Реализация Bluetooth-технологии и обеспечение безопасности взаимодействия Bluetooth-устройств.

Bluetooth — современная технология беспроводной передачи данных и голоса, позволяющая соединять друг с другом при минимальном пользовательском участии любые устройства, имеющие встроенный микрочип Bluetooth (мобильные телефоны, ноутбуки, принтеры, цифровые фотоаппараты, холодильники, микроволновые печи, кондиционеры и т.д.).
Технология, первоначально задуманная как средство соединения компьютера и сотового телефона или других телекоммуникационных устройств между собой, названа в честь датского короля викингов Harald Blutend (по-английски Bluetooth, а по-русски Голубой Зуб), получившего свое прозвище из-за потемневшего переднего зуба. Король Harald Blutend вошел в историю как человек, объединивший Данию и Норвегию в единое государство на основе религии, которую принесли в Скандинавию христианские миссионеры. Через 1000 лет технология беспроводной связи разнородных устройств получила название — Bluetooth (технология стандартизирована, т.е. проблемы несовместимости устройств от конкурирующих фирм быть не должно).

История. В начале 1998 года пять крупных компаний: Ericsson (шведская компания, ставшая инициатором проекта Bluetooth), Nokia , IBM, Toshiba и Intel — объединились, чтобы начать работу над созданием дешевого и неэнергоемкого радиоинтерфейса для обеспечения беспроводной связи Bluetooth. Для дальнейшего продвижения новой технологии на телекоммуникационном рынке 20 мая 1998 была сформирована специальная рабочая группа Special Interest Group (SIG) — союз компаний разных направлений: два лидера телекоммуникационного рынка, два ведущих производителя портативных компьютеров, а также лидер в производстве процессоров для ПК. Очень быстро к Группе присоединились такие компании, как Motorola, Dell, Compaq, Xircom и многие другие. Сегодня в SIG уже состоит около 2000 компаний.

Особенности Bluetooth.

1.Работает в диапазоне частот Industrial Scientific Medical (ISM) 2,4–2,4835 ГГц.
Bluetooth — это маленький чип, представляющий собой высокочастотный (2,4–2,4835 ГГц в США, Японии и Европе (во Франции и Испании доступна лишь часть этой полосы)) приемопередатчик (радио-трансивер), работающий в диапазоне ISM (Industry, Science and Medicine — промышленный, научный и медицинский). Радиосигнал Bluetooth надежно распространяется на расстояние около 10 м, но увеличив мощность передатчика, можно довести дальность связи до 100 м. Энергопотребление (мощность передатчика) не должно превышать 10 мВт, составляя лишь малую долю от потребления мощности основным устройством, в котором будет представлен Bluetooth.

2.Используется система FH/TDD(frequency-hop/time-division-duplex) — технология модуляции с разбросом по частоте, которая делит радиоканал на интервалы продолжительностью 625 мкс, называемые слотами, где каждому слоту соответствует своя частота.

А) *Скачкообразная перестройка частоты в расширенном спектре* (*FHSS — Frequency Hoping Spread Spectrum*)

Частотный диапазон 2,4–2,4835 ГГц свободен от лицензирования, что вносит сложности в использование Bluetooth-устройств, т.к. в этом диапазоне также работают различные медицинские приборы, бытовая техника, беспроводные телефоны, беспроводные локальные

сети стандарта IEEE. Во избежание интерференции с другими беспроводными устройствами Bluetooth работает по принципу скачкообразной перестройки частоты — FHSS (1600 переключений в секунду при передаче однослотовых пакетов). Переход с одной частоты на другую происходит по псевдослучайному алгоритму, что позволяет "освободить" нужные другим устройствам частоты. Технология случайных переходов рабочей частоты — FHSS повышает защищенность системы как от помех, так и от несанкционированного перехвата информации.

В) *TDD — дуплексная схема с временным уплотнением*

Принцип системы TDD заключается в следующем: один пакет данных занимает один слот либо передачи, либо приема; слоты используются попеременно.

3.Поддерживает микросети, состоящие из восьми или менее устройств, использующих один и тот же канал связи.

