DOI 10.37882/2223–2966.2021.01.03

РАЗРАБОТКА И АНАЛИЗ МЕТОДА ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ АППАРАТНОГО И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПРОМЫШЛЕННЫХ ОБЪЕКТОВ, РАБОТАЮЩИХ НА ОСНОВЕ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ РАЗЛИЧНЫХ ИЕРАРХИЧЕСКИХ СТРУКТУР

DEVELOPMENT AND ANALYSIS OF A METHOD FOR INCREASING THE SECURITY OF HARDWARE AND SOFTWARE OF INDUSTRIAL FACILITIES OPERATING ON THE BASIS OF LANS OF VARIOUS HIERARCHICAL STRUCTURES

A. Andryukhin
N. Grachev
N. Lvov

Summary. This paper presents a method developed and used to protect a local area network (LAN) from unauthorized access. The essence of the method is to control the hardware of PCs, that are part of the local network by means of a specialized server that performs a network survey and stores information in a specialized database. The General principle of operation of SOFTWARE based on this method is considered, and flowcharts are provided.

Keywords: information protection, software, local area networks.

Андрюхин Александр Гавриилович
К.т.н., доцент, МИРЭА — Российский технологический университет (г. Москва)
pr1110@list.ru
Грачев Николай Николаевич
К.т.н., профессор, МИРЭА — Российский технологический университет (г. Москва)
nngrachev@mail.ru
Львов Никита Сергеевич
МИРЭА — Российский технологический университет (филиал в г. Фрязино)
lvov_ns@outlook.com

Аннотация. В данной работе представлен метод, разработанный и используемый для защиты локально-вычислительной сети (ЛВС) от несанкционированного доступа. Суть метода заключается в контроле аппаратной части ПК, входящих в локальную сеть, посредством разработанного в данной работе программного комплекса, выполняющего опрос сети и хранящего информацию в специализированной базе данных. Рассматривается общий принцип работы ПО, построенного на основе данного метода, приводятся блок-схемы.

Ключевые слова: защита информации, программные средства, локально-вычислительные сети.

Актуальность данной работы заключается в повышении защищенности аппаратного и программного обеспечения локальных сетей различных объектов, а также оперативного реагирования на случаи несанкционированных изменений аппаратных конфигураций, как в сторону уменьшения (например, при несанкционированной замене комплектующих), так и в сторону увеличения (например, при несанкционированном подключении посторонних устройств для попытки организации канала утечки конфиденциальной информации). В качестве объектов могут выступать различные предприятия и организации, имеющие как обычные, так и территориально распределенные ЛВС на основе структур от выделенного сервера до централизованного кластера серверов [1].

Объектом исследования является уровень защиты дорогостоящего аппаратного и программного обеспечения локально-вычислительных сетей объектов, обладающее уникальными или специализированными свойствами от несанкционированных проникновений и изменений.

Целью проведенных исследований является повышение эффективности защиты локально-вычислительных сетей (ЛВС) от несанкционированного доступа при

