несанкционированного проникновения нарушителя на территорию охраняемого объекта происходит оповещение подразделения охраны.

На сегодняшний день видеонаблюдение стало неотъемлемой частью комплексной системы безопасности любого объекта. Если охраняемый объект большой, то оператору сложно уследить за всеми событиями, происходящими в защищаемой зоне. В таких случаях оправдано использование систем видеоаналитики, которые позволяют анализировать материал, поступающий с видеокамер, в режиме реального времени либо в виде архивных записей, а затем в автоматическом режиме собирать данные и формировать отчеты по различным инцидентам информационной безопасности. Также широко используется возможность создавать визуальные зоны охраняемого объекта и при нарушении их, формировать сигнал тревоги. Сбор данных проходит без участия оператора, однако при фиксации инцидентов, связанных с безопасностью, системы видеоаналитики извещают об этом сотрудника службы безопасности.

Программная часть может включать в себя модули распознания лиц (интеграция с базой МВД), распознания автомобильных номеров, отслеживания движущихся объектов, детекции дыма, огня и звука, контроля активности персонала, обнаружения оставленных предметом и прочие, а также кодеки для сжатия видеосигнала. Аппаратная часть включает серверы видеозаписи, коммутаторы, мониторы, дисковые массивы, камеры различного типа (PTZ- и IP-камеры, тепловизоры).

Архитектура территориально-распределенной системы защиты периметра с использованием видеоаналитики предполагает передачу данных по IP-сетям, а также возможность интеграции с облачными сервисами. При этом возникают такие угрозы информационной безопасности, как несанкционированное прослушивание трафика, его модификация, проведение атаки типа отказ в обслуживании (DoS). Наиболее эффективным решением этих проблем является использование криптографической защиты. Однако, применение криптографии приводит к увеличению объема передаваемого трафика (так называемый IPsec Overhead при использовании VPN-тоннелей), а значит требуются каналы связи с высокой пропускной способностью. Также актуальным вопросом становится аппаратная поддержка алгоритмов шифрования используемым процессором.

ПРИМЕНЕНИЕ СЕРВИСА SELFPORTAL ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОГО КОНТРОЛЯ РЕСУРСОВ ПРЕДПРИЯТИЯ

А.С. Петрович, И.С. Зайкина

Применение в корпоративных сетях технологий виртуализации получило большую популярность. Предприятие занимается ИТ-аутсорсингом и предоставляет ресурсы сотрудников сторонним организациям. В связи с данной спецификой работы, в рабочем процессе может применяется нескольких систем виртуализации: VMWare, vSphere и OpenStack. Для удобного управления, обеспечения безопасного контроля ресурсов и экономии бюджета предприятия используется бесплатная система SelfPortal [1].

Безопасный контроль достигался за счет решения двух основных проблем, возникших при росте количества виртуальных машин на предприятии. Первая проблема заключается в неконтролируемом росте числа машин ввиду отсутствия правильной системы контроля за высвобождением неиспользуемых вычислительных мощностей. С увеличением количества виртуальных машин пропорционально увеличивалось количество векторов атак, которые могли бы быть потенциально использованы злоумышленниками. Вторая проблема – это необходимость построения закрытого участка инфраструктуры, который считался бы небезопасной зоной для проведения тестирования. Ресурсы такой зоны могли бы свободно выделяться пользователям без риска для основной системы.

В докладе обсуждается эффективность применения системы SelfPortal в вычислительной сети крупного предприятия. Данное средство позволило не только обеспечить контроль ресурсов предприятия, но и сократить время на развертывание виртуальных машин (конечный пользователь может получать доступ к сложным системам всего за 15 минут, до применения системы – в среднем 45 минут). Эффективность возросла

за счет упрощения настройки виртуальной машины, предоставляя «из коробки» самые распространенные конфигурации. Таким образом, около 70% запросов на проведение работ по развертыванию виртуальных машин отпадают за счет самообслуживания пользователей, что значительно облегчает работу системного администратора.

Литература

1. Open-sourcing SelfPortal [Электронный ресурс]. – URL: https://www.altoros.com/blog/introducing-selfportal-the-panel-to-launch-virtual-machines-in-a-few-clicks/. (дата обращения: 14.05.2018).

УЛУЧШЕНИЕ ХАРАКТЕРИСТИК ДАТЧИКОВ ЗВЕЗДНОГО НЕБА ПУТЕМ ЭЛЕКТРОХИМИЧЕСКОГО ОКРАШИВАНИЯ

А.А. Повжик, А.А. Устименко

Формирование механически прочных и стойких к ультрафиолетовому излучению анодных покрытий на основе пористого оксида алюминия с упорядоченными сквозными порами – капиллярами микро- и наноразмеров является актуальной задачей. Значительный интерес вызывает использование таких покрытий для элементов конструкции датчика звездного неба с минимальным коэффициентом отражения в оптическом диапазоне.

Возможность контролируемого изменения размеров пор и толщины пористой структуры делает пористый оксид алюминия идеальным материалом для создания наноструктур с заданными структурными параметрами и свойствами. Широкие возможности управления структурными параметрами пористого оксида алюминия и получения на его основе различных наноструктурированных материалов делают исследования в данном направлении весьма актуальными.

Одним из важнейших показателей качества датчика звездного неба является коэффициент отражения, который должен стремиться к нулю. Для достижения этой цели проводят электрохимическое окрашивание алюминиевой конструкции датчика. Электрохимическое окрашивание по сравнению с химическим окрашиванием имеет ряд преимуществ. К примеру, исследование воздействия УФ излучения на покрытия с электрохимической окраской и химической окраской красителями показало, что покрытия, окрашенные электрохимическим методом, не изменяют своей способности к поглощению света после воздействия УФ, что позволяет нам говорить об использовании данных покрытий в условиях космоса, в то время, как у покрытий с химическим окрашиванием после воздействия УФ-излучением наблюдается снижение коэффициента поглощения.

ПРИМЕНЕНИЕ VPN ДЛЯ ЗАЩИТЫ ТРАФИКА

В.М. Прудников, Е.А. Якимов

Технология виртуальных частных сетей Virtual Private Network (VPN) является одним из эффективных механизмов обеспечения информационной безопасности при передаче данных в распределенных вычислительных сетях, позволяет реализовать совокупность различных самостоятельных механизмов безопасности [1, 2].

Безопасная передача данных по незащищенной вычислительной сети использует понятие защищенного канала. Защищенный канал можно построить с помощью системных средств, реализованных на разных уровнях эталонной модели OSI взаимодействия открытых систем. Используемый уровень OSI в основном определяет достижимые функции применяемой VPN, ее совместимость с программами информационной системы и взаимодействие со средствами защиты других реализаций. В соответствии с уровнями модели OSI различают VPN второго (канального) уровня, третьего (сетевого) уровня, пятого (сеансового) уровня.

Для защиты передаваемого трафика при построении VPN применяются протоколы нижних уровней модели OSI, что обеспечивает прозрачность для приложений и прикладных протоколов информационной системы. При этом обнаруживается проблема корреляции протоколов защиты от используемых стандартов сетей. При применении протоколов верхних уровней способ защиты трафика теряет корреляцию с сетевыми технологиями, что дает определенные преимущества, но при этом протокол теряет прозрачность и приложение зависит