DOI 10.37882/2223–2966.2022.01.03

ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ МОНИТОРИНГА РАБОТОСПОСОБНОСТИ И ПРОИЗВОДИТЕЛЬНОСТИ УЗЛОВ ТЕРРИТОРИАЛЬНО- РАСПРЕДЕЛЕННОЙ СЕТИ

A SOFTWARE PACKAGE FOR MONITORING THE HEALTH AND PERFORMANCE OF NODES IN A GEOGRAPHICALLY DISTRIBUTED

A. Andryukhin
N. Grachev
N. Lvov

Summary. This paper presents the results of research and development of a software package for remote monitoring with the possibility of covert and partially full-featured device control, which provides: collection of information about current processes; collection of information about the current installed programs and related services; collection of information about the configuration of the workstation; collection of information about the current state of the processor, RAM, disks and other components of the device; the ability to remotely shutdown and reboot the device; the ability to remotely execute commands. The developed software should significantly facilitate the function of monitoring workstations, as well as control and assistance to employees during remote operation.

Keywords: software tools, monitoring, network management.

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 представлены результаты исследований и разработки программного комплекса для удаленного мониторинга с возможностью скрытного, и частично полнофункционального управления устройством, обеспечивающего: сбор информации о текущих процессах; сбор информации о текущих уставленных программах и соответствующих служб; сбор информации о конфигурации рабочей станции; сбор информации о текущем состоянии процессора, оперативной памяти, дисках и других компонентах устройства; возможностью удаленного выключения и перезагрузки устройства; возможностью удаленного выполнения команд. Разработанное программное обеспечение должно существенно облегчить функцию мониторинга рабочих станций, а также контролирование и оказание помощи сотрудникам при удаленном режиме работы.

Ключевые слова: программные средства, мониторинг, управление сетью.

В эпоху развития вычислительных технологий, а также компьютеризации и автоматизации различных процессов все больше компаний внедряют и наращивают вычислительные мощности. Сложно сказать, что какая-либо компания в настоящий момент не имеет хотя бы пару компьютеров. Зачастую у каждой организации имеется собственная выделенная сеть, в которую входят все компьютеры и устройства, на которых работают сотрудники. Средние и крупные организации как правило имеют несколько различных подразделений, офисов, где также используется выделенная сеть, в которую входят все рабочие станции [1]. Важно понимать, что вычислительная техника требует обслуживания, своевременного выявления проблем, а также инвентаризации установленного программного обеспечения, и контроля за действиями сотрудников при работе с устройством — иначе говоря, мониторинга рабочих станций. Мониторинг обычно осуществляет системный администратор, в полномочия которого входит настройка и поддержания работоспособности всех компьютеров и прочих устройств в сети. Так как зачастую устройств гораздо больше, чем обслуживающих их специалистов, то для удобного управления и мониторинга устройств используется специальное программное обеспечение (ПО) [3].

В последнее время во многих компаниях также увеличилось количество сотрудников, которые работают удаленно со своих устройств без подключения к сетям компаний, что в свою очередь ограничивает контроль работы сотрудников, а также ослабляет безопасность при работе с корпоративными данными.

Исходя из вышеизложенного и текущей тенденции перевода сотрудников организаций на удаленный режим работы остро встает вопрос о мониторинге

Таблица 1. Основные характеристики разработанного ПО

Характеристика	Значение
Максимальное количество пользователей	Неограниченно
Удаленное выполнение команд и скриптов	Команды и скрипты
Возможность скрытного выполнения	Присутствует
Возможность мониторинга	Присутствует
Сетевая архитектура	Клиент-серверная с промежуточным сервером

за устройствами в иных сетях, отличных от корпоративной.

Представленные на рынке готовые программные решения для контроля и мониторинга рабочих станций малоэффективны и зачастую крайне неудобны.

Целью данной разработки является программный комплекс для удаленного мониторинга с возможностью скрытного, и в то же время на 75–90% полнофункционального управления устройством, а именно со следующим функционалом: сбор информации о текущих процессах; сбор информации о текущих уставленных программах и служб; сбор информации о конфигурации рабочей станции; сбор информации о текущем состоянии процессора, оперативной памяти, дисках и других компонентах устройства; получение скриншотов с устройства; с возможностью удаленного выключения и перезагрузки устройства; с возможностью удаленного выполнения команд. Разработанное ПО должно существенно облегчить функцию мониторинга рабочих станций, а также контролирование и оказание помощи сотрудникам при удаленном режиме работы.