Рис. 1. Принцип работы ПО AIDA64

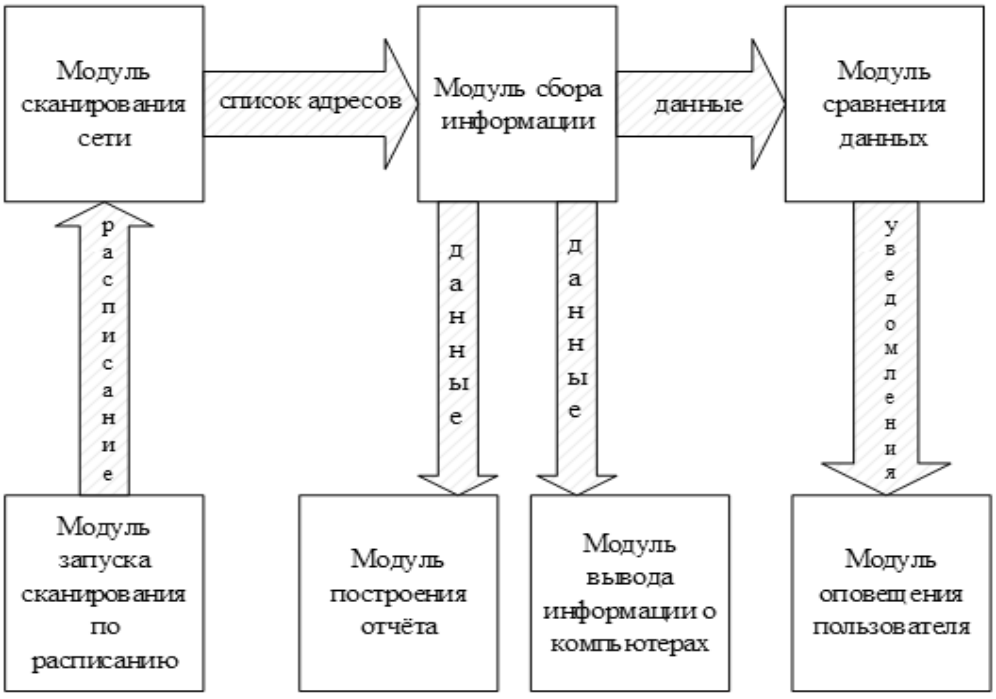

Рис. 2. Структурная схема реализации предлагаемого в данной работе метода

ведении учета аппаратного обеспечения, и разработка средств, позволяющих моментально уведомлять о несанкционированных изменениях.

В настоящее время для попытки решения данной проблемы применяются два метода:

- в части борьбы с попытками подключения несанкционированных устройств — путем механической блокировки корпусов процессорных блоков, а также пломбирования внешних интерфейсов, и ежедневного контроля целостности пломбировки. Данный метод, при его высокой надежности, имеет существенный недостаток —

требуется ежедневное присутствие контролирующего лица;
- в части борьбы с попытками кражи или подмены комплектующих — путем использования специализированных программных комплексов (например, AIDA64 фирмы FinalWire Ltd, или «Инвентаризация компьютеров» отечественного производителя 10-Страйк).

Данные программные комплексы позволяют из любой точки сети получить информацию о аппаратной конфигурации любого узла сети. Однако, данный метод не позволяет выполнить автоматическую сверку текущего состояния аппаратной конфигурации узла сети с его состоянием в предшествующее время. Принцип работы данного и аналогичного ему ПО приведен на рисунке 1.

Для достижения поставленной в работе цели необходимо решить следующие подчиненные задачи, а именно:
- сохранение информации о эталонном состоянии аппаратного обеспечения узлов сети;
- определение статуса узлов сети в параллельном режиме;
- периодический сбор информации о текущем состоянии аппаратного обеспечения узлов сети [2].

В данной работе предлагается использовать следующий оригинальный метод. Его структурная схема приведена на рисунке 2. Локально-вычислительная сеть объекта подвергается круглосуточному мониторингу со стороны центрального сервера сети объекта, имеющего достаточную степень защиты от постороннего вмешательства. Сама структура метода исключает возможность наличия вышеуказанных недостатков. Не требуется выполнять «пломбирование» и «опечатывание» интерфейсов и процессорных блоков, а также выполнять ручное протоколирование состояний аппаратной конфигурации — данные операции происходят автоматически с заданной периодичностью. Уменьшение этого временного отрезка повышает время реагирования на несанкционированные вмешательства, однако повышает нагрузку на сеть.

Модуль сканирования сети (его блок-схема, представляющая собой принцип функционирования модуля сканирования сети, представлена на рисунке 3) Указанный принцип производит производить вычисление допустимой области адресов компьютеров в сети, на основе идентификатора подсети и маски. Далее, он совершает проверку соединения с этими компьютерами, и исключает те адреса, по которым не удалось установить связь. Затем по полученному списку адресов выполняется проверка возможности сбора необходимых данных по WMI, с помощью короткого WMI запроса, таким образом исключаются все устройства, которые её не поддерживают, или к ним по какой-то причине нет доступа в данный момент. Полученный список доступных адресов передаётся следующим модулям.

На первом этапе происходит перевод маски подсети в двоичную систему счисления, затем возведение числа 2 в степень суммарного количества бит в маске, принимающих значение «1», что позволяет получить количество возможных адресов компьютеров. На втором этапе происходит генерация списка возможных адресов хостов, путём инкрементации адреса на количество возможных адресов. На третьем этапе происходит сканирование всех адресов в списке. Если в списке имеется адрес, который ещё не проходил проверку, то выполняется эхо-запрос по нему, в результате которого выясняется наличие или отсутствие доступа к адресу. При наличии доступа к адресу идёт его проверка с помощью короткого WMI запроса, благодаря которой адрес либо записывается в список доступных адресов, либо исключается из списка, затем происходит переход к следующему адресу; При отсутствии доступа к адресу, он исключается из списка и происходит переход к следующему адресу.

Если в списке все адреса прошли проверку, то модуль передаёт список доступных адресов следующим модулям.

