АВТОМАТИЗИРОВАННОЕ РАБОЧЕЕ МЕСТО ПОЛЬЗОВАТЕЛЯ ДЛЯ РАБОТЫ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ РАЗЛИЧНОГО КЛАССА ЗАЩИЩЕННОСТИ

Р. Ю. Дубровин, Д. Г. Аннин, А. П. Афонин, В. В. Жорин, А. А. Логинов, И. А. Нуштаев

ФГУП «РФЯЦ-ВНИИЭФ», г. Саров Нижегородской обл.

Введение

В последнее время возрастает необходимость работы пользователя в автоматизированных системах (АС) различного класса защищенности.

Поэтому становится актуальной задача организации автоматизированного рабочего места (АРМ) пользователя для работы в таких АС. Существуют различные способы организации АРМ для работы в нескольких автоматизированных системах различного класса защищенности, в том числе с использованием переключателей KVM [1], однако их реализация зачастую является дорогим решением. Поскольку существует необходимость работы пользователя в нескольких АС, обрабатывающих конфиденциальную информацию, то разработка способа организации АРМ пользователя для работы в автоматизированных системах различного класса защищенности, является актуальной задачей.

Описание способа организации автоматизированного рабочего места

При организации АРМ для работы в автоматизированных системах различного класса защищенности основной задачей является реализация системы защиты на таком АРМ. Так как АРМ не является изолированным, а подключен к локальной вычислительной сети (ЛВС), дополнительно рассмотрим решения по защите информации, при сетевом взаимодействии АРМ с автоматизированными системами.

Определим основные информационные потоки при работе с АРМ в автоматизированных системах:

- обмен информацией между АРМ и ресурсами других АС;
- ввод/вывод информации в/из АРМ с/на носители и (или) накопители (Н/Н) информации.

Возможными угрозами безопасности информации в части несанкционированного доступа к информации на АРМ являются:

- нарушение конфиденциальности и доступности информации за счет хищения защищаемой информации, находящейся на встроенном Н/Н информации;
- нарушение конфиденциальности информации при взаимодействии с АС различного класса защищенности (при обмене информацией между АРМ и ресурсами других АС);
- нарушение конфиденциальности информации при ее вводе/выводе в/из АРМ с/на внешний Н/Н информации;
- нарушение доступности и целостности защищаемой информации за счет использования вредоносного программного обеспечения (ПО).

Для предотвращения хищения защищаемой информации, находящейся на встроенном Н/Н информации, реализуются следующие мероприятия:

- операционная система (ОС) устанавливается на встроенный Н/Н информации, заблокированный для записи («только на чтение»);
- служебная информация, создаваемая ОС в процессе функционирования АРМ, размещается в оперативной памяти.

Для предотвращения нарушения конфиденциальности информации при взаимодействии с АС различного класса защищенности (при обмене информацией между АРМ и ресурсами других АС):

- разграничение доступа пользователей на АРМ – для работы в каждой АС свой сеанс работы (для каждого сеанса создается учетная запись);
- для каждого сеанса (учетной записи) задается индивидуальный IP-адрес сетевого интерфейса на АРМ;
- сетевое взаимодействие АРМ с автоматизированными системами осуществляется через межсетевой экран (МЭ) на котором настроена фильтрация по IP-адресам и протоколам.

Для предотвращения нарушения конфиденциальности информации при ее вводе/выводе в/из АРМ с/на внешний Н/Н информации для каждого сеанса (учетной записи) разрешен только определенный набор внешних Н/Н информации с определенным уровнем конфиденциальности, соответствующим уровню конфиденциальности выбранного сеанса. Остальные Н/Н информации запрещены.

Для предотвращения нарушения доступности и целостности за счет использования вредоносного ПО на АРМ используется антивирусное средство.

Пример реализации автоматизированного рабочего места

Способ организации АРМ рассмотрим на следующем примере. Пусть имеются две автоматизированные системы различного класса защищенности: АС2 и АС3, построенные на базе ЛВС. Необходимо

организовать для пользователя автоматизированное рабочее место для работы в АС2 и АС3. При этом АРМ и МЭ входят в состав АС1.

Исходя из постановки задачи, схема организации АРМ для работы в АС различного класса защищенности выглядит следующим образом (рис. 1). Стрелками отмечены информационные потоки: обмен информацией между АРМ и ресурсами АС2 и АС3 (1); ввод/вывод информации в/из АРМ с/на внешние Н/Н информации (2).

