ПРИЛАДОБУДУВАННЯ ТА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ СИСТЕМИ

Ю.Довбуш, П.Стухляк, докт. техн. наук
Тернопільський державний технічний університет імені Івана Пулюя

ЗАХИСТ ІНФОРМАЦІЇ В INTERNET (ВІДКРИТІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ). МЕТОДИ ШИФРУВАННЯ ДАНИХ ЯК ОСНОВНИЙ МЕХАНІЗМ ЗАХИСТУ

Проаналізовано технічні та програмні аспекти захисту інформації в глобальній мережі Internet. Показано, як різноманітними програмними, апаратними та адміністративними засобами можна поліпшити захист інформації і підвищити надійність локальних інформаційних систем, під'єднаних до мережі Internet.

Вступ. Internet – глобальна комп'ютерна мережа, що охоплює увесь світ. Сьогодні Internet має майже 15 мільйонів абонентів у понад 150 країнах світу. Щомісяця розмір мережі збільшується на 7-10% (рис.1). Internet - це своєрідне ядро, яке забезпечує зв'язок між різними підмережами, що належать різним організаціям у всьому світі.

На перших порах Internet використовували винятково як середовище передачі файлів і повідомлень електронної пошти. Сьогодні ця система дозволяє розв'язувати більш складні завдання розподіленого доступу до інформаційних ресурсів. Майже п'ять років тому були створені оболонки, що підтримують функції мережового пошуку і доступу до розподілених інформаційних ресурсів та електронних архівів. Ці системи мають багато переваг: швидкодія, дешевий глобальний зв'язок, зручність для виконання спільних робіт, доступність програм, унікальна інформаційна база даних мережі Internet. Більшість організацій вбачають у глобальній мережі Internet логічне доповнення до своїх локальних мереж. Фактично Internet складається з безлічі локальних і глобальних мереж (LAN Local Area Network та WAN Wide Area Network) відповідно, що належать різним компаніям і підприємствам, зв'язаним між собою різними лініями зв'язку.

У мережі Internet використовують в основному стек протоколів на базі TCP/IP. Свою назву протокол TCP/IP отримав від двох комунікаційних протоколів. Це Transmission Control Protocol (TCP) і Internet Protocol (IP). Незважаючи на те, що в Internet використовують багато інших протоколів, його часто називають TCP/IP-мережею, оскільки ці два транспортні протоколи є найважливішими. Як і в будь-якій іншій мережі, в Internet існує 7 рівнів взаємодії між комп'ютерами: фізичний, логічний, мережовий, транспортний, рівень сеансів зв'язку, рівень представлення і прикладний рівень. Відповідно кожному рівневі відповідає відповідний набір протоколів (тобто правил взаємодії).

Протоколи фізичного рівня визначають вид і характер лінії зв'язку між комп'ютерами. В Internet використовують практично всі відомі на сьогодні способи зв'язку: від простого дроту (зкручена пара) до оптоволоконних ліній зв'язку. Для кожно кожного рівня вироблені відповідні протоколи логічного рівня, що займаються керуванням передачі інформації на каналі. Для фізичного рівня це SLIP, PPP; для мережевого - IP,ARP; для транспортного - TCP, UDP; для рівня сеансів - TCP, UDP, UUCP; для рівня представлення - HTTP, FTP, NNTP, SMTP та ін.; до протоколів прикладного рівня належать мережові послуги і програми їх представлення.

Характеристика загальних проблем захисту інформації в глобальній мережі Internet. Internet та інформаційна безпека несумісні за самою природою Internet. Його створювали як чисто корпоративну мережу, але вона сьогодні з допомогою одного стеку протоколів TCP/IP і спільного адресного простору об'єднує не тільки корпоративні і відомчі мережі, що є в принципі мережами з обмеженим доступом, що й звичайних користувачів, що мають можливість отримати доступ до Internet з допомою модемів. Тому нині актуальним є захист складових частин глобальної мережі Internet від несанкціонованого доступу.

