Список литературы

1. Гаврилов О.А Курс правовой информатики: Учебник для вузов. – М.: Издательство НОРМА (Изд. группа НОРМА-ИНФРА-М), 2002. – 432с.
2. Положение о технической защите информации на Украине: Утв. Указом Президента Украины от 27.09.1999 г. №1229.
3. Закон Украины "О защите информации в информационно-телекоммуникационных системах" от 05 июля 1994 г. // Ведомости Верховной Рады. – 1994, № 31. – Ст. 286.
4. Доронин А.И. Бизнес-разведка. – 2-ое изд., перераб. и доп. – М.: Изд-во «Ось-89», 2003. – 384с.
5. Мисюк С. Компьютерная разведка: взгляд на сайт компании из недр Интернета [Электронный ресурс cdaily.sec.ru]. – Доступ к ресурсу: http://www.daily.sec.ru/dailypblshow.cfm?rid=17&pid=8872.
6. Скрыль С.В., Киселев В.В. Аналитическая разведка в оценке угроз информационной безопасности // Системы безопасности, 2003. – № 6(48). – С. 96-97.
7. Киселев В.В., Золотарева Е.А.Признаки распознавания вредоносных программ в компьютерных сетях [Электронный ресурс]. – Доступ к ресурсу: http://agps-2006.narod.ru/konf/2003/sb-2003/sec-1/20.pdf.
8. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки. М.: Российск. гос. гуманит. ун-т,2002. – 399 с.
9. Халяпин Д.Б. Защита информации. Вас подслушивают? Защищайтесь! - М.: НОУ ШО "Баярд",2004. – 432 с.
10. ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
11. Ржавский В.К. Информационная безопасность: практическая защита информационных технологий и телекоммуникационных систем: Учебное пособие. – Волгоград: Изд-во ВолГУ, 2002. – 122с. (Серия «Информационная безопасность»).
12. Хорев.А.А. Защита информации от утечки по техническим каналам. Часть 1.Технические каналы утечки информации: Учебное пособие. – М.: Гостехкомиссия России,1998. – 320 с.
13. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. – Юниор. – 2003. – 504 с.
14. Криминальный кодекс Украины от 5 апреля 2001 г. // Официальный вестник Украины. – 2001. – №21. – ст.920.
15. Закон Украины "О телекоммуникациях" от 18 ноября 2003 г. // Ведомости Верховной Рады. – 2004. – № 12. – Ст. 155.
16. Конвенция о киберпреступности (официальный перевод) //Официальный вестник Украины. – 2007. – № 65. – С. 107. – Ст. 2535.
17. НД ТЗИ 1.1-003-99. Терминология в сфере защиты информации в компьютерных системах от несанкционированного доступа. Утв. приказом ДСТСЗИ от 28 апреля 1999 г. – [Электронный ресурс Государственной службы специальной связи и защиты информации Украины]. – Доступ к ресурсу://www.dstszi.gov.ua/dstszi/control/uk/publish.
18. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ-Петербург, 2000. – 384 с.
19. Ярочкин. В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Академический Проект, Гаудеамус, 2-е изд., 2004. – 544 с. (Gaudeamus).

Поступила 8.12.09

УДК 681.3 **Гарасим Ю.Р., Дудикевич В.Б.**

ТЕХНОЛОГІЇ БЕЗПЕКИ МЕРЕЖ WLAN. МОЖЛИВІСТЬ ОПТИМІЗАЦІЇ БЕЗПЕКИ БЕЗПРОВІДНОЇ МЕРЕЖІ ЗА ДОПОМОГОЮ FPGA ТА ASIC

Вступ

Сучасний ринок вимагає мобільності та постійності зв'язку для ефективної конкуренції. Стільникові телефони та персональні цифрові секретарі (PDA - Personal Digital Assistant) стали обов'язковими при збільшенні продуктивності та покращенні конкурентоспроможності. Ноутбуки, нетбуки забезпечують користувачам мобільність роботи будь-де та будь-коли. Із їхньою появою постало питання щодо безпровідної передачі даних та з'єднання терміналів замість базових провідних мереж. Однією з найбільш відомих безпровідних технологій стала Wi-Fi (Wireless Fidelity) безпровідна LAN (WLAN). Ця

технологія базується на методі передачі інформації за допомогою радіохвиль для з'єднання терміналів в мережу із гарантованою пропускною здатністю – 11 – 54 Мб/с, що працює в діапазоні частот 2,4 – 5 ГГц.

