Для служебного пользования
Экз. №_____

УТВЕРЖДАЮ

Директор
МКОУ СОШ №2 г.Алагира
_____ Сидомонидзе Ф.Н.
«_1_» _____ 20_17_ г.

ТЕХНОЛОГИЯ

обработки информации на объекте информатизации «Информационная система персональных данных «АРМ» МКОУ СОШ №2 г.Алагира»

1. Общие сведения.

Настоящая Технология определяет совокупность процессов при обработке информации, содержащей персональные данные, в процессе ее обработки и хранения на средствах вычислительной техники объекта информатизации «Информационная система персональных данных «АРМ» МКОУ СОШ №2 г.Алагира» (далее - ИСПДн).

Настоящая Технология предназначена для руководителей подразделений, пользователей, ответственных за защиту информации на объектах информатизации, администратора информационной безопасности (ИБ).

Мероприятия по защите информации осуществляются во взаимосвязи с другими мерами по обеспечению установленного режима секретности проводимых работ.

Используемые в составе системы защиты информации (СЗИ) средства защиты информации от несанкционированного доступа (НСД) должны иметь сертификат соответствия требованиям безопасности информации ФСТЭК России.

Ответственный за защиту информации осуществляет общее методическое руководство работами по обеспечению безопасности информации.

Администратор информационной безопасности отвечает за нормальное функционирование и контроль работы СЗИ от НСД.

Периодическое тестирование всех функций СЗИ от НСД с помощью тест-программ, имитирующих попытки НСД, должно проводиться при изменении программной среды и пользователей ИСПДн.

В состав ИСПДн входят стационарные ПЭВМ часть из которых выполняет функции сервера. В ИСПДн реализована многопользовательская модель доступа с разграничением прав. ИСПДн предназначена для обработки персональных данных работников. АРМ из ИСПДн имеет выход в сети общего пользования.

2. Технологический процесс обработки персональных данных.

Обработка информации, содержащей персональные данные, допускается в ИСПДн успешно прошедших аттестацию и предназначенных для этих целей.

При необходимости обработки информации, содержащей ПДн в ИСПДн, пользователь получает разрешение на выполнение работы согласно постоянно действующему (или разовому) заданию (приказу) руководителя подразделения, а также согласовывает свои работы с ответственным за защиту информации.

При первичном допуске к работе в ИСПДн пользователь знакомится с требованиями нормативно-методических и организационно-распорядительных документов по вопросам автоматизированной обработки информации, о чем делается запись в журнале ознакомления с организационно-распорядительными документами (ОРД), проходит инструктаж у

ответственного за защиту информации и администратора ИБ по вопросам организационного и технического характера соответственно, получает под роспись личный идентификатор и личный текущий пароль.

В согласованное с ответственным за защиту информации время пользователь принимает и включает ПЭВМ и необходимое периферийное оборудование, визуально убеждается в целостности печатей, исправности и нормальном функционировании ИСПДн.

Администратор ИБ в соответствии с эксплуатационно-технической документацией входящей в комплект СЗИ от НСД, а так же реализует требования разграничения доступа, при необходимости выполняет настройку СЗИ от НСД для реализации необходимых требований предъявляемых к заданному классу защищенности ИСПДн от НСД.

Для входа в ИСПДн пользователь использует персональный идентификатор, содержащий имя пользователя зарегистрированное в ИСПДн, а также вводит пароль, требования к парольной защите описаны в соответствующей инструкции и приступает к обработке защищаемой информации.

Технологический процесс обработки информации полностью описываются комплексом процедур автоматизированной обработки данных обусловленных функциональными возможностями технических и программных средств ИСПДн.

Множество процедур обработки данных в своей упорядоченной совокупности описывают информационную технологию обработки информации в ИСПДн.

Этапы автоматизированной обработки данных в ИСПДн полностью описываются следующими процедурами:

- ввод данных в ИСПДн;
- формализация и сортировка данных;
- запись данных;
- чтение данных;
- копирование/перенос данных;
- модификация и преобразование данных;
- архивация данных;
- удаление данных;
- транспортировка данных по внутренним каналам связи;
- вывод данных из ИСПДн.

