предельные частоты гармоник в спектрах их сигналов могут достигать значений около 1,5 - 3 ГГц. Таким образом, проблема обеспечения требуемых системных свойств, электромагнитной и информационной защищенности современных компьютеров - это проблема сверхвысоких частот.

Наличие токов проводимости и смещения на СВЧ предъявляет повышенные требования к однородности и сплошному характеру материалов экранов. Наличие неоднородностей (щелей, присоединительных, вентиляционных отверстий) может привести к существенному снижению эффективности экранирования.

Для достижения высоких уровней экранирования в требуемом диапазоне частот эффективными конструкциями являются многослойные экраны с чередующимися магнитными и немагнитными металлическими слоями, которые наносятся на внутренние поверхности корпусов компьютеров вакуумным напылением тонких пленок с толщиной в несколько десятков микрометров. Многослойные экраны существенно более эффективны, чем однослойные одинаковой толщины.

Методики, построенные на основе эффективных принципов декомпозиции, а также соответствующих численных моделей экранов, пригодны для расчета на ЭВМ в широком диапазоне частот (от низких до СВЧ) с точностью, определяемой по критериям практики.

Для того, чтобы не было отставания от современной продукции компьютерного рынка, процесс новых опытно-конструкторских разработок и внедрения в производство отечественных информационно-защищенных компьютеров должен быть практически непрерывным.

Литература: *1. Горбачев О.С. Корпоративные системы - секреты и кухня. Украинский еженедельник по информационным технологиях и компьютерному рынку. - 1999 - №25 - с.1-4. 2. Перлин М.А. Мир финансов. Автоматизация расчетных операций банков и фондовых бирж. - М.: Церих ПЭЛ, 1995. 3. Стрюченко В.А. Отечественный компьютер "Pluton" с технической защитой информации. Бизнес и безопасность. - 1999 - №1 - с.14-15. 4. Северинский Е.А., Савченко А.С. Обзор первых материнских плат на чипсете i810. Компьютерное обозрение. - 1999 - №28 - с.15-19. 5. Левченко Г.Т., Сагайдак В.А. Сучасні тонкоплівкові технології виробництва та модернізації захищених засобів інформаційних систем. Матеріали ювілейної науково-технічної конференції "Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні" - Киев, 1999 - с.123-124. 6. Зиньковский Ю.Ф., Клименко В.Г., Погребняк В.П. Электромагнитная совместимость радиоэлектронных средств. - К.: УМК ВО, 1990. 7.Лейбман А.М. Функционально-модульный подход к проектированию устройств СВЧ и КВЧ. Технология и конструирование в электронной аппаратуре. - 1998 - №3-4 - с.9-11. 8. Зиньковский Ю.Ф., Клименко В.Г.Исследование диффузионного взаимодействия электромагнитных полей и экранов. Известия ВУЗов "Радиоэлектроника" - 1994 - №5-6 - с. 18-24. 9.Зиньковский Ю.Ф., Клименко В.Г. Електромагнітна, інформаційна захищеність та сумісність електронних апаратів. Навчальний посібник для студентів вищих технічних закладів.- ЖІТІ, 1999-357с.*

УДК 681.31

МІЖНАРОДНІ СТАНДАРТИ В ГАЛУЗІ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЇХ МІСЦЕ В РОЗВИТКУ СТАНДАРТИЗАЦІЇ В УКРАЇНІ

Олексій Фаль, Ірина Івченко

Інститут кібернетики ім В.М. Глушкова НАНУ, Національний банк України

Анотація: **Розглянуто питання використання міжнародних стандартів в Україні і їх місце в процесі становлення та розвитку стандартизації в Україні.**

Summary: **The possibility of usng international standards in Ukraine is considered; their place in setting ur and development of standarditation process for Ukraine is determined.**

Ключові слова: **Міжнародні та державні стандарти.**

У 1995 році при Держстандарті України був заснований Технічний комітет ТК 105 "Банківські та фінансові системи і технології", в рамках якого почав функціонувати підкомітет "Захист інформації". Серед завдань, які покладено на цей підкомітет, є приймання участі в розробленні міжнародних стандартів, що стосуються питань забезпечення захисту банківських інформаційних технологій. Згідно з поставленим завданням була налагоджена взаємодія з відповідними комітетами Міжнародної організації зі стандартизації (ISO), офіційним представником України в якій є Держстандарт України.