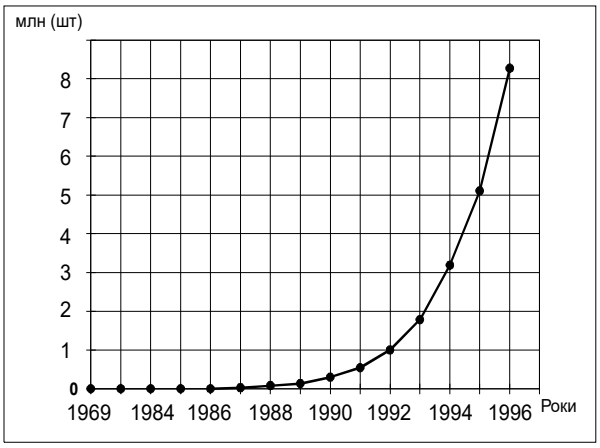

Рис.1. Динаміка зростання кількості комп'ютерів, під'єднаниз до Internet.

Як відомо, чим простіший доступ до мережі, тим нижча її інформаційна безпека. Платою за доступність Internet є загальне зниження інформаційної безпеки. Для запобігання несанкціонованому доступові до своїх комп'ютерів всі корпоративні та відомчі мережі, а також підприємства, що використовують технологію Intranet, ставлять різного роду фільтри (fire-wall) між внутрішньою мережею і Internet, що фактично означає вихід із спільного, чи єдиного, адресного простору. Ще більшу безпеку дає відхід від протоколу TCP/IP і доступ до Internet через шлюзи. Безпека даних є однією з основних проблем в Internet. З'являються все нові факти проникнення зловмисників у чужі інформаційні системи. Будь-яка організація, що має справу з інформаційними цінностями, рано чи пізно стикається з посяганнями на них. Є різні методи їх захисту. Найрадикальніший з них – фізичне від'єднання їх від мережі. Це, зрозуміло, повністю блокує доступ до них. Як тільки до інформації з'являється доступ з мережі, одразу ж теоретично виникає декілька каналів, якими зловмисники можуть отримати доступ до даних без відома власника. Може здатися, що з цієї ситуації немає виходу, але інформаційна безпека трохи подібна до безпеки мореплавання: обидві можливі лише з урахуванням допускового ступеня ризику.

В області інформації дилема безпеки формулюється так: потрібно вибирати між захищеністю системи та її відкритістю. Правильніше говорити не про вибір, а про баланс "відкритість - захищеність", оскільки система, що не є відкритою, не можна використовувати.

Банки останніми роками чи не найбільше стали використовувати глобальні мережі для своїх розрахунків і чи не найбільше зацікавлені у захисті своєї інформації. У банківській сфері проблема безпеки ускладнюється двома факторами: по-перше, майже всі цінності, з якими має справу банк (крім готівки та матеріальних цінностей), існують у вигляді інформації. По-друге, банк не може існувати без зв'язку із зовнішнім світом, без клієнтів, кореспондентів. При цьому зовнішніми каналами передається та сама інформація, що виражає цінності, з якими працює банк (або інформація про ці цінності та їх рух). До банку надходять документи, за якими банк переказує гроші з одного рахунку на інший. За свої межі банк передає розпорядження про рух цінностей на кореспондентських рахунках, так що відкритість банку задана за визначенням.

Інформаційна безпека та інформаційні технології. На початковому етапі автоматизація банківських систем (і взагалі засобів автоматизації банківської діяльності) не підвищувала відкритості банку. Спілкування із зовнішнім світом, як і колись, відбувалося через операторів і кур'єрів, тому додаткова загроза безпеки інформації виходила лише від можливих зловживань з боку спеціалістів з інформаційних технологій самого банку. Справа змінилася після того, як на ринку фінансових послуг стали з'являтися продукти, створення яких було немислиме без використання інформаційних технологій. У першу чергу, це пластикові картки.

