паролі доменних користувачів зберігаються на виділених серверах контролерах домену, які, як правило, захищені від зовнішнього доступу. По-друге, при використанні доменної середовища для аутентифікації використовується протокол *Kerberos*, який значно безпечніше, ніж *NTLM*, що використовується в робочих групах.

- Інтеграція з корпоративними програмами та обладнанням

Великою перевагою служб *Active Directory* є відповідність стандарту *LDAP*, який підтримується іншими системами, наприклад, поштовими серверами (*Exchange Server*), проксі-серверами (*ISA Server*, *TMG*). Причому це не обов'язково тільки продукти *Microsoft*. Перевага такої інтеграції полягає в тому, що користувачеві не потрібно пам'ятати велику кількість логінів і паролів для доступу до того чи іншого додатку, у всіх додатках користувач має одні й ті ж облікові дані – його аутентифікація відбувається в єдиному каталозі *Active Directory*. *Windows Serve*r для інтеграції з *Active Directory* надає протокол *RADIUS*, який підтримується великою кількістю мережевого обладнання. Таким чином, можна, наприклад, забезпечити аутентифікацію доменних користувачів при підключенні по *VPN* ззовні, використання *Wi-Fi* точок доступу в компанії.

- Єдине сховище конфігурації додатків.

Деякі програми зберігають свою конфігурацію в *Active Directory*, наприклад, *Exchange Server*. Розгортання служби каталогів *Active Directory* є обов'язковою умовою для роботи цих додатків. Зберігання конфігурації додатків в службі каталогів є вигідним з точки зору гнучкості і надійності. Наприклад, у разі повної відмови сервера *Exchange,* вся його конфігурація залишиться недоторканою. Для відновлення працездатності корпоративної пошти, достатньо буде перевстановити *Exchange Server* в режимі відновлення.

Н. Бржезинский,
студент 5 курса факультета
Компьютерных наук и инновационных технологий,
Международный гуманитарный университет;
руководитель – д-р. техн. наук, проф. В. В. Никольский

УСОВЕРШЕНСТВОВАНИЕ ИНФОРМАЦИОННОЙ КОМПЬЮТЕРНОЙ СЕТИ ПРЕДУПРЕЖДЕНИЯ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

В настоящее время стремительного технического прогресса, противопожарная безопасность является весьма актуальной. Электроника и разнообразная бытовая техника – это начинка практически любого офиса, жилого помещения, учебного учреждения или завода. Так как все эти элементы являются потенциально пожароопасными, то и обязательное присутствие в любом помещении пожарного оборудования это необходимость.

Противопожарное оборудование – это обширный перечень приспособлений и агрегатов, от простейших бытовых огнетушителей до пожарной специальной техники.

Базовая задача противопожарного оборудования – минимизация последствий возгорания. В идеале, с помощью пожарного оборудования, очаг возгорания должен быть потушен еще до приезда пожарного расчета МЧС. Вот почему важнейшую роль в этом играет грамотное размещение, качество и производительность работы пожарного оборудования.

Пожарное оборудование, необходимо абсолютно в любом помещении, независимо от его площади и цели использования.

Пожарное оборудование – это не единственное, что может помочь в ликвидации пожара. Оптимальная эффективность достигается при осуществлении комплексного подхода к решению вопроса противопожарной защиты. Кроме обязательных огнетушителей, крайне желательно оборудовать помещение системами дымоудаления, датчиками движения, системами оповещения и пожаротушения, проще говоря, системами контроля предупреждения чрезвычайных ситуаций. В зависимости от типа объекта, возникает целесообразность установки той или иной пожарной сигнализации.

Датчики, установленные на объекте, имеют заданный порог срабатывания, и если температура или задымленность (в зависимости от типа датчиков) превышает допустимые нормы, подается сигнал тревоги. Они соединяются с автоматизированной панелью управления, которая передает сигнал бедствия на пульт управления охраны или сразу же в службу спасения. Но наиболее результативно соединять датчики с системой автоматического пожаротушения.

Еще несколько лет назад Ethernet считался не самым подходящим интерфейсом передачи данных в системах реального времени, куда с некоторой натяжкой можно отнести и системы охранно-пожарной сигнализации.