Разрабатываемое ПО может работать в разного рода корпоративных сетях, таких как: централизованная корпоративная сеть; централизованная корпоративная сеть с филиалами; децентрализованная корпоративная сеть; сеть типа «виртуальный офис».

В разработанном программном комплексе сделан упор на детальный мониторинг рабочих станций, а также на гибко регулируемую нагрузку сети. Используется архитектура клиент-серверная с промежуточным сервером, которая позволяет устанавливать соединение как в корпоративной сети, так и за ее пределами в обход возможных ограничений брандмауэра.

Для отслеживания устройства необходимо всего лишь произвести установку агента на рабочую станцию. Агент в данном случае работает скрытно и не затрудняет работу пользователю.

Также предусмотрено удаленное выполнение команд PowerShell, удаленная перезагрузка и выключение рабочей станции.

Агент, в свою очередь, производит сбор информации с компьютера и отправляет ее на удаленный сервер. Информация может быть как запрошена специалистом, так и автоматически отправлена. Производиться сбор следующей информации: об операционной системе, ее версии и дате установки; о загруженности ЦП, ОЗУ, дисков; об установленных программах и службах; об входящем и исходящем траффике; о запущенных процессах; об внутренних компонентах рабочей станции [3].

Основные характеристики разрабатываемого ПО представлены в таблице 1.

Для реализации программного комплекса необходимо было спроектировать его архитектуру. В данной работе, необходимо реализовать работу программного комплекса из любого вида сети, как территориально распределенной, так, например, и из сети, не имеющей доступа к сети компании.

В разработанном программном комплексе были учтены все недостатки аналогов, а следовательно разработанный комплекс должен эффективно решать поставленную задачу и полностью удовлетворять те цели, которые были перед ним поставлены.

Проведя сравнительный анализ наиболее популярных аналогов разрабатываемого ПО, можно выделить основные недостатки в функциональности аналогов программы: частичное либо полное отсутствие возможности мониторинга; нежелательная лишняя нагрузка на сеть; отсутствие возможности скрытного выполнения; ограниченное количество пользователей.

Реализация сценария, где сеть имеет конфигурацию, в которой рабочие станции находятся не в едином сетевом периметре с центральным офисом, требует на-