З'явились банкомати, інші пристрої, що обслуговували ці картки. Тобто вони належали інформаційній системі банку, але їх розміщували поза межами банку з можливістю доступу до них сторонніх осіб. Відкритість системи збільшилася, і це змусило створити спеціальні засоби для контролю і регулювання обміну інформацією: додаткові засоби ідентифікації та аутентифікації осіб, які вимагають доступ до системи (PIN-код, інформація про клієнта на магнітній смузі або в пам'яті мікросхеми картки, шифрування даних, контрольні числа та ін.), засоби криптозахисту інформації в каналах зв'язку та ін. Ще один великий зсув балансу "захищеність-відкритість" у бік відкритості зв'язаний з телекомунікаціями. Системи електронних розрахунків між банками захистити відносно не важко, оскільки суб'єктами обміну інформацією є самі банки. Поряд з цим, там, де захистові не приділяли належної уваги, результатом була втрата інформації. Найбільш відомий для нас приклад – наша країна. Використання вкрай примітивних засобів захисту телекомунікацій в 1992 р. призвело до відчутних втрат через фальшиві авізо.

Загальна тенденція розвитку телекомунікацій і масового поширення обчислювальної техніки призвела в кінці кінців до того, що на ринку банківських послуг у всьому світі з'явилися нові, чисто телекомунікаційні продукти, такі як Home-Bank (вітчизняний аналог – "клієнт - банк"). Це забезпечило клієнтам цілодобовий доступ до автоматизованої банківської системи для виконання операцій, причому повноваження на банківські транзакції одержував безпосередньо клієнт. Рівень відкритості банківської системи значно виріс. Відповідно необхідні особливі, спеціальні засоби для збільшення захищеності інформації.

І, нарешті, настала епоха "інформаційної супермагістралі": вибухоподібний розвиток Internet і зв'язаних з ним послуг. Разом з новими можливостями ця мережа принесла й нову небезпеку. Здавалося, що немає різниці між тим, як клієнт зв'язується з банком: комутованою лінією, що приходить на модемний пул банківського вузла, чи IP–протоколом через Internet. Крім того, мережова адреса банку загальноступна, а на модемний пул може звернутися лише обмежена кількість зареєстрованих користувачів. Відповідно відкритість банку, чия інформаційна мережа зв'язана з Internet, значно вища, ніж у першому випадку. Тільки за п'ять місяців 1995р. у комп'ютерну мережу CitiCorp зловмисно проникали 40 разів! (Це свідчить не стільки про якусь "небезпеку" Internet взагалі, скільки про некваліфіковану роботу адміністраторів безпеки CityCorp).

Огляд шляхів підвищення захисту. Таким чином виникає необхідність перегляду методів забезпечення інформаційної безпеки відкритих мережових систем. При під'єднанні до Internet потрібно знову проаналізувати ризик і скласти план захисту інформаційних ресурсів системи, а також конкретний план ліквідації наслідків, що виникають на випадок певних реалізацій порушень конфіденційності, зберігання і доступності інформації. Необхідний комплексний підхід до інформаційної безпеки. Її потрібно розглядати як складову частину загальної безпеки інформаційної системи, причому як важливу і невід'ємну її частину.

У цій концепції потрібно передбачувати не тільки заходи, пов'язані з інформаційними технологіями (криптозахист, програмні засоби адміністрування прав користувачів, їх ідентифікацію та аутентифікацію, "брандмауери" для захисту входів-виходів мережі назовні та ін.), але і заходи адміністративного та технічного характеру, а саме обмеження фізичного доступу до важливих об'єктів мережової системи, що відповідають за її захист і роботу. Потрібно дуже обережно ставитися до різних сертифікатів безпеки мережових продуктів, особливо вітчизняних, що не всі видаються об'єктивно, і віддавати перевагу тим продуктам, надійність яких підтверджена успішним використанням у світовій практиці.

