В. В. БЕЗСМЕРТНИЙ, А.М.ЗАЧЕПА.

ЕКОНОМІЧНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ РЕСУРСИ УКРАЇНИ.

Розглядаються можливі варіанти доступу до комп'ютерів та безпорадність використання жодних засобів криптографічних шифрувань. Наведені приклади можливої економічної та інформаційної небезпеки для України.

Рассматриваются возможные варианты доступа к компьютерам и бесполезность использования каких бы то ни было средств криптографического шифрования. Приведены примеры возможной экономической и информационной угрозы для Украины.

The possible variants of access to computers and uselessness to use any means of cryptographic enciphering discussed. Examples of possible economic and information threat for Ukraine are presented.

Країнам, що утворились на пострадянському просторі, а також іншим країнам світу може загрожувати не тільки воєнна, але і економічна та інформаційна небезпека.

Обґрунтування можливості такої небезпеки лежить у передбаченні реалізації сучасних можливостей комп'ютерної техніки. Обчислювальні центри вже давно перейшли рубіж низьких частот, на яких захист інформації можна було забезпечити наприклад розв'язкою живлення обчислювальної техніки за допомогою мотор-генераторів та екрануванням приміщень. Такі засоби вже не забезпечують безпеку. Наприклад, радіохвилі мобільного телефону розповсюджуються на достатньо велику відстань. З успіхом вони працюють в металевих ліфтах і шахтах, а також екранованих залах обчислювальних центрів.

Розробники сучасних процесорів можуть закладати можливість передачі всієї інформації, що обробляється на комп'ютері на супутник – розвідник. Слід зазначити, що в даному випадку неможливо здійснити захист інформації жодним методом кодування, так як працівник, який має доступ до цієї інформації власноруч вводить пароль для роботи з нею.

Розробники процесорів без великих зусиль можуть додати можливість керування процесором ззовні, а відтак і в цілому комп'ютером, як мобільним телефоном - з супутника. Наприклад, набравши номер процесора, як номер мобільного телефону, можна до нього безпосередньо "додзвонитись", задати зовнішню команду управління, зчитувати, записувати, знищувати любу інформацію з диску, працювати, з відкритим користувачем, любим засекреченим файлом в реальному часі без потреби знати пароль для доступу, а також взнати пароль, контролюючи натиснуті оператором клавіші на клавіатурі. Причому, мова може йти як про нанесення шкоди явної, так і неявної. Так достатньо внести невелику зміну в деяку програму, або базу даних, і користувач отримує зовсім інші результати роботи або досліджень, і вважати їх до певної міри коректними. Наприклад, в військових системах наведення, це може призвести до зміни координат цілі.

Отже процесор, працюючи на частоті, наприклад в межах 0,8 – 3.6 Ггц, використовуючи в якості антени провідники на материнській платі може, через один із виводів процесора, випромінювати у космічний простір (за аналогом мобільного телефону) любу службову інформацію, яка сприймається супутником і передається за призначенням.

Відмінністю даної гіпотези від інших є те, що до цієї пори у літературі і Інтернеті зустрічається аналіз випромінювання процесора виключно у замкнутому просторі самого тіла процесора, де екраном з однієї сторони являється підкладка, а з другої сторони радіатор процесора. Аналізу ж можливості використання одного з виводів процесора та частини печатного монтажу материнської плати в якості антени не зустрічається.

При цьому значному дослідженню піддавався аналіз та можливість електромагнітного перехвату. Тобто, сучасними технічними засобами отримувати інформацію, безпосередньо підключаючись до комп'ютерної системи за рахунок перехвату випромінювань центрального процесора, дисплею, комунікаційних каналів, принтера і т.п., знаходячись на достатній відстані від об'єкту перехвату. Також отримувати інформацію із зовнішніх комунікаційних каналів, шляхом безпосереднього підключення до ліній периферійних пристроїв. При цьому об'єктами безпосереднього прослуховування можуть бути кабельні і дротяні системи, наземні мікрохвильові системи, системи супутникового зв'язку, а також спеціальні системи урядового зв'язку [1].

Виходячи із згаданої гіпотези можна в великою достовірністю стверджувати, що оператор персонального комп'ютера не має жодної гарантії, що службовий файл, після відкриття його у комп'ютері, не передається процесором на супутник чи інший пристрій управління. За таких

обставин жодний захист паролями, або іншими засобами криптографічних шифрувань, виявляються цілковито безпорадними.

