Автономное рабочее место для обработки конфиденциальной информации

Автономное рабочее место для обработки конфиденциальной информации представляет собой автономную автоматизированную систему, в которой может производиться обработка какой-либо информации ограниченного распространения (за исключением государственной тайны) – служебная тайна, коммерческая тайна, банковская тайна и т.д.

Условия эксплуатации АС:

- Режим обработки информации – многопользовательский;
- В АС пользователи имеют различный уровень полномочий на доступ к защищаемым ресурсам АС;
- В АС хранится и обрабатывается информация разного уровня конфиденциальности "служебная или коммерческая тайна".

В соответствии с (РД АС) руководящим документом "Автоматизированные системы, защита от несанкционированного доступа к информации классификация автоматизированных систем и требования по защите информации" определяется класс защищенности АС.

В качестве средств защиты в автоматизированной системе выступает программное обеспечение общего назначения со встроенными механизмами защиты, сертифицированными по требованиям безопасности ФСТЭК России:

- Сертифицированная операционная система Windows Vista или XP;
- Сертифицированный Антивирус Касперского или Антивирус Dr.Web;
- Сертифицированное средство контроля и протоколирования доступа пользователей к устройствам и портам ввода-вывода DallasLock или SecretNet, позволяющий контролировать весь спектр потенциально опасных устройств: USB-порты, дисководы, CD/DVD-приводы, а также FireWire, инфракрасные, параллельные и последовательные порты, WiFi и Bluetooth-адаптеры, ленточные накопители, КПК, любые внутренние и внешние сменные накопители и жесткие диски;

Перечень требований РД АС и их реализация сертифицированным программным обеспечением для АРМ Оператора приведен в таблице 1.

Таблица 1.

Требование РД АС	Средства, обеспечивающие выполнение требований РД
1. ПОДСИСТЕМА УПРАВЛЕНИЯ ДОСТУПОМ	
Идентификация, проверка под-линности и контроль доступа субъектов: в систему, к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройст-вам ЭВМ к программам к томам, каталогам, файлам, записям, полям записей.	Механизмы идентификация и аутентификация: - ОС Windows Vista/XP, - средства контроля и протоколирования доступа пользователей DallasLock или SecretNet;

Требование РД АС	Средства, обеспечивающие выполнение требований РД
2. **ПОДСИСТЕМА РЕГИСТРАЦИИ И УЧЕТА**	
2.1. Регистрация и учет:: входа (выхода) субъектов доступа в (из) систему (узел сети); выдачи печатных (графических) вы-ходных документов запуска (завершения) программ и процессов (заданий, задач) доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, запи-сям, полям записей.	Механизмы аудита безопасности: - ОС Windows Vista/ XP. - средства контроля и протоколирования доступа пользователей DeviceLock.
2.2. Учет носителей информации	Реализуется с помощью организационно-распорядительных мероприятий. Как правило ведется «Журнал учета машинных носителей»), в котором регистрируются все машинные носители информации АС.
2.3. Очистка (обнуление, обезличива-ние) освобождаемых областей оперативной памяти ЭВМ и внеш-них накопителей.	Механизм безопасности защита данных пользователя ОС Microsoft Windows Vista/XP. Очистка внешних накопителей обеспечивается пользователями и Администратором безопасности в соответствии с инструкциями и должностными обязанностями.
3. **ПОДСИСТЕМА ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ**	
3.1. Обеспечение целостности про-граммных средств и обрабатываемой информации:	Отсутствие на ПЭВМ (серверах) средств разработки исполняемых модулей программного обеспечения. Антивирус Касперского или Dr.Web.
3.2. Физическая охрана средств вы-числительной техники и носителей информации.	Реализуется с помощью организационно-распорядительных мероприятий.
3.3. Периодическое тестирование СЗИ НСД.	ОС Microsoft Windows Vista/XP; Антивирус Касперского или Dr.Web. С помощью организационно-распорядительных мероприятий.
3.4. Наличие средств восстановления СЗИ НСД.	Средство резервного копирования и восстановления ОС.