Рис. 1. Подключение к компьютеру по архитектуре клиент-сервер

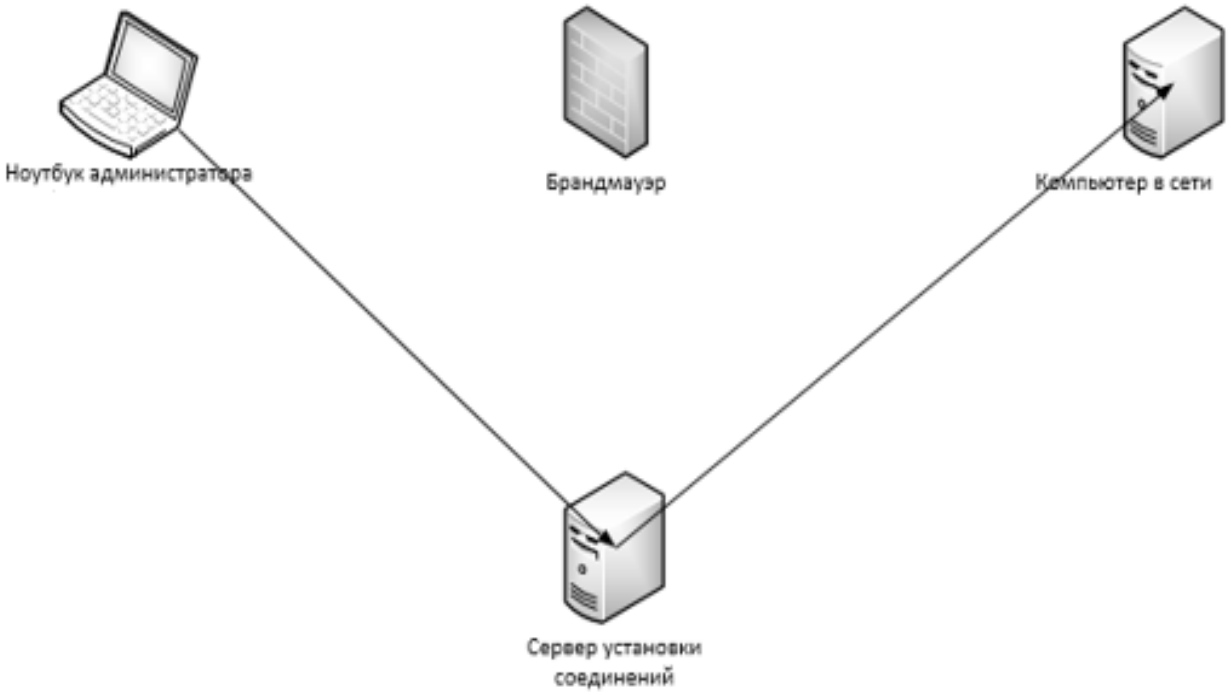

Рис. 2. Подключение к компьютеру по архитектуре «агент-сервер»

личия специально спроектированной архитектуры, так как использование стандартных архитектур, например, клиент-серверной затруднительно. Стоит отметить, что использование стандартных архитектур для реализации вышеуказанной задачи осложнено своей строгой привязанности к работе на публичных IP адресах. Сервер не сможет получить доступ к клиенту, не зная его адреса, только клиент имеет возможность установить соединение с сервером.

Таким образом, если попытаться представить использование классической архитектуры клиент-сервер в решение поставленной задачи, то в роли сервера выступала бы каждая рабочая станция, а в роли клиента устройство администратора с которого ведется мониторинг. В вышеуказанном случае необходимо было бы предусмотреть открытие портов на рабочих станциях, а также обязательного наличия белого IP адреса на каждом устройстве, либо же обязательное наличие механизма NAT, что крайне проблематично. Схематичное изображение решения поставленной задачи по архитектуре клиент-сервер изображено на рисунке 1 [1].

Поскольку реализация программного комплекса стала затруднительной по классической архитектуре, то было принято решение отойти от данной модели посредством введения промежуточного сервера, который располагается в офисе организации. В контексте данной работы обозначим такую архитектуру агент-серверной.

Как уже отмечалось выше, агент-северная архитектура базируется на введении промежуточного сервера, но также, данная архитектура подразумевает инициирование соединения рабочей станцией с сервером. Таким образом, получается, что каждая рабочая станция сама устанавливает соединение с сервером и посредством данного соединения производиться двухсторонний обмен данными. Визуализация данных происходит