Ще більша небезпека може бути у випадках ведення бойових дій, або війни з залученням комп'ютерної техніки.

Як приклад, можна передбачити, закладений в процесор на стадії розробки режим, коли по сигналу з супутника, процесор раптово виключить комп'ютер, або взагалі заблокує його роботу на певний час. Так, на прикладі з мобільним телефоном, оператор мобільного зв'язку одним натиском кнопки може виключити обслуговування одного чи одразу всіх мобільних телефонів, перетворивши їх у кусочки мовчазного непрацюючого заліза.

Пригадаємо війну в Іраку в 1991р. Закуплені Іраком системи ППО французького виробництва були відключені на відстані французькими фахівцями спеціальним кодовим сигналом. Коли ми бачимо в Центрі управління космічними польотами Росії комп'ютерні системи виробництва DELL (США, Великобританія), а на атомних станціях Росії упроваджуються системи американського виробництва, то встає слушне питання: "А чи не буде це все відключено кодовим сигналом як тиск на Росію?" Результат - зупинені потяги, літаки стоять в аеропортах, відключені всі комунікації Росії (за винятком старих аналогових систем російського виробництва), неможливість рахувати будь-яку інформацію з будь-яких електронних носіїв. Це не панічний катастрофізм, а чітке уявлення про те, що жодна людина в Росії не знає досконально, що роблять всі процесори (Pentium, AMD, і т.д.) [2]. Жодна людина в Росії не має у своєму розпорядженні повної інформації про початкові коди Windows (представники Microsoft в Росії теж не мають у своєму розпорядженні даної інформації).

Усе згадане може мати і пряме відношення до України.

Управління комп'ютерними процесорами з супутника у мирний час може дозволити отримати доступ до Національних інформаційних ресурсів України, окремих документів і масивів інформації. А також збирати, обробляти, зберігати та ефективно використовувати результати інтелектуальної, творчої та інформаційної діяльності, бази й банки даних, всі види архівів, бібліотеки, музейні фонди та інші, що містять дані, відомості й знання, зафіксовані на відповідних носіях інформації і мають споживацьку вартість (політичну, економічну, соціокультурну, оборонну, історичну, ринкову, інформаційну тощо).

Для такої системи супутникової розвідки не буде існувати перешкод ні в територіально розподілених державних і корпоративних комп`ютерних мережах, ні на серверах, ні в системах спеціального призначення і загального користування.

Не забезпечить захист інформації і застосування інших операційних систем.

Фактично, виробник - монополіст мікропроцесорів може передбачити і виготовити в кристалі любі додаткові функції передавача, антеною якого можуть бути як виводи самого процесора так і шини материнської плати.

Проблематика інформаційної безпеки в Україні потребує глибокого наукового дослідження на міжгалузевому рівні з метою напрацювання науково обґрунтованих методик виявлення та розкриття правопорушень та комп`ютерних злочинів, що здійснюються за допомогою сучасних інформаційних технологій.

Тобто інформація і сучасна технологія стала чинником, який може призвести до значних технологічних аварій, військових конфліктів та поразок у них, дезорганізувати державне управління, фінансову систему, роботу наукових центрів тощо.

Застосування сучасних технологій можуть знизити бойові можливості збройних сил, а саме:

- блокувати системи управління ракетно-ядерною зброєю та інші стратегічні системи військового призначення;

- порушувати роботу систем управління військово-транспортними перевезеннями та інших систем забезпечення військових формувань (матеріалами, енергією, тощо);

- різке погіршення морально-політичної обстановки у військових формуваннях, серед їх резерву і зниження бойового духу особового складу внаслідок дезінформації, порушення систем забезпечення життєдіяльності, дезорганізації систем управління тощо.

Серед нових, найбільш важливих засобів "*інформаційної війни*", *сьогодні* називають різні математичні, програмні засоби типу "вірусів" і "закладок", засоби дистанційного знищення інформації, що записана на магнітних носіях, генераторами електромагнітних імпульсів, засоби неконтрольованого включення у закриті інформаційні мережі та ін.