Bluetooth допускает соединения электронных устройств и беспроводное сообщение через короткий диапазон, специальные сети, называемые piconet (пикосеть) или PAN (Personal Access Network – Сеть Персонального Доступа). Каждое устройство может соединяться максимально с семью устройствами в piconet. При взаимодействии нескольких Bluetooth-устройств для контроля трафика канала одно из устройств становится главным (master) и управляет частотной (задает последовательность перескоков частот по закону, определяемому его адресом (BD_ADDR)) и пакетной синхронизацией, а остальные устройства (до 7) становятся подчиненными (slave); если устройств станет больше — автоматически образуется еще одна сеть. Каждая пикосеть может иметь только одно ведущее устройство, однако ведомые могут участвовать в различных пикосетях на основе мультиплексирования с временным разделением (time-division multiplex), образуя группы пикосетей с перекрывающимися зонами охвата — скэттерсети (scatternet) (эти пикосети не должны быть синхронизированы ни по времени, ни по частоте).
Когда внутри пикосети не происходит передачи данных устройства Bluetooth переходят в одно из энергосберегающих состояний:
· состояние *Hold* (пауза) требуется при объединении нескольких пикосетей или управлении маломощными приборами (ведомое устройство может отослать запрос о своем переводе в состояние Hold или перейти в него по требованию ведущего устройства);
· в состоянии *Sniff* (внимание) ведомое устройство прослушивает пикосеть с замедленным темпом, что снижает потребление энергии;
· в состоянии *Park* (парковка) устройство остается синхронизированным с сетью, но не участвует в передаче данны.
Пикосети могут взаимодействовать друг с другом с минимальным риском взаимных помех, благодаря возможности микросхемы Bluetooth быстро переходить с частоты на частоту (Frequency Hopping). Единственное условие — разные пикосети одной распределенной сети должны иметь различный порядок смены каналов (hopping sequence): настоящий вариант спецификации стандарта предусматривает 10 вариантов смены каналов – 5 с циклом 79 смен частот (в тех странах, где доступна полоса частот шириной 80 МГц или более) и 5 – с циклом в 23 смены (Япония, Франция и Испания, где полоса частот уже).

Установление соединений. По умолчанию устройство находится в режиме Standby (устройство не входит в состав пикосети). Для вывода из состояния ожидания из общего числа несущих 79 (23), было выделено по псевдослучайному закону подмножество из 32 (16) вызывающих частот, которое определяется идентификатором (сначала используются половина таких частот, а если ответа нет — оставшиеся). В пределах последовательности

несущих, длина которой составляет 32 (16) скачков, каждая из вызывающих несущих повторяется один раз.
В процессе установления соединения предусмотрены процедуры: режимы Inquiry (запрос), Inquiry Scan (просмотр/сканирование запроса), Page (пейджинг) и Page Scan (просмотр/сканирование пейджинга).
Для установления соединения устройство-инициатор периодически входит в состояние page, в котором он передает код доступа DAC (Device Access Code), длиной 72 бита (72 мкс) в течение 10 мс на различных несущих частотах до тех пор, пока принимающее устройство не ответит, либо пока не истечет время ожидания ответа.
Устройство Bluetooth реагирует на запрос в соответствии с режимом, в котором оно находится:
· *discoverable mode* (режим отклика) — устройство отвечает на все полученные запросы всегда;
· *limited discoverable mode* (режим ограниченного отклика) — устройство может отвечать на запросы только ограниченное время или при других определенных условиях;
· *non-discoverable mode* (режим отказа в отклике) — устройство не отвечает на запросы.
Кроме того, при подключении устройство может быть: подключаемым (*connectable mode*) или недоступным (*non-connectable mode*) (устройство не позволяет настроить ряд параметров соединения и обмениваться данными).
Находящееся в состоянии ожидания Bluetooth-устройство периодически, каждые 2048 (1028) слотов (1,28 секунды) входит в состояние сканирования (page scan): прослушивает эфир на последовательности перескоков частот. При сканировании — в интервале прослушивания, который длится 18 слотов или 11,25 мс, — устройство принимает сигналы на одной несущей частоте и сопоставляет их с кодом доступа на основе его собственного адреса. При срабатывании блока сравнения — т.е. когда большинство принятых битов соответствует коду доступа — устройство активизируется и запускает процедуру установления соединения; в противном случае устройство возвращается в режим ожидания до следующего вызова.
Таким образом за время, когда сканирующее устройство слушает одну частоту, опрашивающее устройство успевает послать пакеты на нескольких частотах, и за некоторое число состояний сканирования опрашивающее устройство сумеет “зацепить” искомое.
После ответа искомого устройства, инициатор посылает специальный пакет FHS (frequency hop synchronization), в котором сообщает свой адрес и класс устройства, показания своих часов, назначает ведомому устройству его временный номер и передает некоторые дополнительные параметры — соединение устанавливается, и далее уже идет обмен пакетами данных.
Устройства, подключающиеся к устройству, находящемуся в режиме ожидания, должны знать его идентификатор (BD_ADDR) и, желательно, состояние его таймера (если у инициатора еще имеется и представление о часах искомого устройства, то соединение будет установлено быстрее, поскольку частота будет искаться не вслепую, а с учетом ожидаемой фазы искомого устройства).

