ID: 2014-07-231-A-4061 Оригинальная статья

Кульминский Д.Д., Караваев А.С., Пономаренко В.И., Прохоров М.Д.

Система скрытой передачи данных в медицинских информационных системах, основанная на хаотической синхронизации генераторов с запаздывающей обратной связью

Саратовский филиал Института радиотехники и электроники им. В.А. Котельникова РАН
Саратовский государственный университет имени Н.Г. Чернышевского

Резюме

Разработана система скрытой передачи информации на базе хаотических генераторов с запаздыванием, перспективная для обеспечения скрытой передачи данных медицинских информационных систем и медицинского оборудования.

Ключевые слова: передача данных, медицинские информационные системы

Введение

Сегодня остро стоит вопрос защиты персональных данных граждан, обрабатываемых в информационных системах. Одним из наиболее важных классов таких систем являются медицинские информационные системы (МИС).

Основная функция МИС [1-5] – поддержка деятельности лечебного учреждения. Главное отличие такой системы от других программных продуктов прежде всего в том, что в ней хранится и обрабатывается персональная и конфиденциальная информация. Юридически медицинские сведения о пациентах относятся к информации, составляющей профессиональную тайну, доступ к ней ограничен и регламентируется действующим законодательством [6]. В соответствие с этим в МИС обязательно должен быть реализован ряд мер по обеспечению безопасности, как информации, так и информационной системы в целом, в противном случае использование данной МИС неправомерно. Поэтому обеспечение безопасности и конфиденциальности данных – одно из ключевых требований, предъявляемых к современной МИС, а также реализация в информационно-коммуникационных и вычислительных системах данного условия являются актуальными задачами [7].

На текущий момент защита личных данных в МИС представлена двумя базовыми аспектами. Первым из них является этический (профессиональный) аспект взаимодействия врача и пациента, который регулируется нормами врачебной этики и законом о защите личных данных пациентов. Второй аспект представляет собой защиту информации в медицинской системе с технической точки зрения, то есть, здесь речь идет о создании адекватных механизмов защиты данных непосредственно в рамках программно-аппаратного комплекса информационной системы [8, 9].

Считается, что до 60% утечек медицинской информации происходит из-за действий медицинских работников, причем, не только лечащих или консультирующих врачей, но и обслуживающего и административного персонала медучреждений. Основные факты нарушения и утечки информации происходят не по каналам связи, как иногда пытаются объяснить, а через конкретных людей, которые выносят сведения за пределы организации. Однако применение адекватных административных мер резко снижает вероятность таких утечек.

По техническим причинам происходит порядка 40% утечек информации: взломы информационных систем злоумышленниками, хищения баз данных и персональных компьютеров и др. Причем технический аспект утечки частной информации поддается контролю существенно хуже субъективных факторов [10].

Сейчас резко увеличивается количество используемой медицинской техники, следовательно, возрастает и значимость организационной и программно-технической защиты от несанкционированного доступа. Сегодня, в большинстве случаев, на этапе проектирования не учитываются вопросы информационной безопасности.

Особенности требований к информационной безопасности передачи данных медицинских приборов обычно включают невысокие требования на криптоустойчивость канала и обеспечение обмена нерегулярными транзакциями малыми объемами информации в реальном времени. Развитые в настоящее время системы скрытия информации представлены системами пакетного кодирования с открытым ключом и плохо подходят для решения таких задач, т.к. требуют предварительного накопления значительных по объему пакетов информации.

Нами разработана система скрытой передачи данных с потоковым кодированием, отличающаяся относительной технической простотой и ориентированная на скрытие информации при передаче данных от медицинского оборудования.

Система передачи информации

В ходе проведенных исследований была разработана и создана система скрытой передачи данных, включающая хаотический передатчик, реализованный в виде радиофизического устройства, проводной аналоговый канал связи и приемник, реализованный на базе 8 битного микроконтроллера (МК) Atmel megaAVR.

Передатчик включает три основных структурных элемента: линию задержки (ЛЗ) с 2 отводами, нелинейный элемент (НЭ) и инерционный элемент. При этом все элементы реализованы в цифровом виде на базе МК Atmel ATmega48PA.