Так, наприклад судячи з публікацій у США, використовують наступне визначення для ІВД: " Дії, прийняті для досягнення інформаційної переваги в інтересах національної військової стратегії і

здійснюючі їх шляхом впливу на інформацію і інформаційні системи противника при одночасному захисті власної інформації і своїх інформаційних систем" [3].

Отже інформатизація і автоматизація проникають практично на всі рівні військової ієрархії і практично у всі системи сучасної зброї.

Майже всі користувачі комп'ютерної техніки помічають, що іноді диск комп'ютера починає працювати навіть тоді, коли не завантажена жодна програма. Виникає слушне запитання. А що діється...?

Найгострішим завданням, на наш погляд, залишається також створення центру досліджень та боротьби, з так званою, комп'ютерною злочинністю, в якому необхідно було б організувати контактний пункт для отримання повідомлень про "кіберзлочини" та надання оперативної допомоги їх жертвам, організувати, на рівні держави, лабораторію для проведення комп'ютерних експертиз.

Якщо сьогодні на створення та функціонування такого центру не буде виділено достатніх фінансово-матеріальних ресурсів, то у недалекому майбутньому втрати економіки держави від комп'ютерної злочинності виявляться набагато більшими.

ЛІТЕРАТУРА

1. Владимир Голубев, www.crime-research.ru

2. http://www.is.khakasia.ru/author/

3. Леваков А. Пентагон готовится к "информационной войне" // Красная звезда. - 1995, 17 октября.

А. Л. ВАСИЛЬЧУК

СТРУКТУРНО-ФУНКЦІОНАЛЬНА ХАРАКТЕРИСТИКА МЕРИДІАНІВ (ОСНОВА І ДОДАТКОВІ СТРУКТУРИ МЕРИДІАНІВ)

Розглядаються каналові структури, їх компонування, будова та функції основи і додаткових структур меридіанів.

Рассматриваются каналовые структуры, их компонирование, строение, а также функции основы и дополнительных структур меридианов.

Channel structures including their composing are being researched, the structure and function of basis and supplementary meridian structures.

Основи меридіанів — це сукупності мікроканалів з виростів внутрішніх оболонок усіх тонкоматеріальних тіл (ТМТ) від місць локалізації початкових БАТ меридіанів, окремих мікроканалів з відгалужень вершин чакрових конусів відповідних основних, життєво важливих і функціонально забезпечувальних чакр, окремих вихідних мікроканалів сушумни, меруданди, іди, пінгали, лівого і правого зіркових каналів, відповідних меридіанів, усіх варіантів їх структуризації та з'єднань у багатошаровий каналовий пучок (мал. 1 — 4).

До основи будь-якого меридіана належать каналові шари, пучки, окремі оболонкові мікроканали, окремі чакрові мікроканали відповідних чакр, окремі вихідні сушумнові, мерудандові, ідові, пінгалові, лівозіркові і правозіркові мікроканали, окремі вихідні мікроканали відповідних меридіанів, оболонково-чакрові, оболонково-сушумнові, оболонково-мерудандові, оболонково-ідові, оболонково-пінгалові, оболонково-лівозіркові, оболонково-правозіркові, оболонково-меридіанові, змішані мікроканали, внутрішньомеридіанові кінцеві ультраканали, субультраканали і різні міжмікроканалові з'єднання. **Каналові утворення основ структурно і функціонально автономні** (мал. 2).

Найбільш структурованими каналовими утвореннями основ меридіанів є каналові шари. Вони утворюються оболонковими мікроканалами з виростів внутрішніх оболонок внутрішніх відділів усіх ТМТ. Шари з'єднуються в каналовий пучок, який розміщується між початковою і кінцевою БАТ меридіана. В основі розрізняють 15 кольорових шарів від кожного ТМТ. 1-й шар — внутрішній, 2—14-й шари — проміжні, а 15-й шар — зовнішній. 1-й шар — червоного кольору, утворюється мікроканалами з виростів внутрішньої оболонки внутрішнього відділу червоного ТМТ; 2-й шар — світлосяючого червоного кольору, з виростів внутрішньої оболонки світлосяючого червоного ТМТ; 3-й шар— оранжевого кольору, з виростів внутрішньої оболонки оранжевого ТМТ; 4-й шар — світлосяючого оранжевого кольору, з виростів внутрішньої оболонки світлосяючого