Между ведущим и ведомым устройствами устанавливаются два типа связей:

– SCO (Synchronous Connection Oriented Link) — синхронная связь, ориентированная на установление соединений (связь точка-точка между ведущим и единственным ведомым устройством в пикосети, используемая, как правило, для передачи речи);

– ACL (Asynchronous Connection-less Link) — асинхронная связь без установления соединения (связь точка-мультиточка между ведущим и ведомыми устройствами в пикосети, обычно используется для передачи данных).

Пакеты. Данные между двумя устройствами Bluetooth передаются через слоты, каждый из которых несет один пакет данных. Каждый пакет в общем случае состоит из полей кода доступа (72 бит), который вырабатывается на основе идентификатора ведущего устройства и уникален для канала; заголовка (54 бит) и контейнера для данных (payload) длиной 0–2745 бит. Последние два поля могут и отсутствовать.
Поле *кода доступа* используется для синхронизации и идентификации; коды могут быть трех типов:
· код доступа к каналу (CAC, Channel Access Code), передаваемый в каждом канальном пакете, идентифицирует пикосеть;
· код доступа к устройству (DAC, Device Access Code) используется для специальной сигнальной процедуры (paging);
· код опроса (IAC, Inquiry Access Code) служит для обнаружения устройств, находящихся в зоне охвата.
Заголовок пакета содержит важную управляющую информацию: трехразрядный адрес управления доступом (MAC-адрес), 4-битный код типа пакета, биты управления потоком данных, биты управления потоком данных, индикаторы подтверждения (ARQN) и последовательного номера пакета (SEQN), а также 8-битное поле коррекции ошибок в заголовке (HEC). Заголовок, длина которого фиксирована и составляет 54 разряда, защищен помехоустойчивым кодом (FEC) со скоростью кода 1/3.
Контейнер несет данные различных типов и с различной степенью защиты от ошибок, в зависимости от кода типа пакета и типа физической связи (SCO или ACL). Несколько типов пакетов используются для служебных целей (не все содержат контейнеры). Среди них есть и пакет FHS (frequency hop synchronization), в контейнере которого содержится информация, необходимая для синхронизации перескоков частоты. Этот пакет используется перед установлением каналов пикосети.

Для каждого из типов связи (SCO, ACL) существует свой набор пакетов:

Для канала SCO определено три вида однослотовых речевых пакетов, каждый из которых обеспечивает передачу данных со скоростью до 64 Кбит/с в обоих направлениях. Передача голоса осуществляется без помехоустойчивого кодирования, однако если интервал сигналов в SCO-соединении сокращается, может быть выбрана степень помехозащиты 1/3 или 2/3. При использовании Forward Error Correction code 1/3 (FEC — избыточное кодирование) каждый полезный бит передается трижды, что позволяет выбрать наиболее похожий вариант мажорированием. Эта схема используется для кодирования и заголовков пакетов, и полей данных. Схема FEC 2/3 несколько сложнее, здесь используется код Хэмминга (15, 10) — из каждых полезных 10 битов генерируется 15-битный символ, что позволяет исправлять все однократные и обнаруживать все двукратные ошибки в каждом 10-битном блоке. Если длина защищаемого битового поля не кратна 10, то к нему добавляются дополнительные биты-заполнители.

Пакеты ACL-соединений могут занимать 1, 3 и 5 слотов. Данные могут передаваться как без помехоустойчивого кодирования, так и с кодированием со скоростью кода 2/3. При отсутствии помехоустойчивого кодирования 5-слотовыми пакетами, асинхронный канал может обеспечивать максимальную скорость 723,2 Кбит/с(90 Кбайт/с) в асимметричной конфигурации (оставляя для обратного канала полосу 57,6 Кбит/с) или же 433,9 Кбит/с в каждую сторону в симметричной конфигурации.