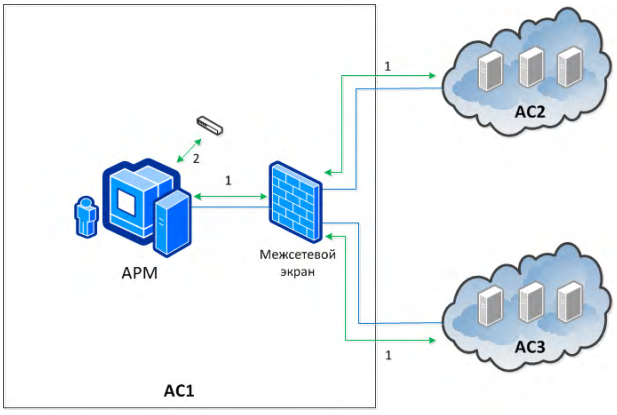

Рис. 1. Схема организации АРМ для работы в АС различного класса защищенности

В качестве аппаратного обеспечения АРМ используются:

1) системный блок;

2) монитор;

3) клавиатуру;

4) манипулятор типа «мышь».

В качестве внешних Н/Н информации используются USB-flash накопители. Для удаленного подключения к АС2 и АС3 используются ПО VMWare View.

В качестве средств защиты информации на АРМ используются:

1) АПМДЗ «Максим-М1» с microSD-картой;

2) ОС Astra Linux SE;

3) антивирусное ПО Dr.Web Enterprise Security Suite;

4) межсетевой экран Altell NEO.

Выполняются основные настройки средств защиты информации:

1) в АПМДЗ «Максим-М1» включим режим загрузки ОС только с microSD-карты;

2) в АПМДЗ «Максим-М1» для microSD-карты включим режим «только на чтение»;

3) в ОС Astra Linux SE для пользователя создадим две учетные записи: первая – для работы в АС2, вторая – для работы в АС3;

4) в ОС Astra Linux SE каждой учетной записи пользователя присвоим свой уникальный IP-адрес, который устанавливается (активируется) при входе в учетную запись и сбрасывается при выходе из сеанса работы;

5) в ОС Astra Linux SE для каждой учетной записи пользователя из графического интерфейса заблокируем все кнопки и ярлыки, кроме ярлыка VMWare View (с заданными настройками подключения) и кнопки выхода из сеанса и завершения работы;

6) на межсетевом экране настроим правила фильтрации по IP-адресам и протоколу PCoIP.

Работа пользователя на АРМ в АС различного класса защищенности состоит из следующих этапов:

1) пользователь включает АРМ, проходит процедуры идентификации/аутентификации на уровне АПМДЗ;

2) после загрузки ОС для работы в АС2 пользователь вводит логин и пароль от учетной записи, которая необходима для работы в АС2;

3) после авторизации в ОС пользователь с помощью ярлыка запускает программу VMWare View, подключается по протоколу PCoIP [2] к своей виртуальной машине в АС2 и начинает на ней работу. При необходимости ввода/вывода информации пользователь подключает в АРМ внешний Н/Н информации с уровнем конфиденциальности, соответствующим уровню конфиденциальности выбранного сеанса, и выполняет операции перемещения/копирования информации;

4) после окончания работы в АС2 пользователь закрывает окно программы VMWare View и выходит из сеанса, либо завершает работу на АРМ;

Для работы в АС3 пользователь выполняет аналогичные действия с учетной записью, которая необходима для работы в АС3.

Для администрирования АРМ администратор безопасности в настройках АПМДЗ «Максим-М1» включает режим записи для microSD-карты, который автоматически отключается после перезагрузки АРМ.

Заключение

Таким образом, с помощью предлагаемого способа организации АРМ возможна работа пользователя в АС различного класса защищенности. При этом:

- разграничение информационных потоков осуществляется с помощью сертифицированных по требованиям безопасности информации межсетевого экрана и ОС;
- пользователь может поочередно работать в нескольких АС различного класса защищенности с одного автоматизированного рабочего места.
- в процессе работы пользователя на АРМ в АС различного класса защищенности отсутствует фактор накопления защищаемой информации;
- после завершения сеанса работы на АРМ защищаемая информация на нем отсутствует.

Литература

1. KVM-переключатели – эффективное сетевое решение [Электронный ресурс] / CitForum, 2005. Режим доступа: http://citforum.ru/hardware/articles/kvm_switches, свободный.

2. Компьютер через IP-протокол (PCoIP) [Электронный ресурс] / PC-over-IP, 2012. Режим доступа: http://pc-over-ip.ru, свободный.