ответный сигнал, который принимается антенной считывателя, обрабатывается его электронным блоком и по интерфейсу направляется в компьютер. Таким образом, ридер имеет приемо-передающее устройство и антенну, которая посылает сигнал идентификатору и принимает ответный сигнал. До последнего времени RFID-системы были более дорогими по сравнению со штрих-кодовыми системами бесконтактной идентификации. Однако прогресс в области идентификаторов и использование новых радиоинформационных технологий привели к тому, что они стали применяться в областях, в которых раньше использовались только штрих-коды.

Мы предлагаем использовать управление системой обратной связи с ридером RFID, применяя модуляцию положением импульса (Pulse Position Modulation, PPM) путем генерирования временных перескоков сверхширокополосных сигналов (Ultra Wide Band, UWB). Использование таких сигналов является наиболее эффективным способом борьбы с подслушиванием, так как злоумышленник практически не может обнаружить выполнение обмена информацией в работающей системе радиочастотной идентификации объектов, поскольку сигналы UWB дают возможность восстановить данные, даже если мощность сигнала вплотную подходит к уровню теплового шума. В докладе изложены результаты моделирования сигналов UWB гауссовской формы и их корреляционной обработки, выполненного в математическом пакете прикладных программ MATLAB. Расчеты проведены для импульсов длительностью от 0,2 до 0,8 пс гауссовсой формы.

ФОРМИРОВАНИЕ ФРЕЙМА ДАННЫХ ДЛЯ ЗАЩИЩЕННОЙ СИСТЕМЫ РАДИОЧАСТОТНОЙ ИДЕНТИФИКАЦИИ ОБЪЕКТОВ

В.Т. Першин

В докладе предлагается использовать фрейм длительностью 10 мс для защищенных систем радиочастотной идентификации (Radio Frequency IDentification, RFID) объетов, отводя при этом интервал длительностью 2 мс на преамбулу для обеспечения синхронизации ридера с идентификатором, а оставшуюся часть фрейма отвести под передачу данных. Позиции импульса выбираются посредством криптографического секретного псевдослучайного генератора чисел (Cryptographically Secure Pseudo Random Number Generator, CSPRNG), так как CSPRNG используется для выбора кода модуляции более эффективно, чем для шифрования. В этом случае можно использовать простой блок шифра, работающего в цепи обратной связи. В предлагаемом формате фрейма можно использовать 16-битный блок шифра, так как никакой стандартный код не использует коды такой длины блока, и выбирать его можно вместо достаточно широко применяемого 64-битного кода, формируя выход каждого шифра для 4 подпоследовательностей позиций импульса в сверхширокополосных сигналах (Ultra Wide Band, UWB). Ключ блока шифра предопределяется секретом, известным ридеру и идентификатору. декодирование сигнала требует, чтобы декодер имел надежную синхронизацию передатчика и приемника. В большинстве случаев реализовать этот механизм не получается, так как собственно используемый сигнал не обеспечивает уверенное декодирование, поэтому для восстановления синхронизации можно использовать манчестерское кодирование информации или применять дифференциальную PPM, так как такая версия кодирования фактически передает данные без использования синхронизации. В этом случае задержка между импульсами не опирается на передний фронт импульса синхронизации. Вместо этого каждая задержка опирается на задний фронт предыдущего импульса. При дифференциальной PPM длительность кодированного сигнала не фиксируется, в то время, как простая PPM всегда создает кодированный сигнал фиксированной длительности, которая формируется только количеством битов и периодом синхронизации.

СИСТЕМА ОХРАННОГО ТЕЛЕВИДЕНИЯ С ДОПОЛНЕНИЕМ ВИДЕОНАЛИТИКИ

С.Н. Петров, Д.В. Ахраменко, С.В. Власюк

Система охранного телевидения предназначена для визуального контроля обстановки на охраняемом объекте с использованием средств телевизионной техники и формирования сигнала тревоги при детектировании проникновения на объект. При попытке

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