УТВЕРЖДАЮ

Директор ТОГАОУ «Мичуринский лицей»

_____В.Н. Самусенко

«___» _____ 20___ г.

ОПИСАНИЕ

технологического процесса обработки информации в автоматизированной системе Тамбовского областного государственного автономного общеобразовательного учреждения «Мичуринский лицей-интернат»
(ТОГАОУ «Мичуринский лицей»)

Автоматизированная система (АС) – автоматизированное рабочее место (АРМ) «АРМ-УО-35» предназначена для обработки документов конфиденциального характера. Основное предназначение АРМ – обеспечение конфиденциальности информации, размещенной в региональном сегменте единой федеральной межведомственной системы учета контингента обучающихся по основным образовательным программам и дополнительным общеобразовательным программам (ГИС "Контингент"). Основной режим работы пользователя: разработка документов с помощью специализированного программного обеспечения.

Режим работы АС коллективный (многопользовательский). Доступ пользователей к работе АС осуществляется в соответствии с утверждаемой разрешительной системой.

Информация может храниться на:

– оптических дисках;

– флэш-накопителях;

– жёстких магнитных дисках в составе системного блока.

Информация может поступать с других АС на:

– оптических дисках;

– флэш-накопителях;

Субъектами доступа автоматизированной системы объекта информатизации ЛВС являются пользователи и администратор защиты информации, которым присвоены идентификаторы.

Пользователи имеют равный доступ к защищаемым ресурсам АС. Администратор защиты информации имеет полный доступ ко всем ресурсам АС.

Объектами доступа АС объекта информатизации являются:

– каталоги всех файлов, текстовые, табличные и графические файлы пользователей, размещаемые на жёстком магнитном диске в составе системного блока;

– каталоги всех файлов, текстовые, табличные и графические файлы пользователей, размещаемые на внешних отчуждаемых носителях;

– клавиатура;

– устройство ввода/вывода данных с оптических носителей;

– устройство ввода/вывода данных с USB-устройств;

– жёсткий магнитный диск в составе системного блока ПЭВМ;

– монитор ПЭВМ с отображаемой на нем информацией;

– оперативная память ПЭВМ;

– операционная система ПЭВМ;

– программы, служащие для разработки документов пользователя;

– программа архивирования данных;

– программы, осуществляющие функции по защите информации ПЭВМ, а также функции просмотра аудита безопасности.

В целях защиты информации от несанкционированного доступа на АС установлена система защиты информации от НСД ARMlock. Настройку системы защиты от НСД для конкретных пользователей и контроль ее работы осуществляет Администратор защиты информации.

Для организации безопасного сетевого взаимодействия на объекте информатизации установлен программно-аппаратный комплекс VipNet Client КС2 версия 3.2. Инсталляция и настройка произведена в соответствии с требованиями руководящих документов ФСТЭК России и ФСБ России.

Для организации антивирусного контроля в автоматизированной системе установлено средство антивирусной защиты DrWeb Enterprise Security 10.

Пользователи имеют право постоянного хранения файлов с секретными данными в специально выделенных Администратором защиты информации каталогах в соответствии с разрешительной системой.

В АС запрещено использование незарегистрированных флеш-накопителей.

Используемые для обработки и хранения накопители на жёстком магнитном диске в составе системного блока, а также внешние отчуждаемые носители информации учитываются перед использованием в журнале учёта носителей и в журнале системе защиты информации ARMlock.

Перечень программного обеспечения, используемого в АС, утверждается руководителем организации.

Копия установленной программной среды, а также копии дистрибутива ARMlock находятся у Администратора защиты информации в опечатанном конверте.

Права доступа пользователей к программам, каталогам и файлам в АС реализуются средствами защиты информации от несанкционированного доступа ARMlock.

Загрузка компьютера осуществляется по паролю конкретного пользователя. По окончании загрузки компьютера пользователь получает установленные Администратором защиты информации права доступа к устройствам, каталогам, файлам и программам АС.

Требование к паролю: длина пароля не менее шести символов, алфавит пароля не менее 60 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 5 до 30 минут, смена паролей не более чем через 120 дней.

Функции, права, обязанности и порядок работы в АС Администратора защиты информации и пользователей по обеспечению защиты конфиденциальной информации регламентируются «Положением по обеспечению защиты конфиденциальной

информации…» и Инструкциями, разработанными в дополнение к указанному Положению.

Антивирусная защита при обработке конфиденциальной информации осуществляется пользователями АС с применением программных средств в соответствии с «Положение по обеспечению защиты конфиденциальной информации…» и Инструкциями, разработанными в дополнение к указанному Положению.

Настройка средств защиты информации осуществляется Администратором защиты информации в соответствии с «Положением о разрешительной системе…».

Печать документов осуществляется субъектами доступа согласно матрице разграничения доступа к защищаемым ресурсам автоматизированной системы, определенной в документе «Положение о разрешительной системе доступа исполнителей к документам и сведениям…».

Схема информационных потоков