|  |  |
| --- | --- |
|  | Приложение № 9  УТВЕРЖДЕНА  приказом департамента государственного регулирования цен и тарифов Костромской области  от « 29 » декабря 2021 года № 95-К |

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ

ответственного за организацию обработки персональных

данных в департаменте государственного регулирования

цен и тарифов Костромской области

Глава 1. Общие положения

1. Объекты вычислительной техники (ОВТ) разрешается использовать для обработки персональных данных при соблюдении следующих условий:

1. право работать на ОВТ предоставляется Администратору информационной безопасности и пользователям;

2) каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ОВТ, несет персональную ответственность за свои действия.

Глава 2. Обязанности пользователя ОВТ

2. Выполнять на ОВТ только те действия, которые определены для него в Разрешительной системе доступа к информационным (программным) ресурсам объекта вычислительной техники - автоматизированное рабочее место на базе автономной ПЭВМ.

3. Знать и соблюдать установленные требования по защите персональных данных, учету, хранению и пересылке машинных носителей информации, а также руководящих и организационно-распорядительных документов на данный ОВТ.

4. Пользователи перед началом обработки на ОВТ файлов, хранящихся на съемных носителях информации, должны осуществить проверку файлов на наличие компьютерных вирусов. Антивирусный контроль ОВТ должен осуществляться пользователем не реже одного раза в неделю.

5. Экран видеомонитора в помещении располагать во время работы так, чтобы исключать возможность ознакомления с отображаемой на них информацией посторонними лицами, шторы на окнах проемах должны быть завешаны (жалюзи закрыты).

6. Соблюдать установленный режим разграничения доступа к информационным ресурсам: получать у Администратора информационной безопасности (АИБ) пароль, надежно его запоминать и хранить в тайне.

7. Немедленно докладывать АИБ обо всех фактах и попытках несанкционированного доступа (НСД) к обрабатываемой на ОВТ информации или об ее исчезновении (искажении).

8. Пользователям ОВТ запрещается:

1. записывать и хранить информацию на неучтенных носителях информации (НИ);
2. оставлять во время работы магнитные НИ (или ОВТ с НИ) без присмотра, передавать их другим лицам и выносить за пределы помещения, в котором разрешена обработка информации;
3. отключать (блокировать) средства защиты информации, предусмотренные организационно распорядительными документами на данный ОВТ;
4. производить какие-либо изменения в электрических сетях, монтаже и размещении технических средств;
5. самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменить установленный алгоритм функционирования технических и программных средств;
6. обрабатывать на ОВТ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам обработки информации;
7. сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам ОВТ;
8. производить копирование дискет, отдельных файлов с учетом НИ на неучтенные НИ, в том числе для временного хранения информации;
9. работать на ОВТ при обнаружении каких-либо неисправностей;
10. хранить НИ вблизи сильных источников электромагнитных изучений и прямых солнечных лучей;
11. хранить на учтенных НИ программы и данные, не относящиеся к рабочей информации;
12. привлекать посторонних лиц для производства ремонта ОВТ.

Глава 3. Организация парольной защиты при работе   
на объектах информатизации

9. Личные пароли доступа к объекту информатизации, системе защиты от НСД, выдаются пользователям АИБ, и при этом необходимо руководствоваться следующими требованиями:

1. длина пароля должна быть не менее 6-ти буквенно-цифровых символов;
2. пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименование АРМ, общепринятые сокращения (ЭВМ, ЛВС, USER, SYSOP, GUEST, ADMINISTRATOR и т.д.), и другие данные, которые могут быть подобраны злоумышленником путем анализа информации   
   об ответственном исполнителе;
3. не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
4. не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например: 1234567   
   и т.п.);
5. при смене пароля новое значение должно отличаться   
   от предыдущего не менее чем в 4 позициях;
6. в числе символов пароля, обязательно должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры;
7. не использовать ранее использованные пароли.

10. Лица, использующие паролирование, обязаны:

1) четко знать и строго выполнять требования настоящей инструкции и других руководящи документов по паролированию;

2) своевременно сообщать АИБ о всех нештатных ситуациях, нарушениях работы подсистем защиты от НДС, возникающих при работе с паролями.

11. При организации парольной защиты запрещается:

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

2) хранить пароли в записанном виде на отдельных листах бумаги;

3) сообщать посторонним лицам свои пароли, а также сведения о применяемой системе защиты от НСД.

Глава 4. Порядок применения парольной защиты

12. Полная плановая смена пароля на ОВТ проводится не реже одного раза в год.

13. Удаление (в т.ч. внеплановая смена) личного пароля любого пользователя ОВТ должна производиться в следующих случаях:

1) в случае подозрения на дискредитацию пароля;

2) по окончании срока действия;

3) в случае прекращения полномочий (увольнение, переход на другую работу внутри организации) пользователя после окончания последнего сеанса работы данного с системой;

4) по указанию АИБ.

14. Смена пароля осуществляется АИБ.

15. Для предотвращения доступа к персональным данным, находящейся в ПЭВМ, минуя ввод пароля, пользователь во время перерыва в работе обязан осуществлять блокирование системы нажатием комбинации Ctr1+Alt+1 или кнопки «Блокировать».

Порядок применения (смены) пароля при работе на ПЭВМ, оборудованных системой защиты от НСД, приведен в эксплуатационной документации на СЗИ.

Глава 5. Технология обработки персональных данных

16. При первичном доступе к работе на ОВТ пользователь знакомится с требованиями руководящих, нормативно-методических и организационно-распорядительных документов по вопросам автоматизированной обработки информации, изучает инструкцию пользователя системы защиты СКЗИ «ViPNet», получает персональный идентификатор или личный текущий пароль у АИБ.

17. В процессе работы пользователь производит обработку персональных данных на ОВТ под управлением операционной системы Windows 8,10 с применением следующих программных обеспечений:

1) ИС ССТУ «Обращения граждан»;

2) федеральная государственная информационная система «Единая информационная система управления кадровым составом государственной гражданской службы Российской Федерации»;

3) АС \_Смета\_Тонкий клиент.

18. При необходимости выводов персональных данных из ОВТ осуществляется следующим образом:

1. копированием персональных данных на учтенные носители;
2. печать на принтере;
3. передача персональных данных по каналам связи   
   с обязательным применением криптографической защиты.