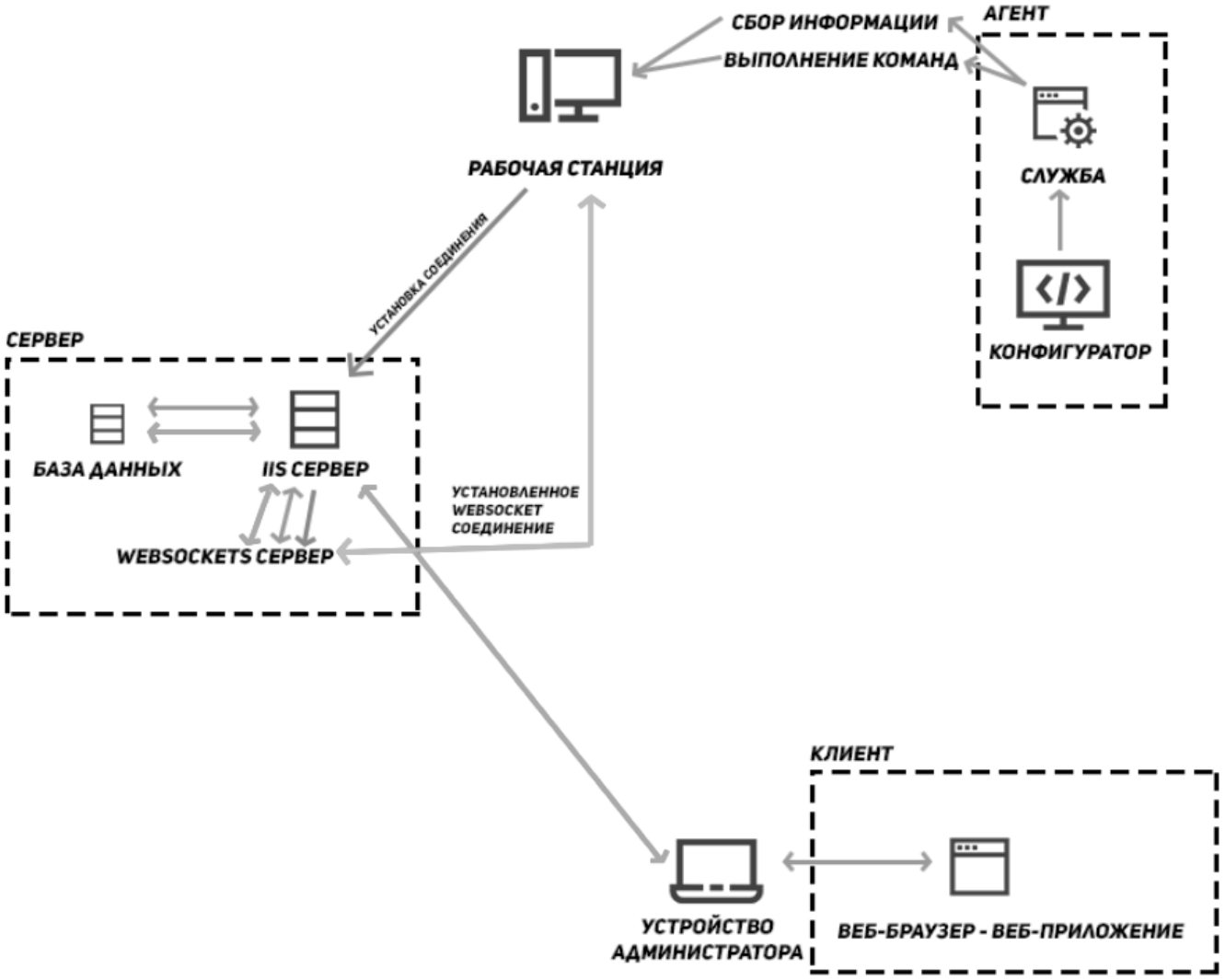

Рис. 3. Архитектура программного комплекса

на стороне администратора, который также подключается к выделенному серверу.

Таким образом, в архитектуру «агент-сервер» входят: сервер, агент, клиент.

Под сервером, как уже отмечалось ранее, подразумевается центральный офис, отвечающий за сбор, хранение и анализ информации.

Агентом, в нашем случае, называется специализированное ПО, устанавливаемое на рабочих станциях, на которых требуется выполнять мониторинг. Агент состоит из: зарегистрированным в качестве служба приложением и конфигуратором для него. Применение служб в решение данной задачи обусловлено тем, что пользователь не может вмешаться в ее работу. Остановить службу без разрешения также невозможно. Важно отметить, что служба имеет возможность запускаться автоматически при загрузке ОС, до входа пользователя в систему.

Под клиентом в данной архитектуре понимается рабочая станция администратора, который инициирует соединение с сервером и получает от него данные мониторинга.

Спроектированная архитектура представлена на рисунке 2.

Также, как можно заметить из рисунка 2, что спроектированная архитектура позволяет обходить возможные ограничения брандмауэра, что полностью решает вышеуказанные трудности при использовании классической архитектуры, включая наличие белых IP адресов и возможного закрытия портов.