Розроблення державних стандартів в Україні, особливо у галузі захисту інформації, здійснюється дуже повільно через брак коштів, недостатню правову та нормативну базу. Однак, такі стандарти дуже необхідні в Україні, особливо в банківської діяльності. Існування і успішне функціонування системи електронних платежів Національного банку України, швидкий розвиток інформаційних технологій в банківської системі України зараз практично не мають достатньої бази стандартів України. Брак відповідних державних нормативних документів до цього часу Національний банк України намагався заповнювати своїми нормативними документами, в тому числі і в галузі вимог до захисту банківської інформації. Саме тому участь у розробці міжнародних стандартів у рамках підкомітетів ТК 105 може бути дуже корисною для збирання та накопичування знань та навичок у стандартизації в галузі захисту інформації і для розробки державних стандартів в Україні.

Розроблення міжнародних стандартів ISO здійснюється у відповідності з прийнятими в цій організації директивами. В цих директивах встановлюється порядок затвердження об`єктів стандартизації, а також регламентується процес розроблення стандартів. Виділяють три основні етапи процесу розроблення стандартів: створення і обговорення робочого проекту, створення і обговорення технічного проекту (в англійській транскрипції - committee draft); створення й обговорення проекту міжнародного стандарта (DIS). Результатом цього процесу повинно бути затвердження міжнародного стандарта. Бувають, хоч і досить рідкі, випадки, коли процес переривається через безперспективність у подоланні недосконалості або хибності стандарта.

Основна робота по розробленню стандартів проводиться в робочих групах, які функціонують в рамках підкомітетів. Кожна країна – член ISO, може мати два статуси: пасивний учасник і активний учасник. Пасивний учасник має право розглядати проекти стандартів і надсилати свої зауваження. Активний учасник в доповнення до цих можливостей має право і зобов`язання приймати участь в голосуванні при вирішенні питання про перехід проекту документа від однієї стадії до іншої.

Наш підкомітет приймає участь в роботі комітету ISO TC 68 “Banking and related financial operations” і підкомітету ISO/IEC JTC1 SC 27 “Security techniques”. Найбільша кількість стандартів, що стосуються безпеки інформаційних технологій, розробляється саме в останньому підкомітеті. Протягом чотирьох років наш підкомітет мав статус пасивного учасника у цьому підкомітеті ISO. Дякуючи активності при поданні зауважень щодо проектів стандартів, нашому підкомітету запропонували стати активним учасником. З березня 1999 року Україна є активним учасником, що демонструє як гарну оцінку наших фахівців в галузі захисту інформаційних технологій, так і підвищення відповідальності з нашого боку при розгляді проектів міжнародних стандартів.

Розглянемо деякі проекти стандартів, щодо яких відбувалося голосування з нашою участю.

Першим таким проектом була нова редакція стандарта ISO/IEC 9798-2 “Автентифікація об`єктів з використанням симетричних алгоритмів”. Ми вирішили утриматися при розгляді остаточної редакції проекту, так як в ній не були враховані зауваження криптологів, в яких вказувалось на неточності в старій редакції стандарта.

Наступне голосуваняня стосувалося трьохчастинного стандарта ISO/IEC 15408 “Критерії оцінювання безпеки інформаційних технологій”. Цей стандарт, що широко відомий під назвою “Спільні критерії”, офіційно став основою для проведення сертифікаційних випробувань в галузі безпеки інформаційних технологій. Стандарт розроблявся протягом шести років з залученням провідних фахівців з усіх країн, які грають ключову роль в дослідженні проблем безпеки інформаційних технологій. Перша частина є вступом і описом загальної моделі. В другій частині викладаються функціональні вимоги, а в третій – вимоги гарантій безпеки інформаційних технологій.

Продовжується робота над п`яти частинним технічним звітом ISO/IEC 13335 “Настанови щодо менеджменту безпекою інформаційних технологій ( GMITS)”. В минулому році успішно дійшла до закінчення четверта частина, що має назву “Вибір засобів захисту”. На останній стадії знаходиться п`ята частина “Зовнішні канали зв`язку”.

Останнім часом багато уваги приділяється криптосистемам, які базуються на використанні еліптичних кривих, заданих в скінченних полях. З огляду на актуальність даного напрямку започаткована робота над трьохчастинним проектом ISO/IEC 15946 “Криптографічні методи, що базуються на еліптичних кривих”. Перша частина має назву “Загальні положення”. Друга частина присвячена цифровому підпису, а третя – розподілу ключів. Найбільше дорікань зазнала третя частина, що позначилося на її затриманні в стадії технічного проекту. Дві інши частини проходять голосування, як остаточні редакції технічного проекту.