Мережеві компоненти стають більш вразливими для зловмисних дій та ненавмисних помилок у політиці безпеки підприємства тому, що роль корпоративної мережі продовжує зростати, забезпечуючи з'єднання обох – внутрішнього та зовнішнього зв'язку у формі додатків Internet, intranet та extranet. Мережева безпека стала критичнішим елементом планування та виконання корпоративної мережі.

Визначивши функціональність і пояснивши потребу, а також переваги комплексної безпеки в комунікаціях і, особливо, щодо безпровідних технологій, ця стаття детально зупиняється на рішеннях, які виконані в апаратному чи програмному забезпеченні та розглядає дві фундаментальні апаратні категорії: з можливістю переконфігурації чи без неї. Вивченими є різні технології існуючих платформ за допомогою швидких виконань інтегрованих рішень безпеки: цифрові процесори сигналів (DSP – digital signal processor) та системи на мікросхемах (SOC – system-on-a-chip) із/без вбудованого функціонального DSP.

Технології безпеки мережі WLAN

З перших днів існування WLAN були запропоновані стандартизовані рішення та велика кількість базових технологій мережевої безпеки. Згодом вони були або покращені, або замінені більш сучасними стандартами.

Деякі з ключових технологій мережевої безпеки, що використовуються у виконаннях WLAN є: ізоляція демілітаризованої зони (DMZ - DeMilitarized Zone), ізоляція радіочастотного діапазону (RF – radio frequency).

Особливості безпеки стандарту 802.11. IEEE 802.11 – метод автентифікації за замовчуванням, що був визначений для 802.11 та є автентифікацією відкритої системи та двокроковим процесом. Станція, що намагається встановити автентифікацію з іншою станцією – відправляє керуючий кадр автентифікації, в якому міститься ідентифікатор станції, що надсилає запит. Станція, що отримала цей кадр у відповідь відправляє кадр, в якому вказує чи автентифікувала вона цю станцію чи ні.

З появою стандартів 802.11 та їх розширень все більше і більше вдосконалених методів безпеки були закладені в ці стандарти. Три найбільш відомі методи захищеного доступу до точок безпровідного доступу були закладені в мережі стандарту 802.11. Ці базові методи широко доступні та можуть бути достатніми для деяких застосувань: SSID, фільтрування адреси MAC (Media Access Control – контроль медіа-доступу), WEP (Wireless Encryption Protocol – протокол шифрування безпровідного зв'язку).

Можливим є використання одного з них, але більша захищеність досягається при їх комплексному використанні. [1]

Безпровідна безпека VPN (Virtual Private Network). VPN рішення широко застосовуються для того, щоб забезпечити захищений доступ віддалених працівників до корпоративної мережі через мережу Інтернет. У цьому додатку віддаленого користувача VPN забезпечує захищений «тунель» крізь «недовірчу» мережу, в даному випадку – мережу Інтернет. Різні «тунельні» протоколи, включаючи протокол тунелювання між вузлами (точка-точка) (PPTP – Point-to-Point Tunneling Protocol) та протокол тунелювання канального рівня (L2TP – Layer 2 Tunneling Protocol) використовуються разом зі стандартними рішеннями централізованої ідентифікації, таких як сервери Cisco RADIUS.

Такі ж VPN технології можуть бути використані для захисту безпровідного доступу у мережах WLAN. У цьому випадку недовірчою мережею є безпровідна мережа. Точки безпровідного доступу конфігуруються для відкритого доступу без WEP кодування, але

безпровідний доступ ізолюється від корпоративної мережі сервером VPN. Точки безпровідного доступу можуть бути з'єднані разом через віртуальну LAN або LAN, яка розгортається в демілітаризованій зоні та з'єднується з сервером VPN. Точки безпровідного доступу все ще необхідно сконфігурувати в закритому режимі із SSID (пристроєм визначення ідентифікатора абонента, що здійснює виклик) для сегментації мережі. Автентифікація та повне шифрування через безпровідну мережу забезпечується через VPN сервери, що також виконують роль брандмауерів та шлюзів до внутрішньої корпоративної мережі. На відміну від WEP ключів та підходів до фільтрування MAC адрес рішення, що базуються на VPN та є масштабовані для великої кількості користувачів. [2], [3]