Ввод информации в ИСПДн осуществляется пользователями ИСПДн следующими способами:

- ввод информации с клавиатуры рабочей станции;
- путем копирования и (или) переноса ее с отчуждаемых носителей информации (Flash-накопители, FDD, CD, DVD-CD, внешние HDD), при этом в ИСПДн не допускается использование не учтенных машинных носителей информации;

Иные способы ввода информации, в том числе речевой, в ИСПДн запрещены.

Формализация, модификация, преобразование, запись, чтение и сортировка данных осуществляется с использованием функционала используемого программного обеспечения.

Программное средство обработки данных выбирается в зависимости от формата представления данных. Эксплуатация функций программных средств должна осуществляться в строгом соответствии с эксплуатационной документацией на данное ПО. Для обработки защищаемой информации в ИСПДн пользователь использует ПО в соответствии с «Перечнем технических и программных средств, входящих в состав автоматизированной системы» утвержденным руководителем организации.

После ввода информации в ИСПДн она подлежит хранению только в тех ресурсах, которые определены как защищаемые. Заданными правилами разграничения доступа (уровнем допуска, правами доступа) определяется запрет или разрешение доступа к защищаемому ресурсу, таким образом, в зависимости от уровня допуска пользователя и заданных правил разграничения доступа, ему может быть разрешено или запрещено использовать любые

ресурсы ИСПДн, включая внешние периферийные устройства и съемные накопители информации. Все документы, создаваемые пользователем и подлежащие защите, сохраняются и/или открываются для обработки только в тех каталогах, которые определены как защищаемые ресурсы.

Права доступа к этим ресурсам определяются в заявке на имя ответственного за ЗИ со стороны начальника структурного подразделения пользователя. После согласования заявки с ответственным за ЗИ, администратор безопасности вносит изменения в матрицу доступа, на основании которой производится настройка прав доступа пользователей к защищаемым ресурсам.

Для модификации, уничтожения, копирования и (или) переноса информации пользователь должен обратиться к защищаемому ресурсу и после проверки его полномочий подсистемой разграничения доступа (диспетчером доступа) выполнить необходимые действия.

Копирование/перенос, удаление и транспортировка данных по внутренним каналам связи осуществляется с использованием средств операционной системы, а именно средствами файловой системы ОС – NTFS и стека протоколов TCP\IP.

Архивация данных осуществляется с использованием как штатных средств операционной системы, так и с использованием прикладного программного обеспечения компрессии данных.

Вывод информации из ИСПДн производится следующим образом:

- на печатающие устройства, на предварительно учтенные бумажные носители;
- копированием информации на учтенные машинные носители информации (ЖМД, ГМД, оптические диски, флэш-накопители).

Иные способы вывода информации из ИСПДн запрещены.

Вывод информации осуществляется посредством перенаправления потока данных на управляющие программы (канальные программы) называемые драйверами, которые понимают стандартный набор команд ОС.

Обработка и хранение защищаемой информации на неучтенных носителях информации ЗАПРЕЩАЕТСЯ.

В процессе работы в ИСПДн пользователь должен выполнять принятые соглашения по безопасности информации в рамках предоставленных привилегий по доступу к ресурсам ИСПДн (дискам, каталогам, файлам, программам).

В процессе работы в ИСПДн пользователю запрещается запускать программы не связанные с выполнением поставленной перед ним задачи.

По требованию администратора ИБ пользователь готовит и предоставляет ему перечень (список) программ, располагаемых на жестких дисках, на гибких магнитных носителях информации, оптических дисках, флэш-накопителях, которые пользователь использует или предполагает к использованию в своей работе.

Администратор ИБ проводит периодический анализ системных журналов СЗИ от НСД на предмет нарушений порядка работ пользователями и попыток несанкционированного доступа к ИСПДн. Такой анализ должен проводится регулярно, не реже одного раза в неделю.

Функции администратора ИБ и ответственного за ЗИ в ИСПДн могут быть возложены на одного человека.

Архивы системных журналов СЗИ от НСД должны храниться не менее 6 месяцев.

Периодический контроль за соблюдением установленных технологий обработки информации и выполнением пользователями инструкций по обеспечению безопасности и защите информации ИСПДн осуществляется администратором информационной безопасности.

Ответственный за защиту информации _____ / _____ /