Захист інформації в глобальній мережі Internet. Засоби захисту. Безсумнівно, що при під'єднанні до Internet піддається ризику безпека локальної мережі та конфіденційність інформації, що знаходиться у ній. За даними CERT Coordination Center, у 1995 році зареєстровано 2421 інцидент – зламів локальних мереж і серверів,

що на 48% більше, ніж у 1994 році. Втрати від них тільки в США становлять приблизно 66 млн. доларів.

Один з найпоширеніших механізмів захисту від інтернетівських зловмисників - "хакерів" - є використання міжмережових екранів – брандмауерів (firewalls). Потрібно наголосити, що внаслідок непрофесіоналізму адміністраторів і недоліків деяких типів брандмауерів приблизно 30% зламів здійснюється після встановлення систем захисту.

Технологія роботи у глобальних мережах системи захисту типу FireWall.

Проблема міжмережового екранування формулюється так. Нехай є дві інформаційні системи або дві множини інформаційних систем. Екран (FireWall) - це засіб розмежування доступу клієнтів з однієї множини систем до інформації, що зберігається на серверах у другій множині (рис.2).

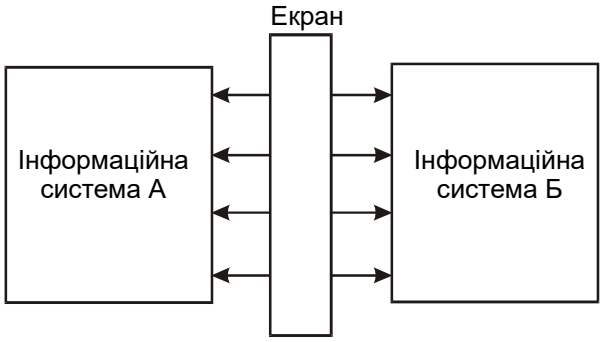

Рис.2 Екран FireWall.

На сьогодні питанням безпеки даних у розподілених комп'ютерних системах приділяють багато уваги. Вироблено безліч засобів для забезпечення інформаційної безпеки, призначених для використання на різних комп'ютерах з різними операційними системами. Один з напрямів - міжмережові екрани (FireWalls), що контролюють доступ до інформації з боку користувачів зовнішніх мереж.

Екран виконує свої функції шляхом контролю інформаційних потоків між двома множинами інформаційних систем, працюючи як "інформаційна мембрана". У цьому випадку екран є набором фільтрів, що аналізують інформацію, яка транспортується через них, і на основі закладених у нього алгоритмів, що приймають рішення - пропустити чи заборонити дану інформацію. Крім того, така система може реєструвати події, пов'язані з процесами розмежування доступу. Наприклад, фіксувати всі "незаконні" спроби доступу до інформації і додатково сигналізувати про ситуації, що потребують негайного втручання. Звичайно екранні системи роблять "несиметричними". Для екранів визначають поняття "всередині" і "ззовні", і завдання екрана полягає у захисті внутрішньої мережі від "потенційно ворожого" оточення. Найважливішим прикладом потенційно ворожої мережі є Internet.

Розгляньмо детальніше, які проблеми виникають при побудові екранних систем. При цьому розглядатимемо не тільки проблему безпечного під'єднання до Internet, але й розмежування доступу всередині екранованих систем. Вимоги до таких систем можна сформулювати у таких пунктах: забезпечення безпеки внутрішньої мережі (тієї, що захищається) та повний контроль зовнішніх під'єднань та сеансів зв'язку; наявність потужних і гнучких засобів управління для простого та повного впровадження в життя політики безпеки і, крім того, забезпечення простої реконфігурації системи при зміні структури мережі; можливість роботи непомітно для користувачів мережі, без створення перешкод у виконанні легальних дій; ефективно обробляти весь вхідний і вихідний трафік у "пікових" режимах (щоб FireWall неможливо було перевантажити, "затопити" великою кількістю запитів, що б призвело до порушення його роботи); надійний захист самої системи від будь-яких несанкціонованих дій, оскільки вона є головною у забезпеченні конфіденційності інформації в організації; в ідеалі, якщо в організації є декілька зовнішніх каналів під'єднань, у тому числі й у віддалених філіалах, система управління екранами повинна мати можливості централізованого керування ними для єдиної політики безпеки; система FireWall повинна мати засоби авторизації доступу користувачів через зовнішнє під'єднання. Типовою є ситуація, коли частина персоналу організації повинна виїжджати, наприклад, у відрядження, і в процесі роботи їм потрібний доступ, принаймі до деяких ресурсів внутрішньої мережі