Модуль сбора информации производит опрос компьютеров по списку адресов, на предмет свойств и параметров их внутренних комплектующих. Затем производит приведение полученной информации к объектной модели, создавая условный объект для каждого компьютера, который содержит в себе объекты его составных частей, которым в свою очередь присваиваются свойства реальных комплектующих. Приведение информации к данному виду обусловлено необходимостью унифицировать обработку всех компьютеров. Полученный массив объектов передаётся следующим модулям.

Опишем алгоритм, представленный блок-схемой (см. рис. 4). На первом этапе, по полученному от модуля сканирования сети списку адресов, выполняется сбор информации от компьютеров [3].

На втором этапе создаются абстрактный объект для каждого компьютера, как совокупность некоторого количества устройств. На третьем этапе для каждого обнаруженного комплектующего создаётся абстрактный объект, как совокупность свойств комплектующего. Происходит заполнение свойств данного объекта информацией о характеристиках реального комплектующего. На четвёртом этапе происходит логическое объедине-

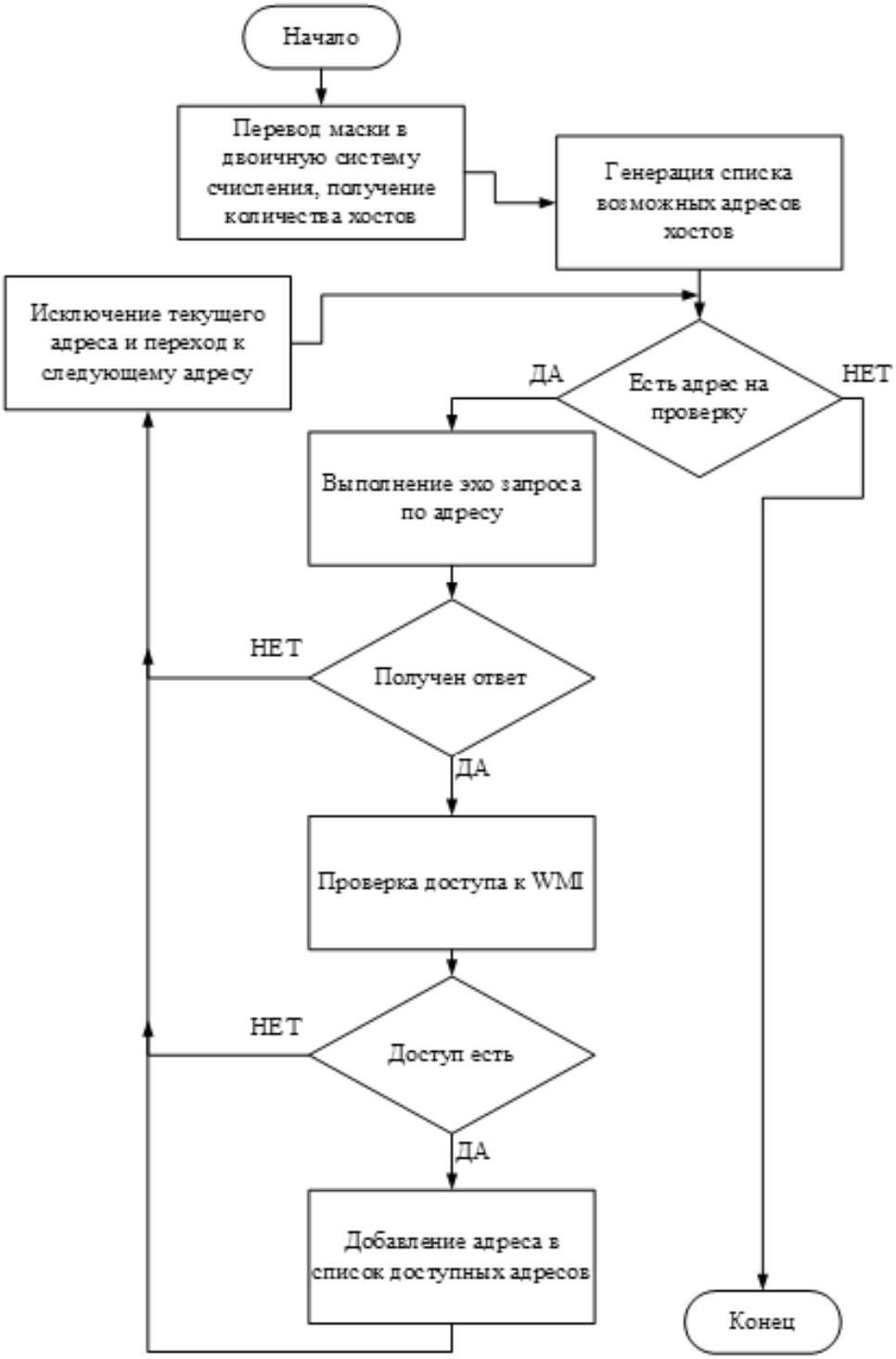

Рис. 3. Блок-схема работы модуля сканирования сети

ние объектов компьютеров с объектами комплектующих, в соответствии с реальным оборудованием. На пятом этапе каждому объекту компьютера присваиваются служебные свойства: имя, адрес и время сканирования, необходимые при обработке данной структуры последующими модулями.