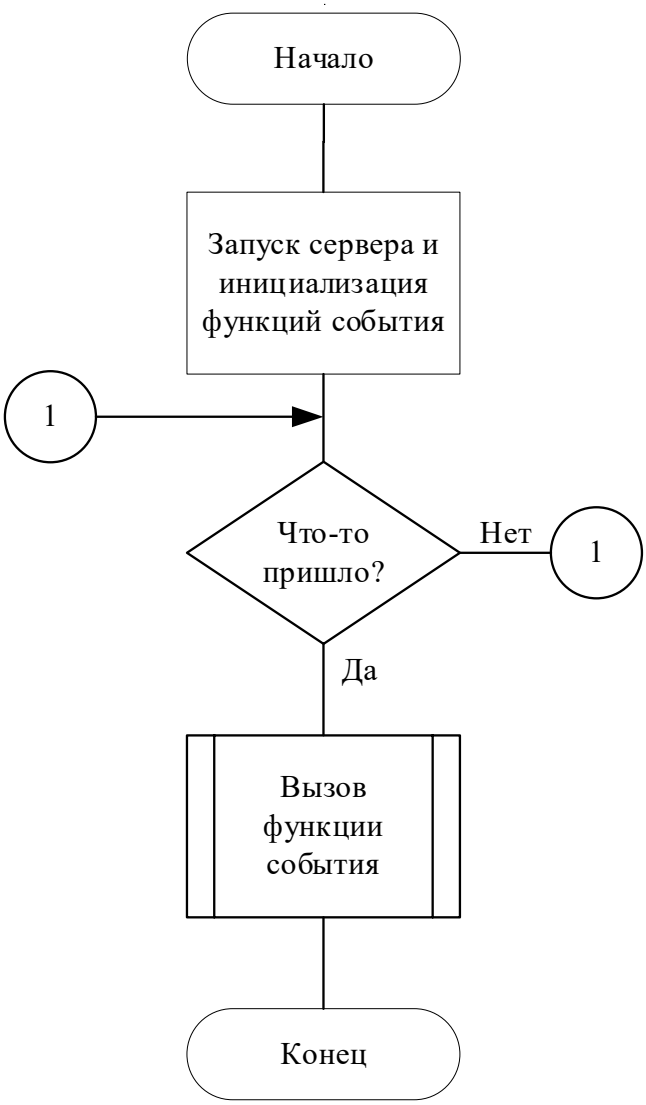

Рис. 4. Блок-схема реализации Websocket сервера

Поскольку разработанный программный комплекс имеет сложную структуру и состоит из нескольких модулей, то для начала его разработки следовало составить схему и разделить на данной схеме несколько основных выполняемых модулей, каждый из которых отвечает за своей определенный набор функционала.

Разработанная архитектура программного комплекса приведена на рисунке 3.

Как можно видеть из приведенного выше рисунка, реализация передачи данных по Websocket не только позволяет в реальном времени отправлять и получать данные, но и избегать излишней нагрузки на сеть [2].

Стоить отметить, что Websockets соединение начинается с HTTP запроса, чтобы обеспечить полную поддержку устаревших решений, а в дальнейшем работает поверх TCP на прикладном уровне по модели OSI. Агент отправляет запрос на сервер и, если сервер поддерживает протокол WebSockets, то отправляется ответ, в котором он перезаписывает заголовок соединения. С этого момента выполняется соединение на основе WebSockets [2].

Реализация Websocket сервера производилась с помощью PHP библиотеки workerman. Данная библиотека уже имеет поддержку создания Websocket сервера и полную поддержку соединений. Рассмотрим следующую блок-схему реализации Websocket сервера с помощью вышеуказанной библиотеки (рисунок 4).

Немаловажную роль играют функции, вызов которых происходит, когда на сервер приходит какое-ли-

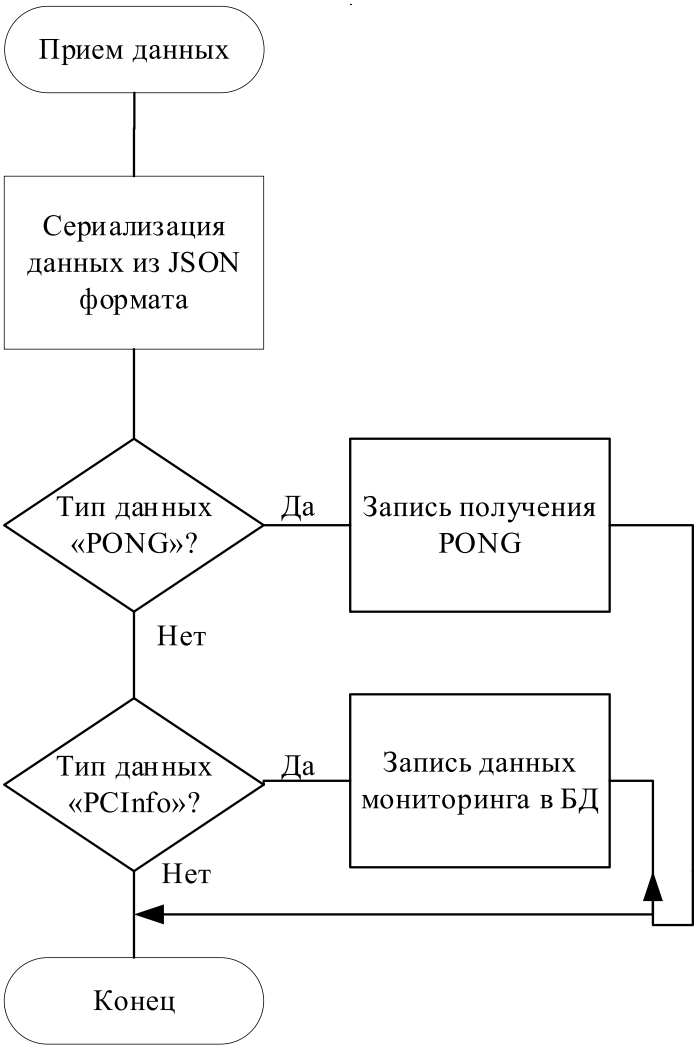

Рис. 5. Блок-схема реализации функции «onMessage»