Мобільність є важливою у безпровідних застосуваннях, оскільки очікується, що мобільний IP діятиме аналогічно дзвінкам в мережах телефонії. WLAN'и повинні співпрацювати, щоб гарантувати санкціонованим користувачам, що їм немає необхідності реєструватися знову до існуючого домену безпеки і, що їх потік інформації та сесії будуть неперервними. Під цим розуміється можливість єдиного введення паролю (при вході в діалогову систему) і доступ, і керування пропускною здатністю, що належить користувачеві. Іншим спорідненим моментом є те, що роумінг між безпровідними мережами не є цілком прозорим. Користувачі здійснюють реєстрацію лише в момент переходу між VPN серверами в мережі або, коли система клієнт відновлює роботу з аварійного режиму. Деякі VPN рішення мають змогу повторно авто-підключитися до VPN.

Предмет оптимізації

Підслуховування – загроза номер один у мережах WLAN. Загрозою може бути випадкова або добре спланована дія, яка має фінансову вигоду чи без неї, зловмисником може бути добре навчений та «озброєний» фахівець, якого може фінансувати чужий уряд. Зловмисником може навіть виявитися старшокласник, який випадково підслухав розмову. Незважаючи на джерело загрози, необхідно забезпечити конфіденційність, цілісність, автентифікацію та неможливість відмови від встановлення комунікаційної сесії та авторства того, що зловмисник не відправляв даного повідомлення.

Існує 12 параметрів проектування, які повинні зберігатися при виборі цієї чи іншої архітектури безпровідної безпеки та при проектуванні захищених безпровідних пристроїв. Без спеціально замовлених показників, параметрів ними є: швидкість роботи в реальному масштабі часу з незначними затримками мережевих додатків; потужність, яка споживається; легкість інтеграції та вбудованість; легкість технічного розвитку; гнучкість та можливість вдосконалення; вартість впровадження; первинна вартість для користувача/замовника; операційна залежність від інших зовнішніх компонентів безпровідної системи; фізична захищеність (захист від невмілого використання та виявлення втручання); стійкість криптографічної системи; потужність двосторонньої автентифікації; випадковість генерування ключів та вектора ініціалізації (IV - Initialization Vector).

Якщо інтегрована система будується на платформі SOC над стандартним CPU або DSP ядром (що називається тут головним внутрішньопроцесорним CPU), тоді функціональність безпеки виконується у вигляді вбудованого програмного забезпечення, що виконується загалом із ПЗП шляхом відбору циклів з внутрішньопроцесорного головного CPU або вбудованого DSP сопроцессора (у вигляді окремої мікросхеми).

Це - класичне правило проектування в галузі безпеки комунікацій, яке означає, що ніщо не може бути довірчим за межами криптографічного модуля. Це особливо видно у застосуваннях урядового зв'язку, де, наприклад, повинна бути забезпечена *Federal Information Processing Standard* (FIPS)-базована технологія виявлення втручань. Ось чому правила не можуть бути загальноприйнятими для завантаження із-зовні (за винятком деяких специфічних та дуже добре контрольованих оточеннь), оскільки доводитиметься мати справу з зловмисним або неправдивим правилом. Результуючим принципом є те, що достатня

функціональність повинна бути інтегрована в середині криптографічного модуля. У HORNET™ проектуванні, наприклад, пристрій CPU (головний CPU терміналу-телефону) є недовірчим місцем. Тому, ключі генеруються в середині криптографічної мікросхеми (кристалу). Випадкові числа, які використовуються для генерування векторів ініціалізації (також відоме як початкове значення) генераторів випадкових чисел також генеруються в середині цієї криптографічної мікросхеми. При мінімізації випадковості виникають проблеми із надмірною довірою до іншого компоненту.

Припустимо, що хочемо забезпечити безпеку безпровідних терміналів, і потім припустимо, щоб наш проект:

- Забезпечував наскрізний захист для голосу і даних.
- Діяв в швидкостях реального часу.
- Був захищений від невмілого використання та складний для зламу.
- Базувався на відповідних стійких криптографічних алгоритмах.

Серед декількох необхідних модулів основою цього рішення є – криптографічний механізм. Шифрування, використовуючи, наприклад, алгоритми DES або 3DES, є привабливими для нашої архітектури.

