УТВЕРЖДАЮ
Начальник управления
ветеринарии Ростовской области

С.Н. Карташов

« 23 » мая 2013 г.

ИНСТРУКЦИЯ

администратора безопасности информационных систем персональных данных управления ветеринарии Ростовской области

1. Общие положения

Данная Инструкция является руководящим документом администратора информационной безопасности (далее - ИБ) систем персональных данных управления ветеринарии Ростовской области (далее – управление).

Требования настоящей инструкции должны выполняться во всех режимах функционирования управления.

Требования администратора ИБ, связанные с выполнением им своих функций, обязательны для исполнения всеми сотрудниками управления.

Персональные данные относятся к категории информации ограниченного доступа.

Наиболее вероятными каналами утечки информации для информационных систем персональных данных (далее - ИСПДн) являются:

- несанкционированный доступ к информации, обрабатываемой в ИСПДн;
- хищение технических средств с хранящейся в них информацией или отдельных носителей информации;
- просмотр информации с экранов дисплеев мониторов и других средств ее отображения с помощью оптических устройств;
- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности обмена, в том числе электромагнитного, через специально внедренные электронные и программные средства («закладки»).

Работа с персональными данными (ПДн) строится на следующих принципах:

- принцип персональной ответственности – в любой момент времени за каждый документ (не зависимо от типа носителя: бумажный, электронный) должен отвечать и распоряжаться конкретный работник, выдача документов осуществляется только под роспись;
- принцип контроля и учета – все операции с документами должны отражаться в соответствующих журналах и карточках (передача из рук в руки, снятие копии и т.п.).

2. Назначение администратора безопасности

На должность администратора ИБ назначается лицо из числа наиболее квалифицированных пользователей ПЭВМ, либо имеющим образование в области защиты информации.

Администратор ИБ в вопросах защиты информации взаимодействует непосредственно с ответственным за обработку персональных данных в управлении.

3. Обязанности администратора безопасности

В своей повседневной деятельности администратор ИБ руководствуется данной инструкцией и другими документами, регламентирующими защиту персональных данных, эксплуатационной документацией на установленные средства защиты от несанкционированного доступа к информации.

Администратор ИБ:

- обеспечивает поддержку подсистем управления доступом, регистрации и учета информационных ресурсов;
- контролирует целостность программно-аппаратной среды, хранимой и обрабатываемой информации;
- контролирует доступность и конфиденциальность хранимой, обрабатываемой и передаваемой по каналам связи информации (устойчивое функционирование ЛВС и ее подсистем);
- обеспечивает доступ к защищаемой информации пользователям согласно их прав доступа.

На администратора ИБ возлагаются следующие обязанности:

- следить за сохранностью наклеек с защитной и идентификационной информацией на корпусах ПЭВМ;
- знать уровень конфиденциальности обрабатываемой информации и класс ИСПДн, следить за тем, чтобы обработка информации производилась только с использованием учтенных съемных носителей информации;
- контролировать соблюдение требований по учету и хранению носителей конфиденциальной информации и персональных данных;
- незамедлительно докладывать ответственному за обработку персональных данных в управлении, обо всех выявленных попытках несанкционированного доступа к информации ограниченного доступа;
- контролировать правильность применения пользователями сети средств защиты информации;
- участвовать в испытаниях и проверках ИСПДн;
- осуществлять контроль монтажа оборудования специалистами сторонних организаций;
- обобщать результаты своей деятельности и готовить предложения по ее совершенствованию;
- при изменении конфигурации автоматизированной системы вносить соответствующие изменения в паспорт ИСПДн, обрабатывающей информацию ограниченного доступа;
- вести журнал учета проводимых работ.

Регистрации в журнале учета работ ИСПДн подлежат:

- обновление программного обеспечения ИСПДн;
- обновление антивирусных баз;
- вскрытие системного блока с целью модернизации или ремонта с указанием цели вскрытия и проводимых работ;
- замена системного блока с указанием факта гарантированного удаления информации с жесткого магнитного диска;
- отклонения в нормальной работе системных и прикладных программных средств затрудняющих эксплуатацию рабочей станции;
- выход из строя или неустойчивое функционирование узлов ПЭВМ или периферийных устройств, принтера и т.п.

При выявлении утечки информации администратор обязан немедленно прекратить работы в ИСПДн.

При выявлении нарушений защиты информации администратор ИБ обязан подать служебную записку ответственному за обработку персональных данных в управлении и занести соответствующую запись в журнал учета работы ИСПДн с изложением факта нарушения, предпринятые и/или рекомендуемые им действия.

3. Ответственность

Администратор ИБ несет всю полноту ответственности за качество и своевременность выполнения задач и функций, возложенных на его в соответствии с настоящей инструкцией и другими нормативными документами по защите информации.