письменном запросе (соглашении, договоре) должны быть указаны следующие сведения:

- цель получения информации;

- конкретное наименование информации (состав персональных данных);

- способ доступа (предоставления), а также сведения о регистрации в уполномоченных органах по защите прав субъектов персональных данных, осуществляющих функции по контролю и надзору в сфере информационных технологий и связи.

26. Запрещается передача электронных копий баз (банков) данных, содержащих персональные данные, любым сторонним организациям, за исключением случаев, предусмотренных законодательством Российской Федерации.