Застосування 3DES шифрування в програмному втіленні в середині мобільного терміналу повинне бути виключене, поки теперішній CPU змінюється. Сучасні мобільні термінали використовують чіпи, що проектуються на основі SOC архітектури. Можливим було б змінити ядро CPU в середині пристрою головного центрального процесору (MCU) та пристосувати таке рішення в програмному забезпеченні разом із цифровим сигнальним процесором (DSP). Інше рішення, яке використовують деякі виробники, - створити зовнішній модуль-приставку, в середині якої 3DES виконується на окремому CPU (з його власною пам'яттю та живленням). Але це не те, що нам необхідно. Це рішення не є вбудованим та не є в середині мобільного терміналу. Це рішення не є швидким та, напевно, не є захищеним від невмілого використання.

Додаючи шифрування в реальному часі, вочевидь, це навантажить ресурси процесора. Якщо розглядати це з точки зору схеми, новіша криптографія може бути не симетричною (використовуючи Rijndael в апаратному втіленні необхідною є різна схема в обох кінцях зв'язку, оскільки планування ключів відрізняється на станціях шифрування та дешифрування).

До тих пір, поки MCU або немодульоване передавання обчислень мікросхеми може бути вдосконалене, наступне зростання споживання потужності пов’язане із тривалістю роботи батареї живлення та відповідно збільшується вартість пристрою. Неможливим буде виконання розглянутого 3DES алгоритму шифрування в програмному забезпеченні в стиснутому пристрої. Негативним є вигляд, коли розглядаються телекомунікації 2.5 або 3 покоління, оскільки багатомегабітний трафік за секунду (в тому числі потокове аудіо або стиснене/кодоване відео) буде посилатися в прямому та зворотньому напрямках.

Це і є причиною того, що телефони із шифроалгоритмом 3DES відсутні у вільному продажі у магазинах. Такі компанії, як Starium, SAGEM, Crypto AG, Siemens тощо (апарати, що продаються Rohde & Schwartz) пробували здійснити це завдання в декількох варіаціях, але найкращим досягненням було створення вбудованого модуля, який з'єднується із мобільним терміналом з власним RISC CPU, пам'яттю та живленням, що забезпечує комплексну безпеку у програмному виконанні низькорівневої криптографії та управління ключами. Це рішення працює на сумісних пристроях одного і того ж виробника і може працювати у низько швидкісних комунікаціях (телефонія), при чому вартість коливається від $100 за модуль до $44,000 за захищений якісних модуль. [4]

Повернемося тепер до апаратного підходу. А що коли ми будемо використовувати DES шифратор замість програмного забезпечення? Існує кілька чудових DES шифраторів у кремнієвій або IP формі ядра. Чому б не ліцензувати один із цих багаточисельних IP ядер

шифрування DES, які можуть бути легко інтегровані в ASIC? Чому б не спроектувати один з них в нашому мобільному терміналі?

Ці ASIC та IP ядра, що базуються на технології потокового шифрування і/або блокового шифрування, що може застосовуватися на дуже великих швидкостях. Це займає відносно маленьку частинку кремнію і може бути пов'язане з різними механізмами генерування випадкових чисел та генерування ключів, планування, заміна та управління з відповідними методами для автентифікації і вимогами до PKI (Public Key Infrastructure – інфраструктура відкритих ключів) нашого суспільства у майбутньому. Вони – сучасні проекти, які використовуються в малопотужних CMOS технологіях і виготовляються для продажу за декілька доларів.

Програмне забезпечення проти технічних засобів

Звертаючись до таксономії систем (з точки зору обчислювальних потреб) безпровідних комунікацій, можна запропонувати загальну класифікацію підходів здійснення безпеки, виходячи з того, що повинно бути захищеним: велика кількість трафіку, який обробляється у швидкісних мережах, особливо, коли він передається в реальному масштабі часу. Типовими прикладами є: телефонні розмови, відео конференц-зв'язок, потокове аудіо або передавання кодованого відео, (наприклад, послуга відео на замовлення), дані телеметрії тощо. Не кожен завжди має можливість повільно обробляти цей тип даних в програмному забезпеченні, потенційно виконуючи подвійні проходи даних (як у деяких алгоритмах компресії), оскільки дані приходять з лінії з постійною швидкістю та повинні бути оброблені в реальному масштабі часу. Апаратних ресурсів не вистачає, щоб тимчасово буферувати масу даних, тому переповнення буферу призводить до втрат, допоки архітектура системи залишається такою, що повна обробка може бути виконана до того, як нова партія даних поступить на вхід; невелика кількість трафіку для обробки у сучасних високошвидкісних мережах, які передаються в реальному масштабі часу. Типові приклади цієї сфери – операції електронної комерції або комерції з використанням сотового зв’язку, передача номера кредитної картки, вибір специфічної послуги для замовлення, вибір розміщення з підписом, інструкціями до свого брокера, витягом інформації банківського рахунку, роблячи електронні платежі та перегляд сторінок HTML у технологіях мікро-браузер (WAPstyle, який в мобільному безпровідному пристрої буде, звичайно, конвертуватися у WML – мову гіпертекстової розмітки документів для безпровідних пристроїв).