4.В системах Bluetooth определены пять типов логических каналов:

– канал (Link Control) служит для низкоуровневого контроля (управление потоком, подтверждения приема, определение характеристик контейнеров для данных);

– канал передачи информации между диспетчерами связи ведущего и ведомых услуг LM (Link Manager);
– асинхронный и изохронный каналы пользовательских данных UA/UI (User Asynchronous/ Isochronous Data);
– канал синхронных данных пользователя US (User Synchronous Data), реализуемый на связи SCO.

5.Стены или стенки портфеля не мешают связи; прямая видимость не требуется.

Как радиотехнология, Bluetooth способна "обходить" препятствия (если они не металлические), поэтому соединяемые устройства могут находиться вне зоны прямой видимости.

6.Помехоустойчивость.

– Скачкообразная перестройка частот FHSS осуществляется с большой скоростью, а длина пакета мала (1600 переключений в секунду при передаче однослотовых пакетов). При потере пакета пропадает лишь малая часть информации.
– Пакеты могут быть защищены с помощью помехоустойчивого кодирования.
– Пакеты защищены системой ARQ (автоматический запрос на повтор), которая позволяет автоматически повторять передачу потерянных пакетов. Принимающая сторона проверяет каждый поступающий пакет на предмет наличия ошибок. Если они обнаружены, это отражается в заголовке возвращаемого пакета. Задержка равна длительности всего одного слота, а повторная передача осуществляется только для утерянного пакета.
– Передача голосовых данных никогда не повторяется. Для речи применяется специальная схема кодирования, основанная на дельта-модуляции с переменной крутизной (CSVD - Continuous Variable Slope Delta Modulation): схема повторяет форму звуковой волны и очень устойчива к ошибкам отдельных битов (ошибки принимаются за шумовой фон, который усиливается пропорционально количеству ошибок).

7.Безопасность.

В зависимости от выполняемых задач, устройство может находиться в одном из трех режимов защиты:

A) минимальный — данные кодируются общим ключом и могут приниматься любыми устройствами без ограничений;

B) защита на уровне устройств — непосредственно в чипе прописывается уровень доступа, в соответствии с которым устройство может получать определенные данные от других устройств;

C) на уровне сеанса связи (link layer) средствами безопасности используется:

– общедоступный 48 – битный уникальный адрес устройства Bluetooth (BD_ADDR – Bluetooth device address);

Каждое устройство имеет формируемый по стандарту IEEE802 уникальный адрес (BD_ADDR). Из 24-битного идентификатора компании (по IEEE) в адресе значащими являются только 8 бит. К ним добавляется (в виде младшей части) 24-битный идентификатор устройства, присваиваемый каждому устройству компанией-производителем. Для того чтобы устройство Bluetooth смогло установить соединение с другим устройством, оно должно предварительно узнать его адрес. Адрес Bluetooth может быть получен в процессе процедуры опроса inquiry. Устройство-исследователь окружения посылает короткие пакеты с кодом опроса IAC (Inquiry Access Code) на одной из специальных (тоже коротких) последовательностях перескоков. Опрос может быть глобальным, с кодом GIAC (Global IAC) - на

него должны отзываться устройства всех классов, или же выборочным, с кодами DIAC (Dedicated IAC). За время прослушивания одной частоты инициатор успевает передать пакеты на 32 (16) частотах, так что рано или поздно он попадет в частоту опроса каждого из устройств, находящихся в зоне охвата. Устройство отвечает на опрос с подходящим (или глобальным) кодом доступа коротким пакетом, в котором сообщает свой адрес и показания часов. При этом возможно, что один и тот же пакет опроса одновременно примут несколько устройств. Для борьбы с этими коллизиями применяется механизм задержки ответов на случайный интервал времени, так что вероятность одновременного ответа двух устройств (это будет воспринято как помеха) снижается.