Такая реализация передатчика позволяет использовать ЛЗ длиной в сотни отсчетов дискретного времени, причем длина ЛЗ ограничивается только объемом доступной оперативной памяти МК. Кроме того, цифровая реализация НЭ позволяет осуществлять достаточно сложные нелинейные преобразования сигналов, задавая параметры с высокой точностью. Вместе с тем, наличие аналогового канала позволяет рассматривать передатчик, как полноценное аналоговое радиофизическое устройство и успешно моделировать эффекты, связанные с прохождением хаотических сигналов через аналоговые элементы.

Динамическая переменная $x(t)$ представляет собой знаковое целочисленное 16 битное число. Линейное преобразование сигнала $x(t)$ осуществлялось нами с помощью низкочастотного цифрового фильтра Баттерворта первого порядка

В зависимости от уровня бинарного информационного сигнала $m(t)=\{0,1\}$, подаваемого на вывод цифровой линии МК, программа обеспечивает выборку задержанного значения из ЛЗ. Ключ S1 реализован программно.

Bulletin of Medical Internet Conferences (ISSN 2224-6150)
2014. Volume 4. Issue 7

Сигнал $x(t-(\tau_1+m(t)\tau_2))$ проходит через НЭ и подвергается нелинейному преобразованию. В работе использовался НЭ с квадратичной нелинейностью. На его выходе присутствует сигнал $\lambda * A - x^2(t-(\tau_1+m(t)\tau_2))/A$, где A – масштабный коэффициент ($A = 2^{14}$).

Далее очередная динамическая переменная помещается в ЛЗ.

Для корректного преобразования знакового цифрового сигнала на выходе НЭ униполярным ЦАП значение на выходе НЭ сдвигается на постоянную величину путем добавления к нему 32768 (половина диапазона). Полученный неотрицательный сигнал преобразуется в аналоговый посредством прецизионного 16 битного ЦАП Analog Devices AD5063. в диапазон от 0 В до $V_{ион}$ В, соответственно. $V_{ион}$ В – напряжение на выходе встроенного в МК источника опорного напряжения (ИОН) и $V_{ион}$ =1.1В. Данные в ЦАП передаются через встроенный в МК трехпроводной высокоскоростной интерфейс Serial Peripheral Interface (SPI).

Арифметические вычислении аналогичны используемым в схеме с нелинейным подмешиванием [11], однако задержка реализована по-другому.

Аналоговый сигнал на выходе ЦАП:

$$\dot{s}x(t) = -x(t) + \lambda * A - x^2(t-(\tau_1+m(t)\tau_2))/A,$$

где время инерционности фильтра: ε = 2, параметр нелинейности: λ = 1,99, время задержки: τ_1 = 100, τ_2 = 10, масштабный коэффициент: $A = 2^{14}$.

В проводной аналоговый канал связи передается сигнал динамической переменной $x(t)$.

Добавление 32768 перед ЦАП является лишь технической операцией, необходимой при использовании ЦАП с униполярным динамическим диапазоном. На динамику системы эта операция не влияет, поэтому она не выписывались явно при выводе уравнения.

Момент запуска очередного преобразования хаотического генератора определялся с помощью точного 16 битного таймера, встроенного в МК. Частота прерывания таймера 1кГц., т.е. время выборки Δt =1мс.

Приемник в системе скрытой передачи был реализован на базе одного МК Atmel ATmega328P (рис. 1). Приходящий из канала связи сигнал $x'(t) = x(t) + \zeta(t)$, где $\xi(t)$ – шум канала связи, оцифровывается встроенным в МК 10 битным АЦП. Периодический запуск АЦП осуществляется с помощью 16 битного таймера с частотой 1кГц, а вычисления проводятся в обработчике прерывания таймера. В качестве опорного напряжения АЦП использует $V_{ион}$ от встроенного ИОН, время выборки АЦП приемника задается равным времени прерывания таймера передатчика - Δt. Оцифрованные значения сдвигались на 6 бит, чтобы динамическую переменную x'_i вписать в 16 бит. Затем x'_i помещаются в ЛЗ.

После каждой очередной выборки в соответствии с разработанным алгоритмом арифметико-логическое устройство (АЛУ) последовательно извлекает из ЛЗ значения x'_{i-k_1} и x'_{i-k_3}. После извлечения из ЛЗ каждое из этих значений проходит НЭ и цифровой фильтр (ЦФ) и вычитается из x'_i. Далее результат вычислений помещается в кольцевые буферы: БУФЕР 0 для задержки k_1 и БУФЕР 1 для задержки k_3. НЭ и ЦФ приемника выполнялся идентичным НЭ и ЦФ передатчика. В случае идентичности параметров приемника и передатчика, при отсутствии в системе передаче неучтенных шумов и искажений сигнала, при установке $m(t) = 0$ (времени запаздывания генератора передатчика равном k_1) значения, помещаемые в БУФЕР 0 после короткого переходного процесса будут строго равны 0. Значения же помещаемые при этом в БУФЕР 1 будут отличны от 0, так как приемник, имеющий время запаздывания k_3, не будет синхронизоваться сигналом передатчика, время запаздывания которого задано равным k_1).

