

ответный сигнал, который принимается антенной считывателя, обрабатывается его электронным блоком и по интерфейсу направляется в компьютер. Таким образом, ридер имеет приемно-передающее устройство и антенну, которая посылает сигнал идентификатору и принимает ответный сигнал. До последнего времени RFID-системы были более дорогими по сравнению со штрих-кодowymi 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 гауссовской 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) объектов, 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