УДК 004.724

И. В. Потуремский, А. В. Мурыгин

СИСТЕМА МОНИТОРИНГА УЗЛОВ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ НА ОСНОВЕ ПРОТОКОЛА SYSLOG

Рассматривается система мониторинга узлов локальной вычислительной сети (ЛВС), в которой реализована поддержка протокола syslog в режиме реального времени. Система основана на обработке событий, регистрируемых в узлах ЛВС, что позволяет своевременно получать достоверную информацию о состоянии этой сети.

Ключевые слова: мониторинг ЛВС, syslog.

Стремительное развитие локальных вычислительных сетей (ЛВС) сопровождается увеличением не только количества подключаемых персональных компьютеров, но и серверных станций и специальных сетевых устройств, обеспечивающих их поддержку и функционирование. К специальным сетевым устройствам относятся маршрутизаторы, коммутаторы, медиаконвертеры, межсетевые экраны и т. д. Администраторам ЛВС все сложнее осуществлять мониторинг работоспособности узлов ЛВС и ежедневно анализировать регистрационную информацию, относящуюся к сети в целом [1].

Сбор регистрационной информации чаще всего проводится с помощью протокола syslog. Этот протокол и программные средства поддержки обеспечивают запись информации о событиях в системный журнал, а также передачу их на сервер журнализации по сети. Компонентами системы являются генератор сообщений (устройство или процесс), протокол обмена, коллектор сообщений (collector, syslog server), релей (relay), принимающий сообщения от одного или нескольких генераторов [2]. Сообщения, переданные по протоколу syslog, используются администратором сети для анализа событий после того, как произошел сбой, для установления его причины.

Для более оперативного получения информации о сбоях в работе сети применяются системы мониторинга узлов ЛВС, большинство из которых построены на следующем принципе: в определенные интервалы времени система мониторинга выполняет запрос назначенному узлу ЛВС и при получении от него отрицательного ответа либо при отсутствии ответа сообщает о сбое администратору сети [3]. Однако если сбой в устройстве происходит после его проверки или в промежутке между опросами, то администратор узнает о сбое по прошествии значительного времени. Для многих организаций такая ситуация может повлечь за собой сбой технологического процесса обработки информации, что является недопустимым.

Рассматриваемая в данной статье система мониторинга узлов ЛВС реализована на основе протокола syslog и позволяет собирать информацию о нарушениях в работе сети в режиме реального времени. Полученные по протоколу syslog сообщения не просто предоставляются системой для хранения и последующего анализа, а проходят процедуру обработки (унификации) и фильтрации по заданной матрице и в зависимости от критичности осуществляют уведомление администратора ЛВС о произошедшем событии.

Система состоит из двух основных частей: серверной и клиентской (рис. 1).

Серверная часть системы устанавливается на отдельно выделенный сервер и выполняет функции получения, унификации, хранения, шифрования и передачи клиентским частям полученных по стандарту syslog сообщений в режиме реального времени (рис. 2).

Функция «Получение» открывает для чтения указанный администратором сети TCP- или UDP-порт (обычно 514) и обеспечивает прием сообщений по протоколу syslog от сетевых устройств ЛВС согласно заданному списку.

Функция «Унификация» работает следующим образом. Структура сообщения, полученного по протоколу syslog, начинается с поля, которое в закодированном виде содержит информацию об источнике сообщения и уровне серьезности сообщения, за ним записывается время, имя или IP-адрес хоста и произвольный текст сообщения [4].

Уровень серьезности кодируется числом от 0 до 7:

– 0 – система неработоспособна;
– 1 – требуется немедленное вмешательство;
– 2 – критическое состояние;
– 3 – ошибка;
– 4 – предупреждение;
– 5 – все нормально, но важно;
– 6 – информационное сообщение;
– 7 – отладочная информация.

Таким образом, сообщение, полученное по стандарту syslog, содержит критерий важности сообщения. Однако в зависимости от типа сетевого оборудования и производителя уровни серьезности и структура текста сообщений существенно отличаются друг от друга. Например, у коммутатора компании D-Link выключение порта характеризуется уровнем серьезности 6 (информационное сообщение), а у коммутатора компании Dell уровень серьезности при данном событии – 4 (предупреждение). Причем очень часто встречаются ситуации, когда выключение одного порта коммутатора является не критичным (например, при выключении компьютера, подключенного к данному порту), а выключение другого порта на этом же коммутаторе является критичным (например, при выключении порта, к которому подключен сервер сети, либо другого важного сетевого устройства). Поэтому для определения уровня серьезности сообщений от различных устройств производится обработка сообщений и их проверка согласно заданным в матрице сообщений правилам.

Обработка сообщений, полученных по протоколу syslog, осуществляется таким образом, что сообщение принимает следующий вид:

– поле № 1 – [дата и время] – указываются дата и время, когда сообщение было получено сервером. Хотя оригинальное сообщение уже имеет штамп времени, здесь используются дата и время, установленные на сервере, так как не у всех сетевых устройств имеется служба синхронизации времени и формат времени у каждого производителя сетевого устройства может отличаться;

– поле № 2 – [имя либо IP-адрес отправителя] – указывается логическое имя или IP-адрес сетевого устройства, отправившего сообщение;

– поле № 3 – [уровень серьезности] – устанавливается идентичным оригинальному сообщению (в числовом виде);

– поле № 4 – [произвольный текст сообщения] – указывается текст оригинального сообщения.

Например, сообщение, полученное от коммутатора Dell PowerConnect 6224 и имеющее вид

[FEB 11 09:21:18] [192.168.64.254] [NOTIFICATION] [Link Down: Unit 1 Port 2],

после обработки станет таким:

[11.02.2009] [09:21:18] [192.168.64.254] [5] [Link Down: Unit 1 Port 2],

после чего уже обработанное сообщение будет проверяться на уровень критичности согласно заданной администратором сети матрице сообщений.

Матрица сообщений формируется следующим образом. Администратор сети разбивает сообщение, полученное по протоколу syslog, на четыре основных блока:

– 1-й блок – наименование устройства, отправившего сообщение: вводится логическое имя либо IP-адрес устройства (если указать ключевое слово ALL, то данное правило будет рассматриваться для всех устройств);

– 2-й блок – объект контроля: вводится идентификатор объекта контроля (для коммутатора это может быть номер порта, доступ к устройству, конфигурационный файл и т. п.);

– 3-й блок – событие с объектом контроля: вводится событие, которое необходимо отследить (для коммутатора это включение или выключение порта, неудачная или удачная попытка доступа к устройству, изменение или сохранение конфигурационного файла и т. п.);

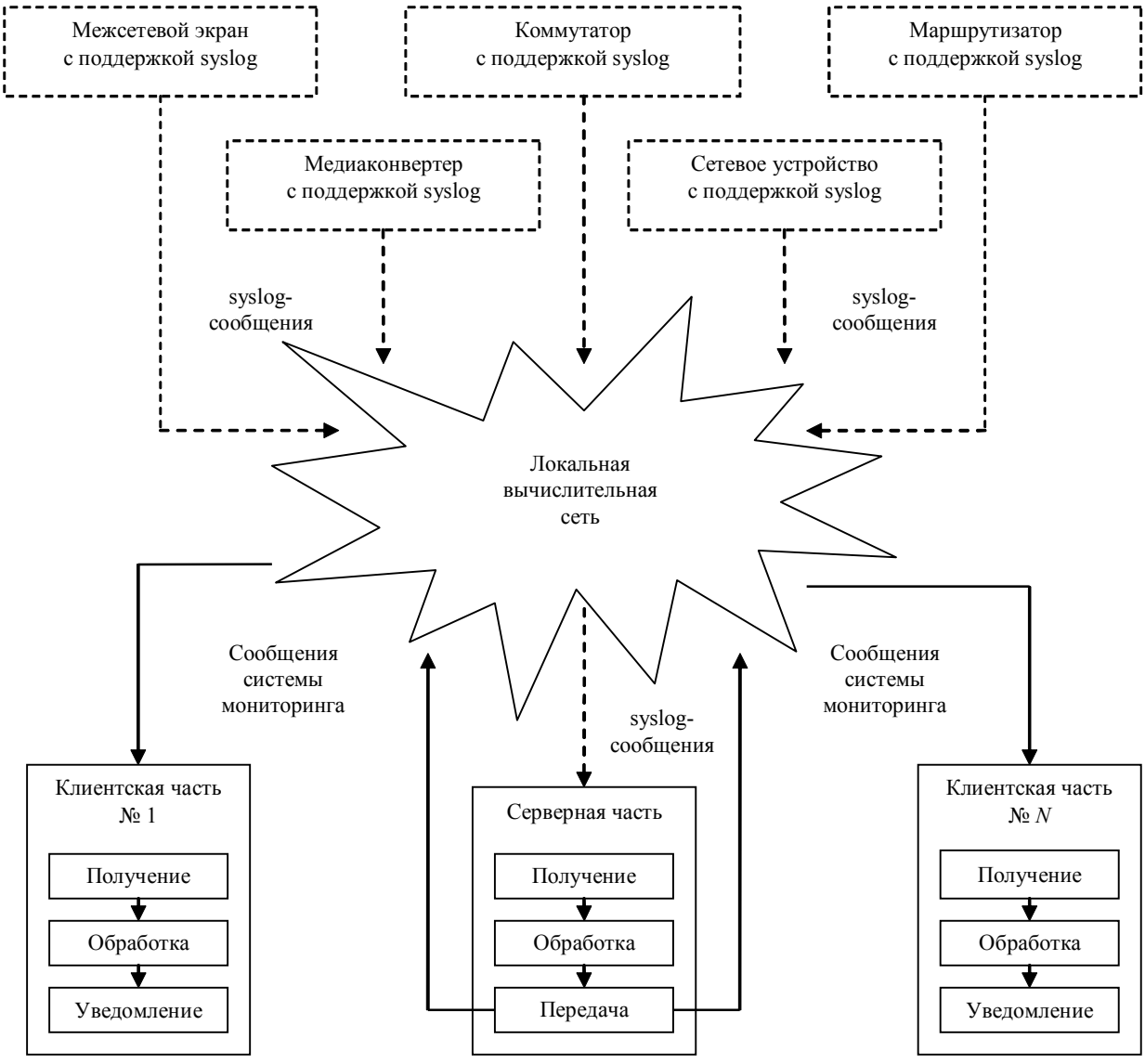

Рис. 1. Общая схема взаимодействия серверной и клиентской частей системы мониторинга узлов ЛВС

– 4-й блок – критичность события: вводится уровень критичности сообщения (0 – критическое состояние, 1 – предупреждение, 2 – информационное сообщение, 3 – не важное сообщение).

Например, если администратору необходимо контролировать все неудачные попытки доступа к устройству по http-протоколу, то он может воспользоваться следующим правилом. Сообщение от коммутатора Dlink

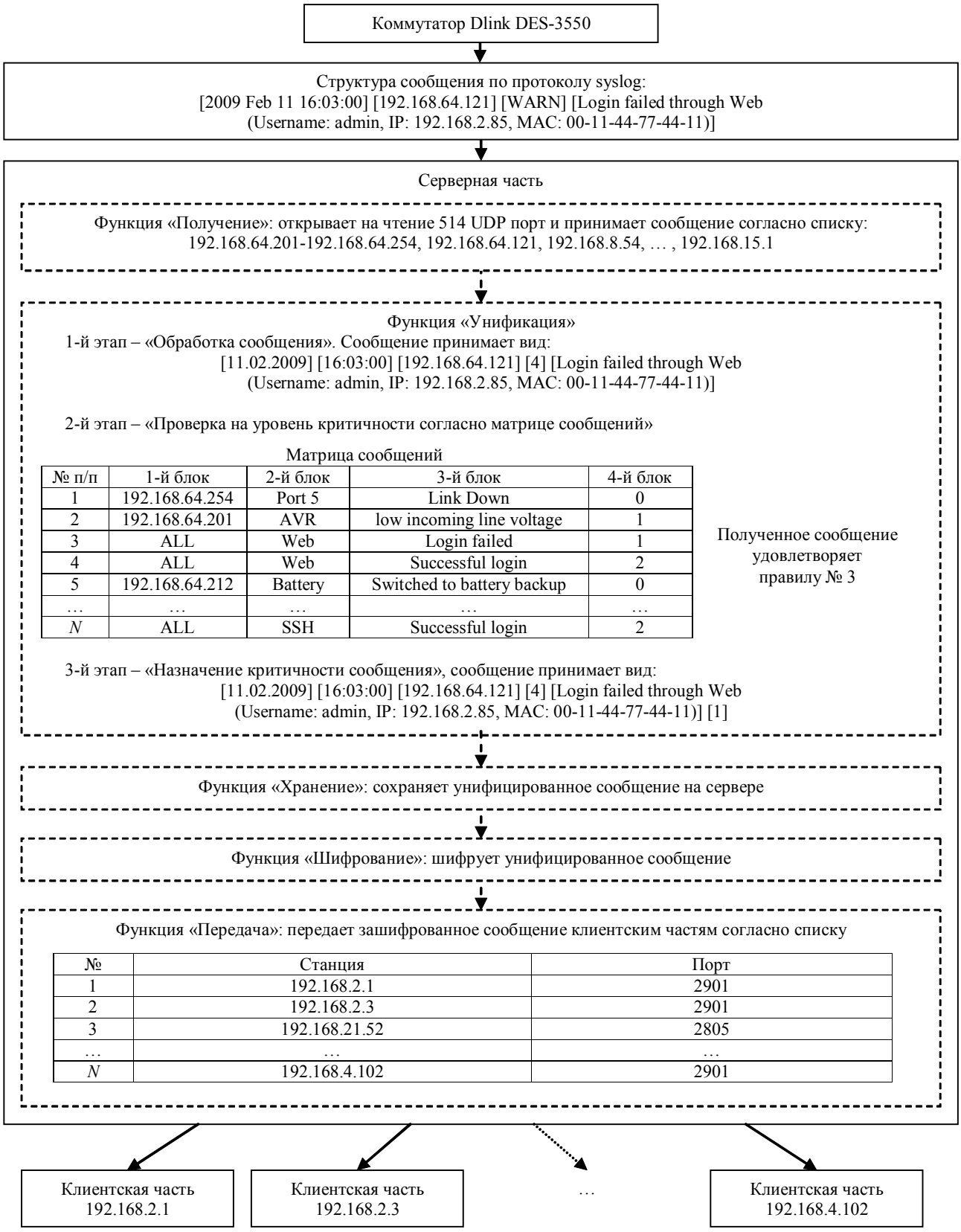

Рис. 2. Схема работы серверной части системы мониторинга узлов ЛВС при получении сообщения по протоколу syslog от сетевого устройства

DES-3550 о неудачной попытке доступа к устройству по http-протоколу, имеющее оригинальный вид

[2009 Feb 11 16:03:00] [192.168.64.121] [WARN] [Login failed through Web (Username: admin, IP: 192.168.2.85, MAC: 00-11-44-77-44-11)],

после обработки примет вид

[11.02.2009] [09:30:15] [192.168.64.121] [4] [Login failed through Web (Username: admin, IP: 192.168.2.85, MAC: 00-11-44-77-44-11)]

и будет вноситься следующим образом:

– 1-й блок – 192.168.64.121 (IP-адрес коммутатора);

– 2-й блок – Web (доступ по http-протоколу);

– 3-й блок – Login failed (неудача);

– 4-й блок – 1 (предупреждение).

Таким образом, если после проверки в матрице сообщение удовлетворяет существующему правилу, то в конец сообщения дописывается указанный в 4-м блоке уровень критичности. Например, сообщение о неудачной попытке доступа к коммутатору Dlink DES-3550 по http-протоколу будет иметь вид

[11.02.2009] [09:30:15] [192.168.64.121] [4] [Login failed through Web (Username: admin, IP: 192.168.2.85, MAC: 00-11-44-77-44-11)] [1].

Если сообщение не подпадает ни под одно правило матрицы и имеет уровень серьезности ниже 3 (ошибка) т. е. от 4 до 7, то ему присваивается критичность сообщения 3 (не важное). Если сообщение не попадает ни под одно правило матрицы и имеет уровень серьезности выше 4 (предупреждение) т. е. от 0 до 3, то сообщению присваивается критичность сообщения 0 (критическое состояние).

Функция «Хранение» осуществляет запись и хранение на сервере унифицированного сообщения.

Функция «Шифрование» проводит шифрование унифицированного сообщения по заданному администратором методу (алгоритму).

Функция «Передача» открывает для записи указанный администратором ЛВС TCP- или UDP-порт и обеспечивает передачу шифрованных сообщений клиентским частям согласно заданному списку. Список содержит поля «Станция» и «Порт», в которых соответственно указываются клиентские станции и удаленный порт, на которые необходимо передать зашифрованное сообщение.

Клиентская часть системы мониторинга узлов ЛВС устанавливается на рабочие станции администратора и/или обслуживающего ЛВС персонала и выполняет следующие функции: получение, дешифрование, хранение сообщений и уведомление о событии в сети пользователя рабочей станции (рис. 3).

Функция «Получение» открывает для чтения указанный администратором сети TCP- или UDP-порт и обеспечивает прием сообщений от серверной части.

Функция «Дешифрование» обеспечивает дешифрование полученного сообщения от серверной части по заданному администратором сети методу.

Функция «Хранения» записывает и хранит обработанное сообщение.

Функция «Уведомление» осуществляет уведомление пользователя рабочей станции, на которой установлена клиентская часть, согласно уровню критичности сообщения.

По умолчанию уведомление проводится следующим образом:

– при уровне критичности полученного сообщения 2 (информационное) – появление всплывающего (неактивного) окна, содержащего принятое сообщение, на заданное администратором сети количество времени;

– при уровне критичности полученного сообщения 1 (предупреждение) – мигание иконки клиентской части в меню systray;

– при уровне критичности сообщения 0 (критическое состояние) – мигание иконки клиентской части в меню systray и появление сообщения в активном окне на рабочем столе рабочей станции.

При необходимости администратор и/или обслуживающий ЛВС персонал может сформировать локальную матрицу на своей рабочей станции для изменения заданных правил уведомления.

Для формирования локальной матрицы уведомлений задаются четыре основных блока:

– 1-й блок – наименование устройства, которое является источником сообщения: вводится логическое имя либо IP-адрес устройства (если указать ключевое слово ALL, то это правило будет рассматриваться для всех устройств);

– 2-й блок – критерий важности согласно протоколу syslog (если указать ключевое слово NULL, то данное правило будет рассматриваться для всех критериев важности);

– 3-й блок – критичность события, которое было назначенное после обработки на серверной части системы (если указать ключевое слово NULL, то это правило будет рассматриваться для всех событий);

– 4-й блок – тип уведомления: 0 – ничего не показывать; 1 – появление всплывающего (неактивного) окна; 2 – мигание иконки клиентской части в меню systray; 3 – мигание иконки клиентской части в меню systray и появление сообщения в активном окне.

Все это позволяет добиться гибкости функции «Уведомление» в тех случаях, когда необходимо осуществлять жесткий мониторинг заданного сетевого устройства либо игнорировать любые сообщения от устройства при режиме тестовой отладки.

Таким образом, для получения оперативной информации о сбоях в работе сети в режиме реального времени система мониторинга узлов ЛВС, поддерживающих протокол syslog, должна быть разделена на серверную и клиентскую части. При этом серверная часть производит процедуру обработки и фильтрации по заданной администратором сети матрице сообщений и в зависимости от критериев важности осуществляет передачу зашифрованного сообщения о произошедшем событии клиентской части системы, которая осуществляет получение, дешифрование, хранение и уведомление администратора (либо обслуживающего ЛВС пер-

сонала) согласно установленному уровню критичности. Администратор и/или обслуживающий ЛВС персонал в случае сбоя или критического события (например, при угрозе безопасности узла) сетевого устройства получает уведомление о произошедшем событии в режиме реального времени, что позволяет оперативно предотвращать или исправлять возникшие неисправности.

Библиографические ссылки

1. Терентьев А. М. Задачи полноценного аудита корпоративных сетей // Концепции. 2003. № 1(11). С. 94–95.

2. Lonvick C. Request for Comments 3164. The BSD Syslog Protocol / Cisco Systems. San Jose, Calif., 2001.

3. Терентьев А. М. Методы и средства наблюдения загрузки локальных вычислительных сетей на примере ЦЭМИ РАН : препр. / Центр. экон.-мат. ин-т Рос. акад. наук. М., 2001. № #WP/2001/110.

4. Rose M. Request for Comments 3195 Reliable Delivery for syslog / Cisco Systems. San Jose, Calif., 2001.

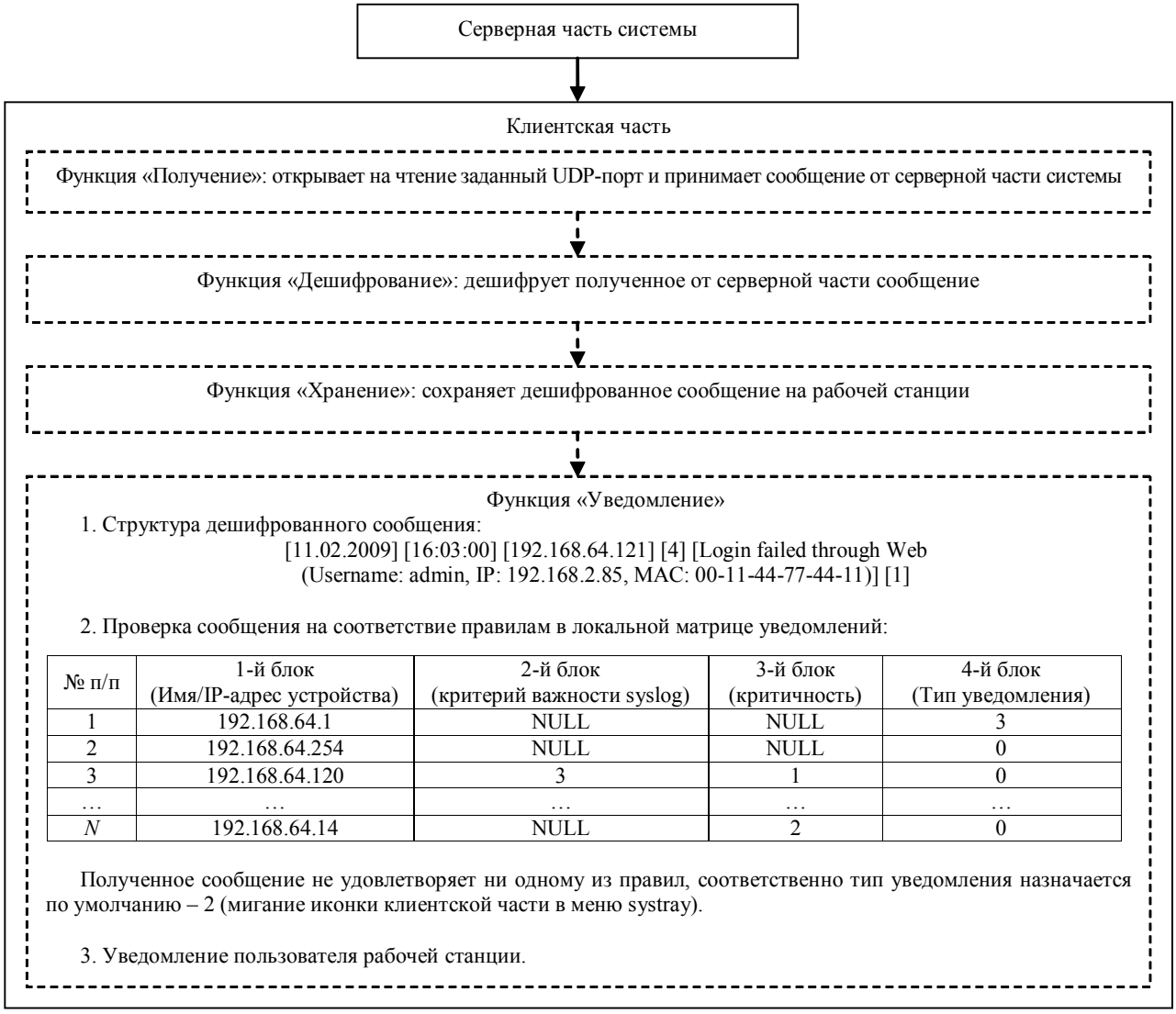

Рис. 3. Схема работы клиентской части системы мониторинга узлов ЛВС при получении сообщения от серверной части

I. V. Poturemskiy, A. V. Murygin

MONITORING SYSTEM OF LAN DEVICES BASED ON SYSLOG PROTOCOL

It is covered a monitoring system for LAN devices which support syslog protocol in real-time mode. The system is based on the processing of events which are registered in LAN devices. This allows receiving of reliable information about network status opportunely.

Keywords: monitoring LAN, syslog.