організації. Система повинна надійно розпізнавати таких користувачів і забезпечувати їм доступ до необхідної інформації.

Типове налаштування FireWall. Адміністраторові безпеки мережі для конфігурування FireWall необхідно загалом виконати такі дії. Визначити об'єкти, що беруть участь у процесі обробки інформації - користувачів та групи користувачів, комп'ютери та їх групи, маршрутизатори і різні підмережі локальної мережі організації. Описати мережові протоколи та сервіси, з якими будуть працювати мережові задачі. Надалі з допомогою впроваджених понять описується політика розмежування доступу в таких термінах: "Групі користувачів А дозволити доступ до ресурсу Б з допомогою протоколу С, при цьому зробити позначку в журналі реєстрацій". FireWall може компілювати модулі фільтрації, що надалі виконуються на маршрутизаторах (Cisco IOS 9.x, 10.x, а також BayNetworks (Wellfleet) OS v.8.). Типова організація роботи FireWall зображена на рис.3.

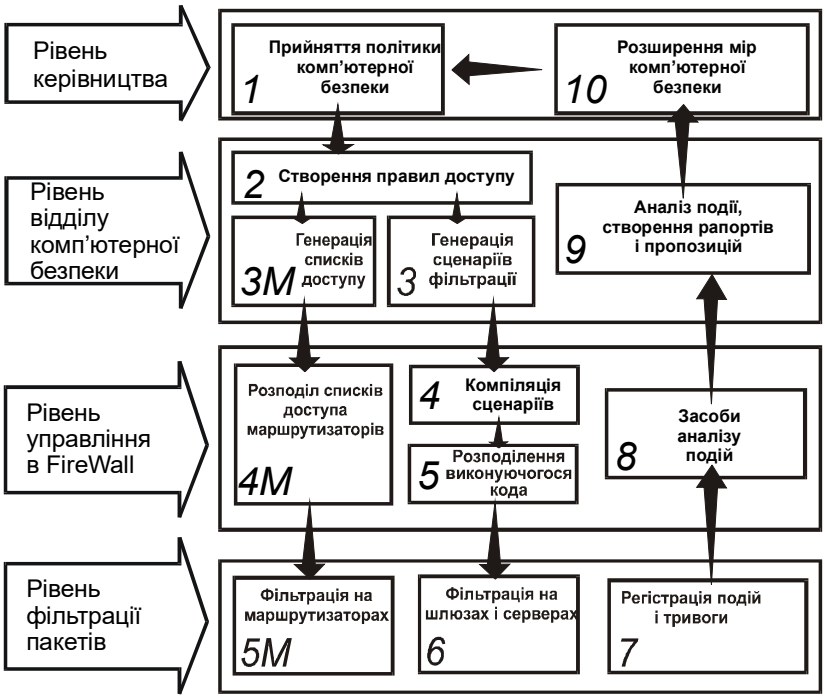

Рис. 3. Типова схема реалізації політики безпеки на базі FireWall

Як вже відзначалося, виробляють і затверджують на рівні керівництва організації правила політики безпеки. Для втілення у життя їх потрібно перевести в структуру типу: "звідки, куди і як доступ дозволено або, навпаки, заборонено". Далі на базі цих правил формуються списки доступу для маршрутизаторів і сценарії роботи фільтрів на мережових шлюзах. Списки та сценарії надалі переносять на фізичні компоненти мережі, після чого правила політики безпеки набувають чинності. У процесі роботи фільтри пакетів на шлюзах і серверах генерують записи про всі події, які їм призначено відстежувати, а також запускають механізми "тривоги", що вимагають від адміністратора негайного реагування.

