УДК 004.056.53

ОРГАНИЧЕНИЕ ДОСТУПА К ВНЕШНИМ ИНТЕРФЕЙСАМ РАБОЧЕГО МЕСТА ОПЕРАТОРА АСУ

Липницкий Л.А., Шалькевич П.К., Бутько А.А.
Учреждение образования «Международный государственный экологический Институт имени А.Д. Сахарова» Белорусского государственного университета, Минск, Беларусь, leonid-l@tut.by

Организации защиты информации ЭВМ зачастую применяются различные системы программного и технического характера, позволяющие обеспечить надежность работы устройства и сохранность хранимой информации и в тоже время замедляющие работу устройства. При этом на автономных рабочих станциях, осуществляющих автоматическое управление технологическим процессом, могут не всегда использоваться данные системы защиты. Однако автономность рабочих мест АСУ ТП не всегда гарантируют безопасную работу системы.

Одной из причин этого может являться несанкционированной доступ к устройству операторов, работающих на рабочем месте. Зачастую операторы могут воспользоваться своим местом, чтобы срочно перекинуть информацию со своего устройства (flash drive, телефон) на рабочую станцию или другой носитель. В таких случаях решающую роль могли принести как административные требования, запрещающие несанкционированный доступ к рабочему месту, так и блокировка интерфейсов ЭВМ.

Проводя анализ двух вариантов решения проблемы, необходимо отметить, что административный метод ограничения, являясь более простым, одновременно не является более надежным и не исключает возможных нарушений принятого регламента. В тоже время блокировка интерфейсов имеет определенные технические проблемы и требует определенной квалификации. Кроме того конструктивные изменения требуют согласования с производителем АСУ. Использование интерфейсов может быть необходимо для установки обновлений программного обеспечения, получения диагностической информации о работе устройства или данных об изменении параметров регулируемого процесса. В этих случаях процесс доступа к портам рабочего места значительно усложняется.

Решением данной проблемы могло бы стать создание списка разрешенного к подключению оборудования и проверка оборудования на соответствие этому списку. Для определения подключенного оборудования можно использовать следующие параметры: тип оборудования, производитель, серийный номер. С помощью специализированного программного обеспечения можно в зависимости от результата проверки подключенного оборудования либо обеспечить его доступ к устройству, либо блокирование или игнорирование данного оборудования, как если бы оно не было вообще подключено к устройству. Также возможно осуществлять контроль за отключением разрешенного оборудования, например, клавиатуры. Реакций на данное действие могло бы быть блокирование работы устройства и/или выдача сообщения. При необходимости с целью предотвращения нарушения целостности программного обеспечения и нарушения работы устройства возможно также предусмотреть его отключение в случае несанкционированного подключения или отключения оборудования.

Анализ показывает, что, для решение поставленной задачи возможно использование как аппаратных, так и программных средств.

При использовании аппаратных средств доступа в PCI слот ЭВМ устанавливается модуль безопасности в виде специальной платы, который может обеспечивать целостность оборудования и осуществлять проверку права доступа подключаемого внешнего устройства [1]. Вместе с тем необходимо отметить достаточно высокую стоимость подобного решения. Что существенно ограничивает его использования в

большинстве случаев.

Программный способ имеет несколько возможных решений. Так, в частности, операционная система Windows при соответствующей настройке можно обеспечить частичное или полное блокирование подключаемых USB устройств [2, 3]. При этом можно обеспечить доступ только для таких USB устройств, как мышь, клавиатура, принтер и т.д., не разрешив доступ USB флеш-накопителям. К недостаткам данного способа можно отнести то, что при определенном уровне знаний можно временно или постоянно снять данную блокировку.

Применение специализированного программного обеспечения позволяет администраторам обеспечить ограниченный доступ к возможности блокирования внешних портов с возможностью, в том числе, удаленного контроля и доступа к этой функции, что позволяет вносить оперативные изменения в работу рабочего места. Данное решение может потребовать определенных финансовых затрат, но позволит более надежно защитить рабочее место от несанкционированного доступа.

Еще одним решением может быть применение гипервизора - программной технологии, позволяющей осуществлять одновременную работу нескольких операционных систем на одном компьютере [4]. Помимо параллельной работы данная технология позволяет обеспечить изоляцию этих операционных систем, разделять их аппаратные ресурсы, обеспечивая защиту и безопасность. Гипервизор обладает возможностью эмулировать аппаратные устройства и скрывать их от операционных систем. Эта возможность позволяет анализировать аппаратные средства, которые подключаются к рабочему месту и в соответствии с выполненными настройками ограничивать доступ этих средств к операционной системе ЭВМ. Особенностью гипервизора является то, что специализированное программное обеспечение для него необходимо разрабатывать индивидуально под требование каждого контролируемого устройства, что значительно удорожает стоимость для каждого отдельного случая. В этой связи целесообразно разрабатывать и поставлять данное программное решение вместе с оборудованием, то есть решать систему безопасности доступа на уровне производителя.

Рассмотренные способы ограничение доступа к портам рабочей станции позволяют защитить ее с определенной степенью надежности от возможных сбоев в работе и сохранить программное обеспечение ЭВМ. Выбранный метод зависит от финансовых возможностей пользователя и требований к степени надежности защиты или же может задан производителем АСУ. При этом нельзя не пренебрегать другими средствами защиты, такими как антивирусная, сетевая и другими, позволяющими в зависимости от способа организации рабочего места обеспечить надежную его работу. Не смотря на то, что количество способов обойти защиту возрастает, увеличивается число и разнообразие методов защиты, которыми не стоит пренебрегать при организации рабочих мест, включая АРМ оператора АСУ.

Список литературы

1. Aladdin Trusted Security Module (TSM) [Электронный ресурс] // Режим доступа: http://www.tadviser.ru/index.php/Продукт:Aladdin_Trusted_Security_Module_(TSM).

2. Запрет использования USB накопителей с помощью групповых политик (GPO) Windows. [Электронный ресурс] // Режим доступа: http://winitpro.ru/index.php/2015/09/22/otklyuchenie-usb-nakopitelej-cherez-gruppovye-politiki-gpo.

3. Как включить и отключить usb порты. [Электронный ресурс] // Режим доступа: http://sudgapc.ru/blog/10-vklyuchit-i-otklyuchit-usb-porty.

4. Всѐ по ГОСТу. Защита информации при использовании технологий виртуализации. Электронный ресурс] // Режим доступа: https://habr.com/ru/company/cloud4y/blog/352178.