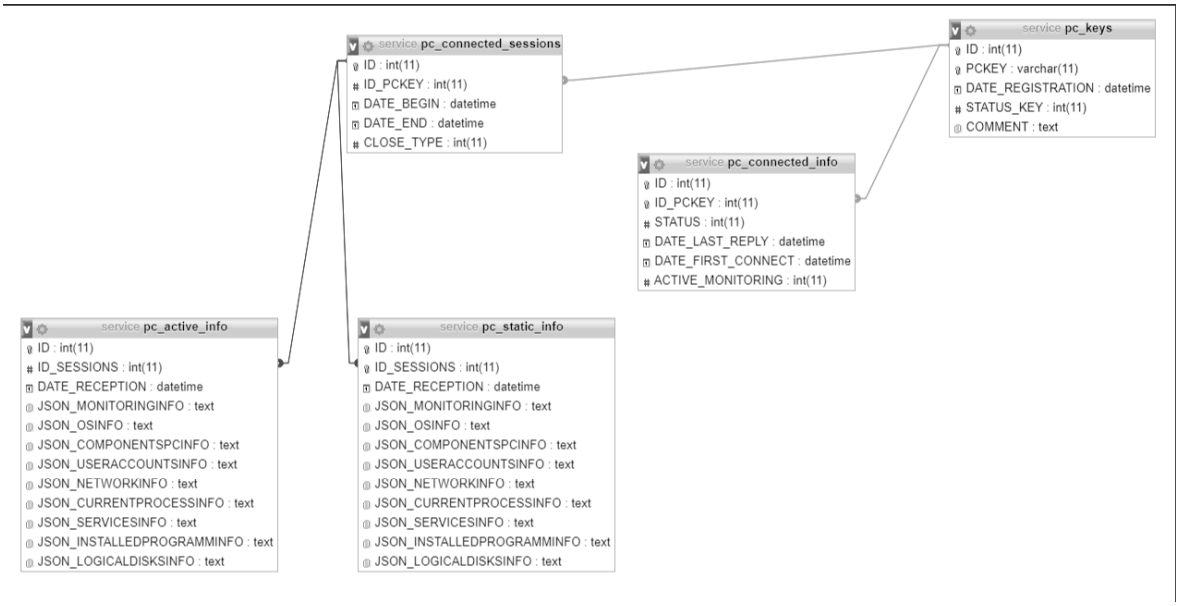

Рис. 6. ERD схема базы данных

бо сообщение. Рассмотрим такую функцию. Функция «onMessage» вызывается, когда на сервер по установленному соединению приходят какие-либо данные от агента, а в теле функции происходит считывание типа данных, и в зависимости от типа происходит, например, запись в базу данных либо отправка PONG сигнала '[4].

Алгоритм работы данной функции, представленный в виде блок-схемы, изображён на рисунке 5.

Также на сервере была реализована база данных под управлением СУБД MySQL [4]. ERD схема базы данных приведена на рисунке 6

Таким образом, разработан программный комплекс, позволяющий выполнять мониторинг рабочих станций в локальных сетях различных архитектур, удовлетворяющий заявленным выше требованиям. имеющий преимущества перед распространенными на рынке аналогами.

ЛИТЕРАТУРА

1. Таненбаум Э. Современные операционные системы, 4-е издание / Таненбаум Э., Бос Х. — СПб.: Питер, 2018–1120 с.
2. Хокинс С. Администрирование Web-сервера Apache и руководство по электронной коммерции / Хокинс С. — М.: Вильямс, 2011. — 336 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.

© Андрюхин Александр Гавриилович (pr1110@list.ru),
Грачев Николай Николаевич (nngrachev@mail.ru), Львов Никита Сергеевич (lvov_ns@outlook.com).
Журнал «Современная наука: актуальные проблемы теории и практики»

МИРЭА — Российский технологический университет