Приложение 11 к приказу № 47/1

ИНСТРУКЦИЯ

администратора безопасности информации в
МКДОУ ЦРР-ДС №36 «Ласточка» г.Светлоград

1. Общие положения

Данная Инструкция является руководящим документом администратора безопасности информации в МКДОУ ЦРР-ДС №36 «Ласточка» г.Светлоград далее (ДОУ)

Требования настоящей инструкции должны выполняться во всех режимах функционирования.

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

Персональные данные относятся к категории информации ограниченного распространения.

Наиболее вероятными каналами утечки информации для информационных систем персональных данных (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 безопасности назначается лицо из числа наиболее квалифицированных пользователей ПЭВМ, либо имеющим образование в области защиты информации, в котором эксплуатируется информационная система.

Администратор безопасности в вопросах защиты информации взаимодействует с сотрудниками отдела по защите информации Правительства края.

1. 3.Обязанности администратора безопасности структурного подразделения

В своей повседневной деятельности администратор руководствуется данной инструкцией и другими документами, регламентирующими защиту персональных данных от утечки по техническим каналам и НСД, эксплуатационной документацией на установленные на объекте информатизации системы защиты от несанкционированного доступа к информации (СЗИ НСД) и от утечки информации по техническим каналам.

Администратор безопасности совместно со специалистами по информационным технологиям и защите информации:

- 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).

На администратора безопасности 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 и несъемных носителей информации;

- контролировать соблюдение требований по учету и хранению носителей конфиденциальной информации и персональных данных;

- совместно со специалистами по информационным технологиям и защите информации обеспечивать доступ к защищаемой информации пользователям согласно их прав доступа;

- незамедлительно докладывать руководителю учреждения, обо всех выявленных попытках несанкционированного доступа к информации ограниченного доступа;

- контролировать правильность применения пользователями сети средств защиты информации;

- участвовать в испытаниях и проверках ИСПДн;

- не допускать к работе на рабочих станциях и серверах посторонних лиц;

- осуществлять контроль монтажа оборудования специалистами сторонних организаций;

- участвовать в приемке для нужд новых программных средств;

- 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 работы с ИСПДн.

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;

- создание резервной копии базы данных и пр. служебной информации;

- 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 (дисководов, принтера и т.п.);

- перебои в системе электроснабжения;

- и.т.п.

При выявлении нарушения первой категории (утечка информации) администратор обязан немедленно прекратить работы в ИСПДн.

При выявлении нарушений первой, второй и третьей категорий администратор обязан подать служебную записку руководству и занести соответствующую запись в журнал учета работы ИСПДн с изложением факта нарушения, предпринятые и/или рекомендуемые им действия.

Форма журнала регистрации работ ИСПДн:

Дата	Наименование работ	Ф.И.О. исполнителя работ	ИСПДн _____	Роспись
1	2	3	4	5

3. Ответственность

Администратор безопасности 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.

С инструкцией ознакомлен: