

**Курносов  
Юрий Анатольевич,**  
начальник отделения ЦИТСИЗИ УМВД России по  
Мурманской области, капитан внутренней службы



**Панов  
Владимир Николаевич,**  
инженер отделения ЦИТСИЗИ УМВД России по  
Мурманской области

### Состояние проблемы

При решении задач, стоящих перед органами внутренних дел, сегодня большую роль играют современные информационные технологии. Они используются для ускорения передачи информации между отделами, для упрощения документооборота, а также для реализации новых, более удобных и выгодных способов организации взаимодействия, таких, в частности, как видеоконференцсвязь и IP-телефония. Использование современной информационно-телекоммуникационной инфраструктуры прописано в Федеральном законе №3-ФЗ от 7 февраля 2011 г. «О полиции». Реализуется программа «Единая информационно-телекоммуникационная система органов внутренних дел», а также иные программы, направленные на развитие информационных технологий.

## Визуальное слежение за информационно-телекоммуникационной инфраструктурой УМВД России по Мурманской области

В целом объём технологий, используемых в повседневной деятельности ОВД, постоянно растёт, как растёт и зависимость ОВД от них. А именно — повышение эффективности от использования достижений прогресса означает, что в случае, скажем, часового простоя информационно-телекоммуникационной инфраструктуры количество невыполненной работы будет больше, чем когда эта инфраструктура функционирует без сбоев. В связи с этим значительно повышаются требования к бесперебойности работы информационных систем.

К сожалению, от аварий и неисправностей полностью застраховаться невозможно. Но вполне реально минимизировать ущерб, причиняемый ЧП служебной деятельности. Для этого необходимо незамедлительное реагирование на любую возникшую ситуацию. И здесь возникает проблема, связанная с особенностью эксплуатации современной информационно-телекоммуникационной инфраструктуры — «невидимость» аварий. Обычные происшествия заметны — пожар, автомобильная авария, крушение поезда... Их сложно не заметить. С авариями в информационных технологиях все иначе. К примеру, в безлюдном лесу может упасть дерево и оборвать кабели. Значительная часть информационно-телекоммуникационной инфраструктуры физически располагается в местах, где её не видно или она незаметна со стороны — серверные помещения, фальш-потолки, канализация, технические помещения, безлюдная местность вдоль дороги между городами. Заметить информационно-телекоммуникационную аварию, не связанную с каким-либо заметным происшествием, очень сложно.

Ещё большую сложность создаёт в этом вопросе, как ни странно, автоматизация рабочих процессов. Всё чаще и чаще непосредственным пользователем информационно-телекоммуникационной инфраструктуры становится не человек, а автоматизированное рабочее место, которое человеком только управляется. К



примеру, при отправке электронной почты человек формирует письмо и даёт команду АРМ отправить его. В случае аварии, не затрагивающей связь данного АРМ с почтовым сервером, отправка письма может пройти успешно, но адресату оно доставлено не будет. Адресат узнает об этом далеко не сразу. А если это письмо содержало срочную информацию? Зная об аварии, человек мог бы, допустим, отправить своё письмо по иному каналу связи. Если бы это был телефонный разговор, он сразу бы заметил, что собеседник его не слышит. Однако с отправкой почты такого не произойдёт. И это лишь один из примеров.

Для решения проблемы «невидимых» аварий был создан мониторинг — автоматизированный контроль состояния информационно-телекоммуникационной инфраструктуры. В УМВД России по Мурманской области он реализован на базе сервера с ОС GNU/Linux версии Calculate и представлен связкой ПО Nagios/Nagvis/Munin. Nagios в этой связке отвечает за опрос и хранение качественного состояния инфраструктуры, Munin собирает и хранит количественные показатели, а Nagvis отвечает за визуализацию. Все три программы доступны через веб-интерфейс, эксплуатируются с 2008 года и отлично себя зарекомендовали. Тем не менее мы снова упираемся в человеческий фактор — для реализации мониторинга с использованием этого комплекса необходимо постоянное слежение человеком за веб-интерфейсом, что практически невозможно в рабочих условиях. Подобная проблема является традиционной для всех организаций, в рабочем процессе которых присутствует монито-



ринг — центры управления, центры мониторинга... Существует два типа стандартных решений этой проблемы — установка большой видеостены с выводом всей необходимой информации, и установка информационного щита со световой индикацией. Решение с видеостеной является более гибким по выводимой информации и подходит для организаций с постоянно меняющимися наблюдаемыми объектами. Информационный щит же больше подходит для мониторинга жёстко зафиксированной структуры и значительно дешевле в изготовлении. Именно этот вариант и был выбран для визуализации состояния информационно-телекоммуникационной инфраструктуры УМВД России по Мурманской области.