Дело в том, что основным недостатком этого интерфейса является способ доступа оборудования к среде передачи данных CSMA/CD (множественный доступ с контролем несущей и обнаружением коллизий). Все устройства в сети имеют равные права на передачу, время доступа регламентируется случайной задержкой, а контроль коллизий в Ethernet разрушающий, т. е. при одновременном выходе на линию нескольких передатчиков, происходит искажение передаваемых данных, прекращается работа всех передатчиков на некую случайную величину времени, и затем передача повторяется. Все это может приводить к непредсказуемым задержкам в передаче данных, что во многих приложениях недопустимо.

Поэтому в свое время считалось, что для критических к времени передачи задач следует применять опросные системы, где время доставки данных определено и гарантировано. В основном по такому принципу работают так называемые полевые шины Profibus, Modbus. А также протоколы с неразрушающим контролем коллизий на основе приоритетов сообщений, такие как CAN.

Однако со временем Ethernet благодаря повсеместности применения и вследствие этого дешевизны смог проникнуть и в сферу промышленной автоматики. Появился стандарт Industrial Ethernet, который обеспечивает регулярную и частую передачу по сети небольших объемов информации, что характерно для обмена данными между контроллерами. Кроме того, с помощью специальных коммутаторов можно организовать кольцевую топологию линии связи, которая при обрыве восстанавливает связь, что позволяет значительно повысить живучесть системы.

Сегодня уже, наверное, не осталось ни одной отрасли приборо или машиностроения, куда бы ни проникли IP-технологии. Широкое распространение они получили и в системах безопасности. Более всего они востребованы в охранном телевидении в связи с огромным объемом передаваемых видеоданных. Всеобщая IP-зация не обошла стороной и системы охранно-пожарной сигнализации.

Сейчас уже значительное количество выпускаемых приемно-контрольных приборов имеет встроенный интерфейс Ethernet. IP-соединение используется для связи с ПЭВМ верхнего уровня, а также для объединения отдельных приборов в сеть. В ряде

приборов имеется встроенный web-сервер, что позволяет подключаться к нему без специального программного обеспечения, используя лишь стандартный браузер. Если же в ПК нет встроенного интерфейса, то в большинстве случаев подключить прибор в сеть можно с помощью преобразователя интерфейсов, например RS-232 – Ethernet.

Подключение к ПЭВМ через Ethernet имеет целый ряд преимуществ перед традиционным способом подключения по последовательным интерфейсам RS-232 или RS-485. Большинство объектов уже имеет развитую сетевую инфраструктуру, поэтому отпадает необходимость прокладки отдельной кабельной линии от приборов до ПЭВМ. Приборы могут быть размещены в любом месте объекта охраны, в пределах охвата локальной сети. В случае выхода из строя ПЭВМ появляется возможность в автоматическом режиме перевести подключение приборов на резервный компьютер.

В отличие от систем охранного телевидения объем передаваемых данных в охранно-пожарной сигнализации крайне мал и практически не оказывает никакого влияния на загрузку сети, что позволяет использовать общую сеть предприятия без риска конфликтов с другими сетевыми приложениями. В то же время остаются открытыми вопросы безопасности передачи данных, если используется сеть общего назначения. Для защиты передаваемых данных крайне желательно использовать шифрование или организовать для системы безопасности виртуальную выделенную сеть (VPN). В идеальном варианте это организация своей собственной физически выделенной сети. Это решит если не все, то многие вопросы и с защитой, и с надежностью. Ведь если охранно-пожарная сигнализация не оказывает большое влияние на другое оборудование, подключенное в ту же сеть, то обратное вполне возможно. И в случае каких-либо неполадок в сети по вине стороннего оборудования есть большой риск сбоя, и в работе системы охранной или пожарной сигнализации, что, крайне нежелательно.

Сетевое подключение дает широкие возможности по организации совместной работы непосредственно между приборами охранно-пожарной сигнализации. К примеру, обмен тревожными событиями или управление постановкой на охрану с пульта, подключенного к одному прибору шлейфами на другом приборе. Ethernet является идеальным решением для построения распределенных систем безопасности. Как правило, распределенная система объектов уже связана корпоративной сетью передачи данных. В этом случае мы получаем готовую транспортную сеть для централизованного администрирования, управления системой, создания единого корпоративного центра реагирования.