При $m(t) = 1$, соответственно наоборот, будет синхронизоваться контур приемника с временем запаздывания k_3, поэтому в БУФЕР 1, будут помещаться нулевые значения, а в БУФЕР 0 – ненулевые.

В таких условиях, один из контуров оказывается избыточным. Однако для любой реальной системы передачи наличие измерительных шумов в канале связи будет приводить к тому, что даже при идентичности времен запаздывания генератора передатчика и контура в приемнике значение на выходе этого контура будет отличным от нуля. Полагая шумы канала связи статистически независимыми от хаотического сигнала несущей в канале связи, можно оценить дисперсию такого ненулевого сигнала на выходе контура приемника величиной порядка дисперсии этих шумов.

Поэтому, для борьбы с шумами, оказалось необходимо, ввести избыточность, дополнительные элементы в приемник и специальную процедуру обработки.

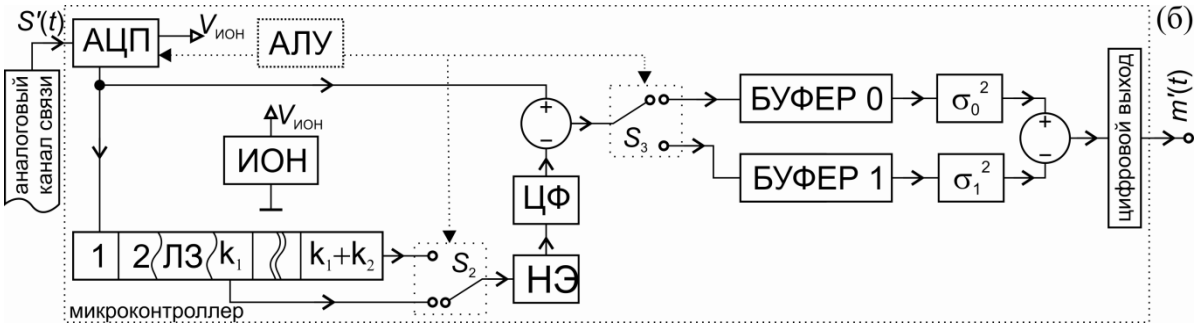

Рис. 1 Схема приемника системы скрытой передачи данных.

Дисперсия сигнала на выходе несинхронизованного контура приемника оказывается близкой к дисперсии хаотической несущей, а для синхронизованного контура, в силу приведенных выше соображений, близкой к дисперсии шума канала связи. Предполагая, что последняя имеет интенсивность меньшую, чем дисперсия несущей, была предложена следующая процедура выделения информационного сигнала в приемнике.

В кольцевых буферах накапливаются данные и после помещения в буфер каждого нового *i*-го значения по накопленным в буферах последовательностям отсчетов рассчитываются значения эмпирической оценки дисперсии (далее, просто “дисперсии”) сигналов σ_{0i}^2 для данных из буфера БУФЕР 0 и σ_{1i}^2 - для БУФЕР 1. Далее вычисляется $\Delta\sigma_i = \sigma_{0i}^2 - \sigma_{1i}^2$. Если $\Delta\sigma > 0$, то считается, что передается логическая 1, т.е. значение выделенного информационного сигнала $m'(t) = 1$ и высокий логический уровень выставляется на выводе цифровой линии МК. Если $\Delta\sigma < 0$, то $m'(t) = 0$ и на выводе цифровой линии выставляется низкий уровень.

Длина информационных битов фиксирована и равна 100 дискретным отсчетам АЦП, т.е. составляет 100 мс. Длина каждого из буферов БУФЕР 0 и БУФЕР 1 установлена равной длине информационного бита. Такая организация кольцевых буферов и алгоритма работы с ними эквивалентна расчету σ_{0i}^2 и σ_{1i}^2 в скользящих окнах шириной 100 отсчетов со сдвигом на один дискретный отсчет.

