АВТОМАТИЗИРОВАННОЕ РАБОЧЕЕ МЕСТО ПОЛЬЗОВАТЕЛЯ ДЛЯ ПЕРЕНОСА ИНФОРМАЦИИ МЕЖДУ АВТОМАТИЗИРОВАННЫМИ СИСТЕМАМИ, ОБРАБАТЫВАЮЩИМИ ИНФОРМАЦИЮ РАЗЛИЧНОГО УРОВНЯ КОНФИДЕНЦИАЛЬНОСТИ

В. О. Носков, Д. Г. Аннин, А. П. Афонин

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

Несмотря на стремительное развитие информационных технологий, для некоторых автоматизированных систем (АС) единственным возможным каналом обмена информацией остается так называемый «воздушный зазор», то есть канал передачи информации через носители информации [1]. Если, при этом, в АС обрабатывается конфиденциальная информация, то становится актуальной задача предотвращения утечки при переносе информации. В основном для этого используются промежуточные АС, состоящие из одного или нескольких автоматизированных рабочих мест (АРМ), в которых используются внешние носители информации, предназначенные для переноса информации из одной АС в другую АС. Однако при этом риски утечки информации, связанные с ошибками пользователя («человеческий фактор») сохраняются. Поскольку АС, обрабатывающие информацию различного уровня конфиденциальности, широко используются на практике, разработка способа организации специализированного АРМ для обмена информацией между такими АС является актуальной задачей.

Описание способа организации автоматизированного рабочего места

При организации АРМ для переноса информации между автоматизированными системами, обрабатывающими информацию различного уровня конфиденциальности, основной задачей является реализация системы защиты информации на таком АРМ. Поскольку АРМ предназначается только для переноса информации, причем перенос информации может выполняться между АС, обрабатывающими информацию различного уровня конфиденциальности, АРМ является изолированным, то есть не подключенным к каким-либо локальным вычислительным сетям (ЛВС) [2]. Основными информационными потоками взаимодействия с АРМ являются ввод/вывод информации через внешние носители и (или) накопители (Н/Н) информации.

Возможными угрозами безопасности информации, передаваемой через АРМ, в части несанкционированного доступа к информации являются:

- нарушение конфиденциальности информации при ее вводе/выводе в/из АРМ с/на внешние Н/Н информации;
- нарушение доступности и целостности информации за счет использования вредоносного программного обеспечения (ПО).

Для предотвращения нарушения конфиденциальности информации при ее вводе/выводе в/из АРМ с/на внешние Н/Н информации на АРМ реализуются следующие мероприятия:

- операционная система (ОС) устанавливается на встроенный Н/Н информации, заблокированный для записи («только на чтение»);
- дискреционно ограничиваются права пользователя в ОС АРМ так, что из возможных действий у него остается только просмотр содержимого внешних Н/Н информации и перемещение/копирование информации с одного внешнего Н/Н информации на другой внешний Н/Н информации;
- в АРМ настраивается мандатное разграничение доступа таким образом, что пользовательским учетным записям устанавливаются сеансы доступа, соответствующие уровням конфиденциальности переносимой информации;
- служебная информация, создаваемая ОС в процессе функционирования АРМ, размещается в оперативной памяти;
- уровень конфиденциальности используемого сеанса равен высшему уровню конфиденциальности внешних Н/Н информации;
- уровень конфиденциальности внешнего Н/Н информации - передатчика информации не превышает уровень конфиденциальности Н/Н информации – приемника информации.

Для предотвращения нарушения доступности и целостности информации 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: АС1 и АС2, обрабатывающие информацию различного уровня конфиденциальности. Необходимо организовать перенос информации ме-

жду АС1 и АС2. При этом количество уровней конфиденциальности переносимой информации равно двум, АРМ входит в состав АС3.

Исходя из постановки задачи, схема организации АРМ для переноса информации выглядит следующим образом (рис. 1). Стрелками отмечены информационные потоки ввода/вывода информации в/из АРМ.

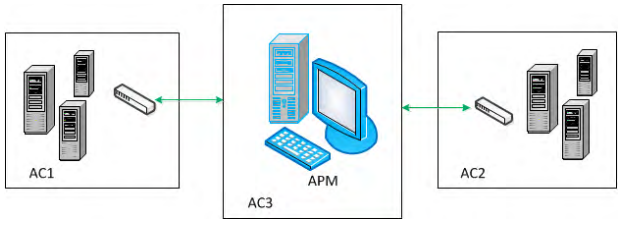

Рис. 1. Схема организации АРМ для переноса информации

В качестве аппаратного обеспечения АРМ используются:

1) системный блок;
2) монитор;
3) клавиатуру;
4) манипулятор типа «мышь».

В качестве внешних Н/Н информации будем использовать USB-flash накопители.

В качестве средств защиты информации на АРМ будем использовать:

1) АПМДЗ «Максим-М1» с microSD-картой;
2) ОС Astra Linux SE;
3) антивирусное средство Dr.Web Enterprise Security Suite.

Выполняются основные настройки средств защиты информации на АРМ:

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 учетную запись с двумя сеансами, соответствующими уровням конфиденциальности переносимой информации;

4) в ОС Astra Linux SE для учетной записи пользователя дискреционно ограничим права: оставим возможность выполнять вход только в графический интерфейс своей учетной записи; заблокируем все кнопки и ярлыки, кроме кнопки выхода из сеанса и завершения работы; из возможных действий в ОС оставим только просмотр содержимого внешних Н/Н информации и перемещение/копирование информации с одного внешнего Н/Н информации на другой внешний Н/Н информации.

Перенос информации на АРМ состоит из следующих этапов:

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

2) для переноса информации из АС1 в АС2 пользователь выбирает сеанс, равный высшему уровню конфиденциальности внешних Н/Н информации;

3) пользователь вставляет Н/Н информации АС1 и Н/Н информации АС2 в АРМ (при подключении Н/Н информации происходит автоматическая проверка на вредоносное ПО антивирусным средством), убедившись, что уровень конфиденциальности Н/Н информации АС1 не превышает уровень конфиденциальности Н/Н информации АС2;

4) пользователь переносит информацию из Н/Н информации АС1 на Н/Н информации АС2;

5) пользователь отключает Н/Н информации обоих АС и выходит из сеанса, либо завершает работу на АРМ.

Перенос информации из АС2 в АС1 выполняется аналогично.

Для администрирования АРМ администратор 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 возможен перенос информации между автоматизированными системами, обрабатывающими информацию различного уровня конфиденциальности. При этом вероятность нарушения конфиденциальности, целостности и доступности информации в результате непредумышленных действий пользователя при переносе информации сведена к минимуму.

Литература

1. Гирфанова Л. Р. Системы автоматизированного проектирования изделия и процессов. Уфа, 2014. С. 45.

2. Современные технологии защиты от утечки конфиденциальной информации [Электронный ресурс] / Диалог Наука, 2010. Режим доступа: https://dialognauka.ru/press-center/article/4761/, свободный.