Глобальные сети могут использоваться для организации централизованной охраны коммерческих и частных объектов. Уже сейчас интернет используется для связи объекта охраны с пунктом централизованной охраны. Более того, владелец может через тот же интернет получать информацию, о состоянии своего объекта и даже управлять им. Конечно же, если система безопасности имеет выход в интернет, задачи защиты от искажения передаваемых данных или несанкционированного доступа к управлению выходят на первый план.

Как уже говорилось выше, в настоящее время в основном Ethernet используется для связи приемно-контрольных приборов между собой или с верхним уровнем. Иногда через IP связываются адресные расширители с центральной панелью. Новым этапом в развитии IP-технологий в охранно-пожарной сигнализации может стать появление на рынке извещателей с встроенным интерфейсом Ethernet. Этому способствует все большее распространение технологии Power over Ethernet (или PoE – стандарт IEEE 802.3af). PoE – это технология, позволяющая передавать удаленному устройству вме-

сте с данными электрическое питание через стандартную витую пару в сети Ethernet. Данная технология предназначена прежде всего для IP-телефонии, точек доступа беспроводных сетей, web-камер, сетевых концентраторов и других устройств, к которым нежелательно или невозможно проводить отдельный электрический кабель.

Данное решение вполне подходит для подключения охранных и пожарных извещателей. В этом случае система охранно-пожарной сигнализации будет представлять собой приемно-контрольный прибор, транспортную систему Ethernet, по которой вместе с данными передается питание и извещатели, к каждому из которых подключается сетевой патчкорд от ближайшего концентратора. При этом значительно упростится монтаж и пусконаладка системы, снизится стоимость работ. В процессе эксплуатации упрощается модернизация системы.

При наличии на объекте структурированной кабельной системы (СКС) добавить новый извещатель или перенести ранее установленный в другое место будет очень не сложно. Конечно, наличие в каждом датчике встроенного Ethernet интерфейса, причем в случае использования PoE еще и сплиттера (разделителя, который отделяет цифровые данные от электропитания и подает их на два разных выхода) удорожает изделие. Но все, что связано с IP-технологиями, стремительно дешевеет. И конечно, не нужно забывать, что кабельная система при этом разделяемая с другими приложениями и системами здания, что значительно удешевляет проект в целом.

За основу магистерской работы взят Международный гуманитарный университет, а точнее его охранно-пожарная система. Будет предложен и рассмотрен новый вариант этой системы, который значительно будет отличаться от предыдущей в плане ценовой и практической политики.

Мауя А. Бургила,
студент 6 курсу факультету
Комп'ютерних наук та інноваційних технологій,
Міжнародний гуманітарний університет;
керівник – д-р. техн. наук, проф. С. А. Михайлов

РОЗРОБКА СТРУКТУРИ ЕЛЕКТРОННОГО РЕЄСТРАТОРА ДАНИХ («ЧОРНОЇ СКРИНЬКІ») МОРСЬКОГО СУДНА

Офіційна назва нового електронного пристрою, яким незабаром належить оснастити більшість судів – Реєстратор Даних Рейса – РДР (Voyage Data Recorder – VDR) або, як його називають з відтінком трагедії, «чорний ящик». Мається на увазі, що, як в міфічному ящику Пандори, в ньому берегтимуться всі біди і неприємності, що виникли на шляху судна. Насправді – це електронна комп'ютерна система, створена для запису і тривалого зберігання інформації від різних джерел, таких, як станції (РЛС) радіолокацій, суднові системи, зв'язне радіоустаткування, інформація з містка, аварійна сигналізація та ін. Причому збереження записаної інформації забезпечується, у тому числі, при пожежі, вибуху, глибокому зануренні реєстратора VDR під воду. VDR записує майже всі навігаційні параметри і інформацію з містка, включаючи голосові розмови і радіозв'язок, а також дані РЛС. Записана інформація об'єднується і синхронізується в часі, що дозволяє судновласнику і відповідним органам легко проводити розслідування у разі якого-небудь інциденту на борту судна або в безпосередній близькості від нього.