На основі аналізу записів, зроблених системою, відділ комп'ютерної безпеки організації може виробляти пропозиції про зміну і дальший розвиток політики безпеки.

Фільтрація UDP – пакетів, динамічне екранування. UDP – протоколи, що належать до TCP/IP, є особливою проблемою для забезпечення безпеки. З одного боку, на їх основі створено безліч програм. З другого, всі вони є протоколами "без стану", що призводить до відсутності різниці між запитом і відповіддю, яка надходить із зовнішньої мережі. FireWall реалізовує цю проблему шляхом створення контексту з'єднань понад UDP сесій, запам'ятовуючи параметри запитів. Назад пропускаються тільки запити зовнішніх серверів на надіслані запити, що однозначно відрізняються від будь-яких інших UDP пакетів (незаконних запитів), оскільки їх параметри зберігаються в пам'яті FireWal.

Подібні механізми залучають також для задач, що використовують RPC, і для FTP сеансів. У даному випадку аналогічні проблеми, зв'язані з динамічним виділенням портів для сеансів зв'язку, які FireWall відстежує так само.

NAT (Network Adress Translation) – механізм доступу з локальної мережі в Internet. Нещодавно з'явився ще один досить ефективний спосіб зв'язку локальної мережі з Internet NAT (Network Adress Translation – Підміна мережевої адреси). Суть його полягає в тому, що на шлюзі, який з'єднує локальну мережу та Internet, сервіс NAT підмінює локальну адресу клієнта в IP пакеті на адресу шлюзу. Оскільки сервіс NAT, як і FireWall, зберігає контекст TCP, UDP сесій, то при поверненні пакета він повертає йому локальну адресу. Так повністю відокремлюється локальна мережа від Internet, оскільки локальні комп'ютери можуть мати локальні "нереальні" адреси типу "192.168.xxx.xxx". Зовні це виглядає так, ніби в Internet є тільки один комп'ютер – шлюз, тому що всі пакети мають його адресу. А локальні клієнти виходять в Internet без перешкод – для них все це прозоро. Ще про переваги NAT: достатньо мати лише одну реальну адресу в Internet, щоб мати нормальний доступ до нього. Це важливо, оскільки адресний простір в Internet обмежений – всього може бути приблизно два мільярди унікальних адрес, що не так багато при нинішніх темпах розвитку Internet. Фізичний доступ в Internet є тільки до одного комп'ютера, тільки він потребує хорошого захисту.

Обмеження доступу в WWW серверах. Є два основних види обмеження доступу:

- за IP адресами клієнтських машин;
- за ідентифікатором одержувача з паролем для даного виду документів.

Такі обмеження стали використовувати досить часто, оскільки багато хто намагається використати його комунікації для доставки своєї інформації споживачеві. З допомогою такого механізму для розмежування прав доступу зручне самопоширення інформації, на отримання якої існує договір. Доступ до приватних документів можна дозволити або заборонити, використовуючи конкретні адреси машин або мереж, наприклад: 194.123.56.56 або 195.23.98.168/255.255.255.248. У даному випадку доступ дозволений (або заборонений залежно від контексту) для машини 194.123.56.56 і для всіх машин підмережі 195.23.98.168/255.255.255.248.

Доступ до приватних документів можна дозволити або, навпаки, заборонити, використовуючи присвоєне ім'я і пароль конкретному користувачеві, причому явний пароль ніде не зберігається. Досі цей метод мав один суттєвий недолік. При введенні клієнтом паролю на локальній машині він явно передавався на WWW сервер, тому його можна було перехопити по дорозі. Зараз для передачі важливих даних використовується протокол з шифруванням даних SSL (Security Socket Layer), або HTTPS. У ньому всі дані передаються в зашифрованому вигляді, що значно підвищує конфіденційність інформації. Такий протокол створювали спеціально для передачі конфіденційних даних на відкритих каналах.

