позволяет повысить качество и эффективность подготовки специалистов. К таким инструментам относится электронный учебно-методический комплекс (ЭУМК), представляющий собой программно-методический обучающий комплекс, включающий систематизированные учебные, научные и методические материалы по учебной дисциплине и призван обеспечить реализацию учебных целей и задач на всех этапах образовательного процесса.

В данной работе авторы рассматривают использование материалов авторского ЭУМК как возможные пути повышения эффективности учебного процесса в рамках перехода на двухуровневую систему высшего образования «бакалавр-магистр».

Дисциплина «Квантовые системы для обеспечения информационной безопасности» II-ой ступени высшего образования заочной формы обучения учреждения образования «Белорусская государственная академия связи» специальности 1-98 80 03 «Аппаратное и программно-техническое обеспечение информационной безопасности» призвана формировать у обучающихся теоретические знания и практические навыки, необходимые для разработки и проектирования квантовых систем безопасности различного уровня и назначения.

ЗАЩИТА ИНФОРМАЦИИ ПРИ ОБРАБОТКЕ ЭЛЕКТРОННЫХ МЕДИЦИНСКИХ КАРТ

В.И. Пачинин, В.А. Пуйдак, Г.В. Сечко, М.А. Тимонович, И.С. Харкевич

Рассматривается защита конфиденциальной персональной информации пациентов в белорусских медицинских учреждениях. Источником такой информации может быть электронная медицинская карта (ЭМК), широкое внедрение которой в поликлиниках Минска началось в 2018 г. и согласно планам Министерства здравоохранения Республики Беларусь должно полностью завершиться к 2020 г. По мнению авторов доклада, внедрение ЭМК в Беларуси будет осложнено отсутствием белорусского закона «О персональных данных», проект которого Национальное собрание Республики Беларусь планирует обсуждать только в 2019 г. Таким образом, сегодня в Беларуси никто не требует у пациента согласия на обработку его персональных данных из ЭМК, что предусмотрено статьей 6 (пункт 1 подпункт 1.1) закона Российской Федерации «О персональных данных» от 27.07.2006 № 152-ФЗ. Следовательно, доступ к персональным данным пациента при обработке ЭМК автоматически получает целый круг медицинских работников, обрабатывающих данные [1], а правовой гарантии защиты этих данных в Беларуси пока нет. В этом аспекте в России у пациента больше возможностей: не согласившись на обработку своих данных без своего участия пациент может разместить эти данные в архиве, доступ к которому будет иметь только он с помощью системы распознавания личности по радужной оболочке глаза (РОГ) [1]. Стоимость такой системы в последние годы резко снижается за счет сканирования РОГ с помощью смартфона. Обработку данных из архива медицинский работник сможет вести только в присутствии пациента и под его контролем (либо в присутствии доверенного лица пациента, имеющего доступ к архиву). Тем самым пациент получит высокий уровень защиты своих данных (если ему это, конечно, необходимо).

Литература

1. Ситник, М. Ю. Состояние защиты персонифицированных медицинских данных в Беларуси в 2018 году // Материалы 54-й науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8 «Информационные системы и технологии». Минск, 21 апреля 2018 г. С. 92–94.

ИСПОЛЬЗОВАНИЕ МОДУЛЯЦИИ ПОЛОЖЕНИЕМ ИМПУЛЬСА В ТЕХНОЛОГИИ РАДИОЧАСТОТНОЙ ИДЕНТИФИКАЦИИ ОБЪЕКТОВ

В.Т. Першин

Система радиочастотной идентификации (Radio Frequency IDentification, RFID) объектов в общем случае содержит три компонента: считыватель (ридер), идентификатор (карта, метка, тег) и компьютер. Считыватель излучает в окружающее пространство электромагнитную энергию. Идентификатор принимает сигнал считывателя и формирует

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