

Утверждена
приказом заместителя начальника
управления по делам архивов
Белгородской области
от 12 июля 2012 года № 44-ГС

ИНСТРУКЦИЯ
ответственному за обеспечение безопасности персональных данных
в управлении по делам архивов Белгородской области

1. Общие положения

1.1. Настоящая Инструкция определяет основные функции, права и обязанности ответственного за обеспечение безопасности персональных данных в управлении по делам архивов Белгородской области (далее – Управление).

1.2. Ответственный за обеспечение безопасности персональных данных (ПДн) назначается из числа сотрудников Управления и отвечает за организацию работ по обеспечению защиты ПДн и разработке организационно-распорядительной документации на объекты вычислительной техники (ОВТ) в Управлении.

1.3. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения конфиденциальности и защиты персональных данных, используемых Управлением.

2. Функции ответственного за обеспечение безопасности
персональных данных Управления

2.1. Выполняет требования действующих нормативных документов по вопросам обеспечения конфиденциальности и защиты персональных данных, используемых в Управлении.

2.2. Осуществляет:

разработку организационно-распорядительной документации на ОВТ по вопросам обеспечения безопасности персональных данных в Управлении;

обучение лиц, вводит описания пользователей ПЭВМ в информационную базу установленной на ПЭВМ системы защиты информации (СЗИ) от несанкционированного доступа (НСД);

резервирование и восстановление информации в ИСПДн;

своевременно удаляет описания пользователей из базы данных СЗИ и средств криптографической защиты информации (СКЗИ) при изменении списка допущенных к работе на ПЭВМ лиц;

ежемесячно осуществляет смену паролей для доступа к ПЭВМ пользователями ПЭВМ.

2.3. Настраивает и сопровождает подсистему регистрации и учета действий пользователей при работе на ПЭВМ:

вводит в базу данных установленной на ПЭВМ СЗИ и СКЗИ от несанкционированного доступа описания событий, подлежащих регистрации в системном журнале;

регулярно проводит анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам;

своевременно информирует начальника Управления о несанкционированных действиях сотрудников Управления и проведение расследования попыток НСД.

2.4. Сопровождает подсистему обеспечения целостности информации на ПЭВМ:

проводит периодическое тестирование функций установленной на ПЭВМ СЗИ от НСД, особенно при изменении программной среды и полномочий исполнителей;

восстанавливает программную среду, программные средства и настройки СЗИ при сбоях;

осуществляет ведение двух копий программных средств СЗИ от НСД и контроль их работоспособности;

поддерживает установленный порядок и правила антивирусной защиты информации на ПЭВМ;

осуществляет контроль за отсутствием на съемных носителях остаточной информации по окончании работы пользователей;

периодически обновляет антивирусные средства (базы данных), установленные на ПЭВМ, контролирует соблюдение пользователями порядка и правил проведения антивирусного тестирования ПЭВМ.

2.6. Осуществляет сопровождение подсистемы защиты информации от утечки за счет ПЭМИН, контроль соблюдения требований по размещению и использованию ПЭВМ, указанных в Предписании на эксплуатацию.

2.7. Осуществляет обязательный контроль ведения электронного журнала и регулярно проводит анализ данного журнала.

3. Ответственный за обеспечение безопасности персональных данных Управления обязан:

3.1. Обеспечивать функционирование и безопасность средств защиты информации и криптосредств;

3.2. Проводить инструктаж пользователей по правилам работы на ПЭВМ с установленными СЗИ или СКЗИ от НСД;

3.3. В случае отказа средств и систем защиты информации принимать меры по их восстановлению;

3.4. Докладывать начальнику Управления о неправомерных действиях пользователей, приводящих к нарушению требований по обеспечению защиты персональных данных;

3.5. Вести документацию на ИСПДн (ПЭВМ) в соответствии с требованиями нормативных документов.

4. Ответственный за обеспечение безопасности персональных данных Управления имеет право:

4.1. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;

4.2. Требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.

Ознакомлен:

**Главный специалист управления
по делам архивов Белгородской области**

А.А. Беляева

«___» _____ 2012 года