Для имитации зашумленности канала связи использовался аналоговый генератор шума Agilent Technologies 81150A. Также была разработана и создана схема смешивания несущего и шумового сигналов.

В ходе радиофизического эксперимента был выявлен порог чувствительности к шумам в канале связи, при котором система перестает функционировать. Для этого была посчитана стандартная мера битовых ошибок BER (bit erorr rate). В качестве аддитивного шума использовался гауссовский шум (Gauss(CF 3.1)), смещением 550мВ, входным импедансом 1МОм, выходным импедансом 50Ом двумя способами: без фильтрации (т.е. шум, ограниченный в спектре частотой Найквиста) и в полосе, равной времени инерционности цифрового фильтра хаотического генератора. Показано, что система скрытой передачи информации без ошибок работает при 30% уровне нефильтрованного шума (10 dB) и 20% уровне фильтрованного шума (15 dB) (рис. 2). Это на порядок лучше, чем для системы скрытой передачи из работы [12].

Для подсчета отношения сигнал/шум, SNR (signal to noise ratio), сигнал канала и сигнал шума оцифровывался. Далее с помощью программы считалось среднеквадратичное отклонение сигнала канала и шума в вольтах. SNR=20*lg($\sigma^2_{\text{канал}}/\sigma^2_{\text{шум}}$). Фильтрованный шумовой сигнал был малоаплитудным, поэтому использовался шум с максимальной амплитудой. Его амплитуда увеличивалась с помощью операционного усилителя. Коэффициент усиления соответственно умножали на $\sigma^2_{\text{шум}}$ для расчетов SNR.

Также проведено исследование стабильности работы при изменении амплитуды сигнала в канале. Для систем связи характерно затухание в канале связи. Для хаотических систем это критично. В ходе эксперимента сигнал в канале связи масштабировался с помощью операционного усилителя. Установлено, что при расстройки амплитуды в канале связи на 10%, т.е. при коэффициенте усиления 0,9, BER равен 0 (рис. 2). Для всех расчетов использовались последовательности длиной около 100000 бит.

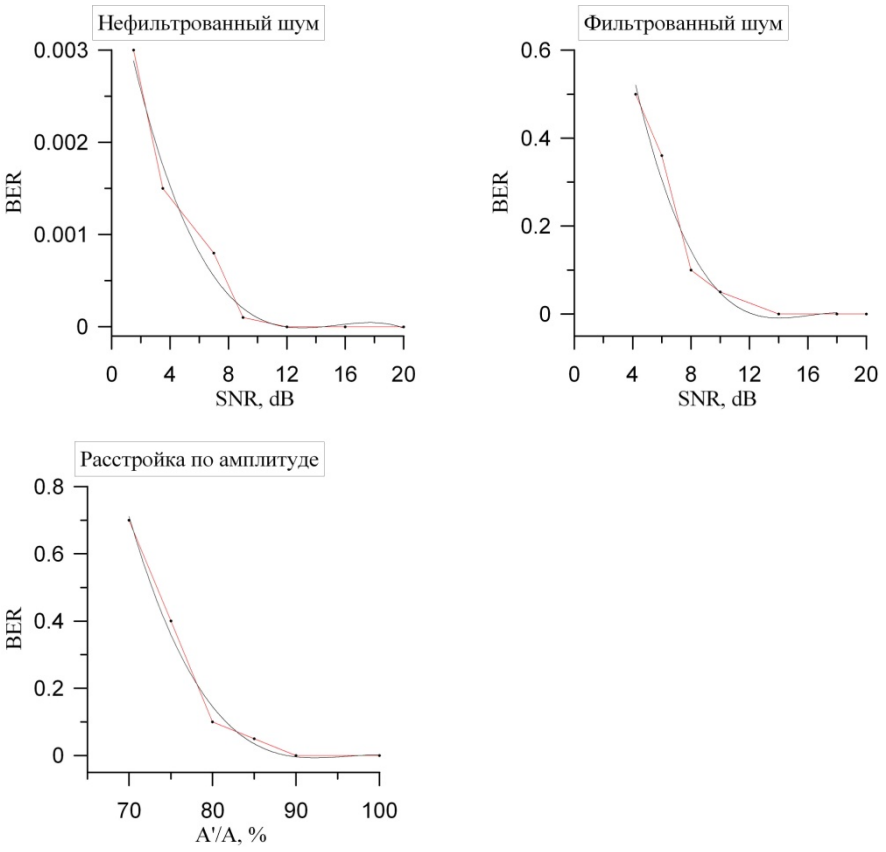

Рис. 2 Зависимости BER от уровня шума.