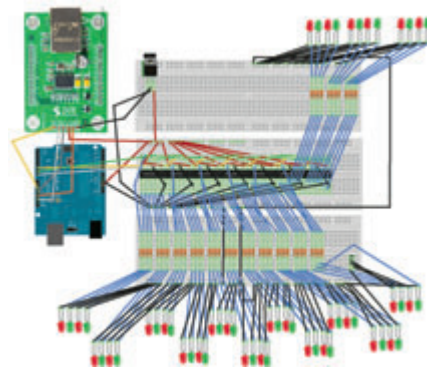
Для построения щита было использовано оргстекло, на которое были наклеены распечатанные карты города и области. Визуализация информации выполняется за счёт светодиодов. Для управления щитом используется микроконтроллер Arduino с подключенными сдвиговыми регистрами SN74HC595N. Передача контроллеру информации о состоянии инфраструктуры осуществляется по сети через Ethernet контроллером ENC28J60 с интерфейсом SPI. Питание осуществляется через 5 В (стабилизатор напряжения L7805CV) от обычного сетевого адаптера, в данном случае 9 В. Данный выбор комплектующих обеспечивает следующие преимущества:

1. Использование для управления системы выделенного микроконтроллера позволяет сделать щит не зависящим от состояния АРМ администраторов.



2. Выбор в качестве микроконтроллера Arduino обусловлен простотой реализации проектов на его основе.
3. Подключение светодиодов через сдвиговые регистры позволяет наращивать объём индицируемой информации практически неограниченно. Регистры соединяются цепью, и каждый регистр позволяет подключить 8 светодиодов.
4. Питание через стабилизатор позволяет использовать в качестве источника питания легко доступные сетевые адаптеры напряжением от 9 В до 15 В, не требуя каких-либо специализированных источников.
5. Контроллер использует ethernet-плату на основе чипа ENC28J60 с интерфейсом SPI, что позволяет ему получать информацию от сервера мониторинга по сети из любого места и не привязывает его к физическому расположению сервера.

Для микроконтроллера на основе примеров по работе с Ethernet-платой и сдвиговыми регистрами была собрана простая прошивка, реализующая функционал веб-сервера. Необходимое состояние светодиодов передаётся через GET-запрос строкой вида <http://10.80.4.222/?raw=01101001>



0100101...01001. Такой подход позволяет написать простую программу и интегрировать информационный щит практически в любую систему, не привязывая его к конкретному ПО мониторинга.

В нашем случае для интеграции с Nagios был использован тот факт, что Nagios с модулем ndodb помещает все результаты опроса состояния инфраструктуры в БД MySQL. Был написан простой Perl-скрипт, который SQL-запросом получает состояние логически объединённых объектов — Хост-групп — и формирует строку запроса к щиту. Впрочем, для данной задачи можно выбрать абсолютно лю-



бой язык программирования, позволяющий делать HTTP GET-запросы и имеющий доступ к данным системы мониторинга.

### Перспективы развития

В своём текущем виде информационный щит отражает общую ситуацию по области, имеет всего два типа индикации для каждого города — зелёный и красный, и учитывает только сетевую доступность объектов внутри группы — полная доступность обозначается зелёным светодиодом, недоступность хотя бы одного объекта (к примеру, выключенного на техобслуживание сервера) зажигает красный светодиод для всего города. В перспективе планируется добавить индикацию для всех площадок внутри областного центра и расширить диапазон выводимых состояний за счёт учёта не только сетевой, но и функциональной доступности. К примеру, мигание красного светодиода совместно с постоянно горящим зелёным может означать нарушения в работе инфраструктуры, не приводящие к разрывам связи, такие как повышенная загрузка канала или падение какой-либо сетевой службы на одном из серверов. Также возможен вывод на щит отдельно состояния оборудования в главном здании. Подобное расширение позволит не только реагировать на непосредственные угрозы инфраструктуре, но и оперативно устранять проблемы на этапе зарождения. К примеру, своевременное выявление вышедшей из строя батареи ИБП на удалённой площадке позволяет предотвратить возможные проблемы в будущем в случае непредвиденного отключения электропитания.

Также стоит отметить, что подобный информационный щит является универсальным решением для мониторинга и может быть использован не только для слежения за состоянием информационно-телекоммуникационной инфраструктуры, но и для множества иных задач.