– различное для каждой транзакции 128 – битное случайное число RAND (синхропосылка), определяемое псевдослучайным образом каждым устройством Bluetooth;

– 128 – битный ключ аутентификации пользователя;

Соединения могут требовать односторонней, двусторонней , либо совсем не требовать аутентификации:
В основе односторонней аутентификации абонентого устройства лежит классическая схема аутентификации Challenge/Response (вызов/ответ) — составляющая общего алгоритма аутентификации абонентов.
Сторона A передает проверяющей стороне B свою временную метку и идентификатор, зашифрованные общим ключом:

$$A \longrightarrow B : E_k(t_A, id(B))$$

Расшифровав сообщение, сторона B проверяет: соответствие временной метки допустимому интервалу; совпадение полученного и собственного идентификаторов.
Временные метки могут быть заменены случайными числами с помощью дополнительной пересылки:

$$A \longleftarrow B : z_B$$
$$A \longrightarrow B : E_k(z_B, id(B))$$

Расшифровав сообщение, сторона B проверяет: соответствие полученного числа случайному числу, переданному им на шаге (1); совпадение полученного и собственного идентификаторов.
Проведением односторонней аутентификации в одном, а затем и в обратном направлении (прямым направлением выбирается направление от стороны, инициализирующей сеанс связи) достигается взаимная аутентификация абонентов канала связи:

$$A \longleftarrow B : z_B$$
$$A \longrightarrow B : E_k(z_A, z_B, id(B))$$
$$A \longleftarrow B : E_k(z_A, z_B)$$

При сбое в процессе аутентификации, Bluetooth-устройства, прежде чем предпринять новую попытку, должны выждать некоторое время. Экспоненциальное увеличение времени задержки перед каждой следующей попыткой ограничивает возможность применения злоумышленником метода тотального опробования всех возможных ключей. Недостаток этого механизма — появление “атаки на отказ в обслуживании”.

> Злоумышленник может провести несколько попыток аутентифицировать себя, используя неверные ключи. Фиксирующее сбои в процессе аутентификации устройство будет увеличивать время ожидания (до определенного максимума) до активизации возможности следующей попытки, игнорируя этим и легитимных пользователей.

Способ избежать этого — вести список устройств (по их адресам), попытка аутентификации которых была безуспешной. Однако, на устройствах с ограниченными вычислительными ресурсами такой список ,если и будет существовать, то весьма малого размера, не достаточного для нормального функционирования.

– ключ шифрования K_c переменной длины (с шагом в 8 бит) от 8 до 128 бит;

Длина ключа шифрования выбрана изменяемой по двум соображениям:
во-первых, возможность выбора требуемой надежности шифрования (для большинства приложений пока вполне достаточно 64 бит);
во-вторых — удовлетворение государственным требованиям, ограничивающим разрешенную стойкость шифрования (допускаемый уровень секретности в разных странах различен).

Разделяемым секретом симметричной схемы шифрования является 128-битный "ключ связи" двух абонентов: абоненты канала, используя один и тот же ключ связи, могут формировать ключ шифрования нового сеанса связи и аутентификации сторон.
В соответствии со спецификацией Bluetooth определяются четыре вида ключей связи по типу применения в приложениях, организующих аутентификацию и шифрование данных:
· сочетательный ключ K_{ab} вычисляется для двух абонентов сети путем динамического взаимодействия на основе обмена открытыми сообщениями без какой либо общей секретной информации, распределяемой заранее (алгоритм соглашения о ключах Диффи-Хеллмана);
Для выполнения алгоритма открытого распределения ключей Диффи-Хеллмана стороны должны договориться о значениях большого простого числа p и порождающего элемента α мультипликативной группы $Z_p^* = \{1, 2, \ldots, p-1\}$.
Каждый пользователь выбирает случайным образом число $1 \leq x \leq p-2$ и держит его в секрете. Далее он вычисляет значение $\alpha^x mod p$.
Сторона A: Выберает случайное число x_a в интервале $1 \leq x_a \leq p-2$ и вычисляет значение $\alpha^{x_a} mod p$.

$$K_{private} = x_a, \quad K_{public} = (p, \alpha, \alpha^{x_a} mod p)$$

Сторона B: Выбирает случайное целое число x_b в интервале $1 \leq x_b \leq p-2$ и вычисляет значение $\alpha^{x_b} mod p$.

$$K_{private} = x_b, \quad K_{public} = (p, \alpha, \alpha^{x_b} mod p)$$

Затем стороны должны обменяться сообщениями:

$$A \longrightarrow B : \alpha^{x_a} mod p$$
$$B \longrightarrow A : \alpha^{x_b} mod p$$

Искомый общий ключ вычисляется по формуле: $K_{ab} = (\alpha^{x_b})^{x_a} = (\alpha^{x_a})^{x_b} mod p$.
· ключ Bluetooth-устройства K_a вычисляется на этапе инсталляции Bluetooth-устройства в вычислительную среду (однажды вычисленный, он затем хранится в энергонезависимой памяти и никогда не меняется);
· ключ широковещания K_{master} для организации широковещательной связи для доступа к информации только определенного круга абонентов;
· ключ инициализации K_i используется, либо на этапе установления сеанса связи, когда еще не определен ключ устройства или сочетательный ключ абонентов; либо в процессе регенерации ключа шифрования в результате сбоя в синхронизации системы. Он предназначен для защиты параметров аутентификации от несанкционированного доступа и вычисляется из случайной синхропосылки, PIN-кода и значения BD_ADDR данного

устройства. Значение PIN-кода (некоторый фиксированный набор цифр для удобства использования) поставляется, либо производителем вместе с устройством связи, либо пользователем устройства.

Обмен ключами производится на этапе инициализации сеанса связи, который состоит из следующих шагов:
· вычисление ключа инициализации K_i из PIN-кода и адресов абонентских устройств;
· аутентификация;
· вычисление ключей связи;
· обмен ключами связи и затем уничтожение ключа инициализации на обоих устройствах;
· вычисление ключа шифрования из ключей аутентификации и синхропосылки.
По завершении процесса инициализации устройства готовы к обмену данными. Для проведения следующего сеанса связи процесс повторяется, за исключением первого шага схемы.

В настоящий момент действует спецификация Bluetooth 1.1, но уже утверждена спецификация 1.2 (5 ноября 2003), в ней:
– улучшена защищенность передачи сигнала в диапазоне 2.4 ГГц от интерференции от устройств, использующих этот диапазон (технология Согласованного Перехода Частоты - Adaptive Frequency Hopping (AFH));
– увеличена помехозащищенность при передаче голоса;
– оптимизирована процедура установления связи с другим устройством Bluetooth.
Спецификация 1.2 полностью включает предыдущую - 1.1, т.е. обратно совместима с ней.

У Bluetooth имеются конкуренты: IrDA OBEX (Infrared Data Association) и HomeRF.

Современные портативные устройства используют для взаимодействия друг с другом инфракрасный (также беспроводной) канал связи (IrDA).
Преимущества IrDA — скорость передачи данных (4 Мбит/с) — выше, чем у Bluetooth (1 Мбит/с); инфракрасные приемопередатчики стоят меньше.
Недостатки IrDA : малая дальность передачи данных (обычно от одного до двух метров); порты устройств должны находиться в зоне прямой видимости друг друга; инфракрасные приемопередатчики могут использоваться только для соединения двух устройств.
Преимущества Bluetooth: помимо того, что организация радиоинтерфейса не требует каких-либо усилий со стороны пользователя, радиоволны имеют: гораздо больший радиус действия (до 100 м); могут распространяться сквозь различные объекты и материалы; использоваться для соединения многих устройств одновременно.

Спецификация HomeRF предназначена для связи бытовых аудио- и видеоустройств и построения домашних радиосетей.
Технология имеет много общего с Bluetooth, в частности: цена модулей; потребляемая устройствами мощность; передача данных осуществляется на тех же частотах 2.4 ГГц, что и Bluetooth.
Различия заключаются в максимальном числе узлов в сети (Bluetooth – 8, HomeRF – 127); скорости изменения частоты (Bluetooth – 50 c^{-1}, HomeRF – 1600 c^{-1}) и радиусе действия (Bluetooth – до 100 метров, HomeRF – до 50 метров).

Таким образом Bluetooth должна обеспечить сервис и средства для серьезной конкуренции.

Список литературы

[1] www.ixbt.com/mobile/review/bluetooth-1.shtml

[2] www.bluetoothclub.ru/info02.shtml

[3] www.prizmapr.ru/megatel/forum/post.php?cat=1fid=3pid=2page=1

[4] diccionario.h1.ru/cgi-bin/getxt.cgi?id=1233491940015703873301=es

[5] www.cinfo.ru/CI/CI_basic.htm

[6] www.osp.ru/os/2001/02/049.htm

[7] www.ichip.ru/index.php?page=archive_viewhtmlid=1174

[8] Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. *Основы криптографии: Учебное пособие, 2-е изд., испр. и доп.* — М.:Гелиос АРВ, 2002.