Якщо програмне забезпечення не може зробити це – це повинна зробити апаратна частина. Але постає питання апаратне забезпечення якого типу?

Апаратне забезпечення з можливістю переконфігурації чи без неї

Під технічними засобами, що переконфігуровуються ми маємо на увазі клас інтегральних схем, які відомі швидше як FPGA (програмована вентильна матриця), хоча є також інші пристрої, що схожі на програмовані логічні пристрої (PLDs), які могли б наблизитися до того ж визначення, але не до властивостей), їх можна купити у магазині та сконфігурувати за бажанням проектувальника. Кожна конфігурація може перероблятися в межах долі секунди та впродовж неї; інтегральна схема FPGA може бути запрограмована на виконання цілком різних функцій. Тому можна вважати про безмежну кількість переконфігурацій. Тема надзвичайно детально розроблена, оскільки різні виробники пропонують різну архітектуру, різні техніки конфігурування, засновані на різних технологіях об’єднання. Тому лише поверхнево оглянемо важливість та переваги застосування FPGA в розвитку захищених безпровідних комунікаційних систем.

Пристрої FPGA можуть переконфігуровуватися з метою змінити логічні функції, при розташуванні у системі. Ця здатність дає системному проектувальникові виняткову свободу, яку не надають інші типи логік. Технічні засоби можуть бути змінені так легко як програмне

забезпечення. Вдосконалення моделі або її модифікації є простими та можуть бути зроблені в польових умовах. FPGA можуть навіть переконфігуровуватися динамічно, щоб виконувати різні функції в різні моменти часу. Перепрограмована логіка може використовуватися у різних видах систем для виконання системної самодіагностики, для створення систем, які б мали можливість переконфігуровуватися для різних середовищ або операцій, або використовувати універсальні апаратні засоби для заданих додатків. Додатковою перевагою, використовуючи пристрої FPGA, що повторно конфігуруються є спрощення апаратного засобу, відлагодження та зменшення часу на виготовлення готової продукції. В той же час, в деяких контекстах проектувальники використовують логіку FPGA, що повторно конфігуруються, щоб здійснювати в цих технічних засобах обидва алгоритми з відкритим ключем для генерування та захисту обміну сесійного ключа та алгоритмів з індивідуальним ключем, що традиційно використовується у груповому шифруванні трафіку. Цей підхід є дуже корисним в наземних системах, але через вартість і споживання потужності він не може бути використаний у малих портативних безпровідних системах. Єдиним виключення до цього правила є потенційно великі безпровідні установки або транспортабельні пристрої, що схожі на ті, які знаходяться під увагою уряду та військового сектору. [5]

Базуючись на цих фундаментальних характеристиках технології, ми можемо сказати, що в безпровідній сфері використання логіки, що повторно конфігурується, обмежене певним набором аспектів:

- Для проектування дизайну з обмеженими ресурсами, FPGA може бути використаний як емулятор фактичної схеми, для того, щоб одного разу його втілити на спеціальному PCB (power control block – силовий блок управління) адаптері, тоді користувач зможе вставити його в слот ПК та з відповідними драйверами та програмним забезпеченням відновити модельоване середовище для наочності, визначення параметрів, аналізу і/або оцінки функціональності.
- Завдяки їх фізичним розмірам, високому споживанню енергії і (для вищих ступенів інтеграції) низькій швидкодії (в порівнянні з ASIC швидкості вх/вих і обчислювальній потужності), і високій вартості (вартість деяких пристроїв FPGA сягає кількох тисяч доларів), пристрої FPGA не можуть бути віддалено оглянуті для забезпечення функціональності в будь-яких недорогих безпровідних пристроях, які орієнтовані на споживача, наприклад, PDA та мобільні телефони. Деякі новіші моделі можуть бути легко інтегровані у високошвидкісні системи комунікації.
- Пристрої FPGA є ідеальними для відлагодження проекту, особливо, якщо синтезований апаратний опис може бути нанесений на план командою проекту від сімейства FPGA на контекст ASIC.
- Пристрої FPGA, вочевидь, можуть бути використані у великих безпровідних системах, великих (транспрортабельних або ні) передавачах та приймачах, репітерах, пристроях сканування спектру та обладнанні розвідки. Легкість інтеграції в більшу платформу, проста зміна робочої програми є суттєвою перевагою у сфері урядового зв'язку, де різносторонність, гнучкість, і функціональність в багатьох випадках мають первинну важливість в порівнянні з вартістю або споживанням енергії.