Bulletin of Medical Internet Conferences (ISSN 2224-6150)
2014. Volume 4. Issue 7

Случайная битовая последовательность генерировалась следующим образом: с одного из каналов генератора подавался гауссовский шум (Gauss(CF 3.1)) амплитудой 2,2В, смещением 1,1В, входным импедансом 1МОм, выходным импедансом 50 Ом на вход, встроенного в МК компаратора. Шум сравнивался относительно опорного напряжения МК в 1,1В. Если шум был больше по амплитуде, тогда на цифровую ногу контроллера, имитирующую информационный вход, выставлялась логическая единица. И наоборот, если шум был меньше по амплитуде опоры, то логический уровень опускался.

Заключение

Разработан и создан лабораторный макет радиофизической системы скрытой передачи информации с модуляцией времени запаздывания хаотического генератора информационным сигналом. Предложенная система скрытой передачи подразумевает потоковое кодирование информации с малой задержкой и может использоваться для скрытия канала передачи информации от медицинского оборудования. Система отличается технической простотой и может быть реализована на базе простых низкопотребляющих 8 битных микроконтроллерах Atmel, что позволяет встраивать ее даже в носимые медицинские устройства.

Экспериментально показано, что система позволяет без ошибок (BER не ниже 10^{-5}) передавать данные при наличии в канале шумов и искажений на уровне 10 дБ, при этом информационный сигнал передается на скорости около 1Кбод.

Работа выполнена при поддержке Российского научного фонда, грант № 14-12-00324.

Литература

1. Назаренко Г.И., Гулиев Я.И., Ермаков Д.Е. Медицинские информационные системы: теория и практика. Физматлит, 2005; 320 с.
2. Гулиев А.В., Романов Ф.А., Дуданов И.П., Воронин А.В. Медицинские информационные системы. Петрозаводск: ПетрГУ, 2005; 404 с.
3. Посненкова О.М., Гриднев В.И., Киселев А.Р., Шварц В.А. Клинический аудит качества медицинской помощи больным артериальной гипертонией в поликлинике города Саратова с использованием компьютерной информационно-аналитической системы. *Саратовский научно-медицинский журнал* 2009; 5(4): 548-554.
4. Киселев А.Р., Гриднев В.И., Посненкова О.М., Попова Ю.В. Значение регистров заболеваний в системе управления здравоохранением. *Проблемы стандартизации в здравоохранении* 2013; (1-2): 15-18.
5. Бирюков А.П., Васильев Е.В., Думанский С. М., Тихонова О.А., Герт Ю.А., Капитонова Н.В. Выбор компьютерных технологий для аналитической поддержки базы данных крупномасштабных медицинских информационных систем. *Саратовский научно-медицинский журнал* 2013; 9(4): 983–987.
6. Домарев В.В. Защита информации в медицинских информационных системах: врачебная тайна и современные информационные технологии. *Клиническая информатика и телемедицина* 2004; 1(2): 147–154.
7. Гулиев Я.И., Фохт И.А., Фохт О.А., Белякин А.Ю. Медицинские информационные системы и информационная безопасность. Проблемы и решения. В кн.: Программные системы: Теория и приложения: тр. Междунар. конф. Переславль-Залесский, 2009: 175–206.
8. Карабаев М.К., Абдуманонов А.А. Алгоритмы и технологии обеспечения безопасности информации в медицинской информационной системе externet. *Программные продукты и системы* 2013; (1): 150-155.
9. Юргель Н.В. Никонов Е.Л. Гармаш И.В. Мерзлов Л.Ю., Поздняков И.Г. Защита информации в регистре медицинских и фармацевтических работников. *Вестник Росздравнадзора* 2008; (1): 75-76.
10. http://www.cnews.ru/reviews/free/national2006/articles/datasecure/.
11. Ponomarenko V.I., Prokhorov M.D., Karavaev A.S., Kulminskiy D.D. An experimental digital communication scheme based on chaotic time-delay system. *Nonlinear Dynamics* 2013; 74(4): 1013–1020.
12. Stankovski T., McClintock P.V.E., Stefanovska A. Coupling functions enable secure communications. *Physical Review X* 2014; 4: 011026.