Модуль сравнения данных производит сравнение так называемых «архивных данных» предыдущего сканирования и «новых данных» полученных при последнем сканировании. Если же архивных данных нет, то новые данные автоматически станут архивными. Такое происходит при самом первом запуске программы.

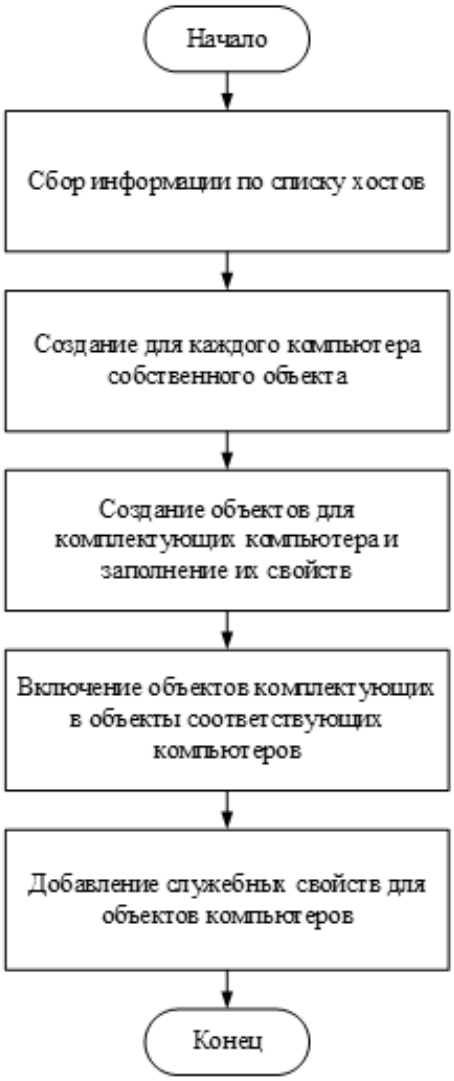

Рис. 4. Блок-схема работы модуля сбора информации

Опишем алгоритм, представленный блок-схемой (см. рис. 4). На первом этапе происходит попарное сравнение каждого свойства, каждого комплектующего в каждом компьютере. На втором этапе при нахождении изменений далее происходит проверка наличия архивной информации о несовпадающем свойстве. Если информация о данном параметре ранее присутствовала в архиве, то модуль сделает вывод о том, что вероятно устройство отсутствует и перейдёт к следующему параметру. Если никакой информации о несовпадающем параметре найти не удалось, то модуль сделает вывод что этот параметр принадлежит новому устройству и перейдёт к следующему параметру. При отсутствии изменений модуль просто завершает свою работу [4].

Таким образом, разработанный метод повышает защищенность аппаратного и программного обеспечения локальных сетей различных объектов от несанкционированного доступа и дает возможности оперативного реагирования на несанкционированные изменения, отличающийся от ныне существующих методов за счет отсутствия необходимости физического контроля аппаратного обеспечения, а также за счет возможности выполнения сверки текущего состояния аппаратной конфигурации узла сети с его состоянием какое-то время назад. Программное средство, созданное на основе разработанного метода, позволяет отказаться от приобретения дорогостоящих программных пакетов (стоимость лицензии AIDA64 на 1 рабочую станцию составляет около 14 тысяч рублей и если офис организации содержит около 20 компьютеров, то лицензия им обойдется в 280 тысяч рублей а при обновлении парка ПК или смене системной платы лицензию придется приобретать заново) для проведения мониторинга состояния аппаратного обеспечения ЛВС на базе ОС Windows.

ЛИТЕРАТУРА

1. Таненбаум Э. Современные операционные системы, 4-е издание / Таненбаум Э., Бос Х.— СПб.: Питер, 2018–1120 с.
2. Попов А. В. Введение в Windows PowerShell / Попов А. В.— СПб.: БХВ-Петербург, 2009.— 464 с.
3. Линн С. Администрирование Microsoft Windows Server 2012 / Линн С.— М.: Орелли, 2014–304 с.
4. Прайс М. C# 7 и.NET Core. Кросс- платформенная разработка для профессионалов / Прайс М.— СПб.: Питер, 2019–640 с.

МИРЭА — Российский технологический университет