Як відомо, при використанні асиметричних алгоритмів велике значення надається сертифікатам відкритих ключів. Виготовлення цих сертифікатів здійснюється так званими центрами сертифікації. Крім виготовлення сертифікатів такі центри можуть надавати інші послуги, пов`язані з використанням асиметричних алгоритмів (часові відмітки, ведення архівів, відновлення ключів і т.п.). Всі ці послуги створюють так звану інфраструктуру відкритих ключів. Важливість цих питань знайшла відображення у великій кількості проектів, які розробляються в різних органах зі стандартизації. Безпосередньо в підкомітеті SC 27 розробляються два документи: технічний звіт ISO/IEC 14516 і стандарт ISO/IEC 15945. В стандарті “Специфікації послуг третьої довіреної сторони щодо підтримки застосування цифрових підписів” описується технологія забезпечення автентичності електронних

документів. Технічний звіт “Настанови щодо використання і менеджементу послугами третьої довіреної сторони” стосується організаційних аспектів діяльності виділених центрів сертифікації віжкритих ключів.

Найбільших змін зазнав стандарт ISO/IEC 9796 “Цифровий підпис з відновленням повідомлень”. Нагадаємо, що колишній одночастинний стандарт мав бути доповнений іншими частинами. Після кількох ітерацій було вирішено, що це буде трьохчастинний стандарт. Перша частина – з використанням надлишковості, друга частина - з використаняям хєш-функцій, третя частина – на основі дискретних логарифмів. Після кількох атак, які спричиняють екзестинціальну підробку підпису, від першої частини довелося відмовитися, а в другій частині назріла необхідність зміни способу форматування.

Ряд проектів стандартів стосується подальшого розвитку і застосування базового стандарта з оцінювання засобів забезпечення безпеки інформаційних технологій (ISO/IEC 15408). В даний час проходить голосування, що стосується започаткування таких стандартів: безпека інформаційних мереж, генерування випадкових чисел, генерування простих чисел, декларування постачальників засобів захисту про їх відповідність прийнятим стандартам.

Таким чином, навіть короткий перегляд стандартів, за якими наш підкомітет приймав участь у голосуванні, показав, яка велика увага приділяється у світі питанням захисту інформаційних технологій. Розширення таких питань не може бути дивним у зв`язку з бурхливим розвитком інформаційних технологій, особливо у банківській і фінансовій сфері: використання карток для оплати послуг і товарів, електронна комерція, домашне банківське обслуговування, інтернет-технології тощо.

Слід також відмитити тенденцію, яку чітко видно у сфері стандартизації, а саме: спроби створення стандартів, які описують ідеологію застосування тих або інших принципів побудови захисту інформації в інформаційних технологіях. Замість опису конкретних алгоритмів часто надаються принципові підходи до їх побудови. Це дає змогу дуже гнучкого використання таких стандартів для побудови системи захисту інформаційних технологій.

Така тенденція у розвитку міжнародних стандартів може бути дуже корисною з точки зору побудови системи державних стандартів. Гармонізація міжнародних стандартів в галузі захисту інформації і безпеки інформаційних технологій може надати можливість швидкої побудови основи для розвитку стандартизації в Україні. Такий шлях створення стандартів України є достатньо дешевим і швидким, який одночасно дозволить усунути велику кількість проблем, які вже виникали в інших державах при створенні стандартів у галузі захисту інформації і безпеки інформаційних технологій. Це зовсім не означає, що потрібно повністю копіювати міжнародні стандарти для України, але застосування найкращих з них в Україні дозволить швидко вирішити частину наших питань при побудові основ стандартизації в Україні.

УДК 006.4.2:002; 53.081:006.354

НОРМАТИВНЕ ТА МЕТРОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

Ярослав Юзьків, Євген Козир, Олександр Шевченко
Український науково-дослідний інститут стандартизації, сертифікації та інформатики

Анотація: **У статті розглянуто нормативні документи захисту інформації в комп’ютерних системах та метрологічне забезпечення у галузі ТЗІ, зокрема, державні стандарти України з повірочних схем для повірки засобів вимірювальної техніки, що можуть використовуватися у сфері технічного захисту інформації.**

Summary: **This article deals with normative documents of security of information in computer systems and metrological support in domain of technical security of information in particular state standards of Ukraine concerning verification schemes for verification of aids of measurement technique which way be used in sphere of technical security of information**.

Ключові слова: **інформація, стандарт, захист інформації.**

Міжнародні та міждержавні стандарти

1. Згідно з каталогом Міжнародної організації зі стандартизації ISO за станом на 01.01.1999 безпосередньо захисту інформації в комп’ютерних системах стосуються понад 50 стандартів, які розподілено в основному по таких групах:

- 35.040 «Коди і кодування інформації» - 20 стандартів;
- 35.100.01 «Взаємозв’язок відкритих систем взагалі» - 7 стандартів;