Окрім скорочення циклів проекту і розробки, пристрої FPGA також можуть використовуватися для виготовлення прототипів як рентабельного рішення для виробничих потужностей аж до декількох тисяч систем за місяць. З наступним зменшенням собівартості продукції, розробники FPGA пропонують засоби і технологічні прийоми для міграції проекту на масково-програмовані пристрої.

Для проектувальника захищеного чіпа комунікації, FPGA пропонує безпрецедентну гнучкість системного проектування. Архітектор безпеки може зараз експериментувати з різними блоковими або потоковими шифрами, з різними хеш-механізмами, різними інтерфейсами з головним термінальним CPU (пристрій керування), поки характеристики не

будуть проаналізовані та оцінені. Системні рішення основані не лише на програмному моделюванні, яке вирішує або ні усі недоліки продукції, що випускається. Кінцевий продукт реалізовується на FPGA, фактична поведінка якого може документуватися.

Завантаження даних конфігурації в спеціальні елементи оперативної пам'яті виготовляє пристрої FPGA за спеціальним замовленням. FPGA можуть активно зчитувати їх дані конфігурації із послідовного або паралельного PROM (Programmable Read-Only Memory - ППЗП) (привілейований режим), або дані конфігурації можуть бути записані в FPGA від зовнішнього пристрою (у непривілейованому або периферійному режимах). Розробник FPGA, зазвичай, забезпечує його потужним і сучасним програмним забезпеченням, перекриваючи кожен аспект проекту, від схематичного або динамічного запису, планування, моделювання, автоматичне розміщення блоків ярусу, виконуючи розводки з'єднувальних елементів, до створення, завантаження, зчитування лише із записаної інформації потоку бітів конфігурації [6], [7].

Висновок

В статті були розглянуті програмовані вентильні матриці (FPGA) та проблемно-орієнтовані інтегральні мікросхеми (ASIC), завдяки яким здійснюється рух щодо мінімізації, більшої інтегрованості, швидкості та меншої вартості пристроїв захисту безпровідних мереж. Цей курс пришвидшить ріст технологій захисту безпровідних мереж. В статті також була розглянута можливість оптимізації безпровідної безпеки за допомогою FPGA та ASIC.

Список літератури

1. Unified Security Architecture for Enterprise Network Security [Text]. – Nortel Networks white paper, 2003. – NN 102060-0902.

2. The CIO's Guide to Wireless [Text]. – Synchrologic (Intellisync) white paper, 2003.

3. Webb, William. The Future of Wireless Communications [Text] / William Webb. – Boston: Artech House, 2001.

4. Wilcox, D. A DES ASIC Suitable for Network Encryption at 10Gbps and Beyond [Text] / D. Craig Wilcox, G. Pierson Lyndon, J. Robertson Perry, L. Witzke Edward, Karl Gass // Cryptographic Hardware and Embedded Systems Int'l Workshop Proceeding: Lecture Notes in Computer Science. – Springer-Verlag, 1999. – Vol. 1717. – pp. 37-48.

5. Ярочкин, В. И. Безопасность информационных систем [Текст] / В. И. Ярочкин. – М.: Ось-86, 1996. – 320 с.

6. Dobkin, Daniel. RF Engineering for Wireless Networks [Text] / Daniel Dobkin. – Elsevier, Burlington, MA: Hardware, Antennas and Propagation, 2005.

7. Бачинський, І. В. Термінологічний словник з інформаційної безпеки [Текст] / І. В. Бачинський, В. Б. Дудикевич, В. С. Зачепило, Л. Т. Пархуць, В. В. Хома, О. В. Яструбецький. – Львів, 2005. – 140 с. – ISBN 966-8041-34-8.

Надійшла 4.11.09