Ще можна з цією метою використовувати протокол PPTP (Point to Point Tunneling Protocol). Він створює шифрований канал точка – точка, і в ньому вже інкапсулюються "відкриті IP датаграми". Це хороший варіант для з'єднання віддаленого офісу організації з базовою установою через "відкритий" Internet. У них може нічого і не шифруватися, все може бути відкритим, але під час проходження каналу точка – точка всі дані шифруються. Його відмінність від SSL полягає в тому, що SLL - це один із звичайних протоколів TCP (441 порт), і тільки ті дані, що передаються з його використанням, шифруються. PPTP ж інкапсулює в собі весь стек протоколів TCP/IP. Він шифрує абсолютно всі дані, що передаються між двома комп'ютерами.

Вироблення мережової політики безпеки Internet. Політика безпеки визначається як сукупність документованих управлінських рішень, спрямованих на захист інформації та асоційованих з нею ресурсів. При її виробленні та втіленні доцільно керуватися такими принципами:

- неможливістю обминути захисні засоби;
- підсилення найслабшої ланки;
- неможливість переходу в небезпечний стан;
- мінімізування привілеїв клієнтів;
- розподіл обов'язків;

- ешелонування захисту;
- різноманітність захисних засобів;
- простота та керованість інформаційного середовища;
- забезпечення загальної підтримки заходів безпеки;

Розгляньмо це детальніше. Якщо зловмисник або незадоволений користувач має можливість обминути захисні засоби, він, напевне, так і вчинить. На прикладі міжмережових екранів даний принцип означає, що всі інформаційні потоки в мережу, що захищається, і з неї мають проходити через екран. Не повинно бути "таємних" модемних входів або тестових ліній, які обходять екран. Надійність захисту визначається найслабшою ланкою. Зловмисник не буде боротися з силою, він спробує знайти слабке місце. Дуже часто це не комп'ютер, а людина, яка володіє інформацією про безпеку мережі.

Принцип неможливості переходу в небезпечний стан означає, що при будь-яких обставинах, у тому числі й нештатних, захисний засіб або повністю виконує свої функції, або повністю блокує доступ для всіх.

Принцип мінімізації привілеїв рекомендує надавати користувачам і адміністраторам тільки ті права доступу, що необхідні їм для виконання своїх обов'язків.

Принцип розподілу обов'язків пропонує такий розподіл ролей і відповідальності, при якому одна людина не може порушити критично важливого для організації процесу. Це може захистити від зловмисних або некваліфікованих дій одного з системних адміністраторів.

Принцип ешелонованості захисту пропонує не покладатися повністю на одну лінію захисту, якою б надійною вона б не виглядала. За засобами фізичного захисту мають стояти програмно-технічні засоби, ідентифікація-аутентифікація управління доступом, і як остання лінія захисту – протоколювання та аудит, що суттєво ускладнює зловмисні дії.

Принцип різноманітності захисних засобів рекомендує організовувати різноманітні за своїм характером лінії захисту, щоб від потенційного зловмисника вимагалося знання різних, "не сумісних" між собою навиків (наприклад, різнотипні захисти на базі різних операційних систем).

Дуже важливий принцип простоти та керованості інформаційної системи в цілому і захисних засобів зокрема. Тільки для простого захисного засобу можна формально чи неформально довести його коректність. Лише в простій і керованій системі можна перевірити узгодженість конфігурації різних компонентів і виконувати централізоване адміністрування. Тут треба відзначити інтеграційну роль Web-сервісу, що приховує різноманітні об'єкти, які він обслуговує і який представляє єдиний, наочний інтерфейс. Відповідно, якщо об'єкти певного виду (таблиці, бази даних) доступні через Web, необхідно заблокувати прямий доступ до них, оскільки інакше випадку система стане складною для в керування.

Останній принцип – загальна підтримка заходів безпеки має нетехнічний характер. Потрібно забезпечити низку заходів, спрямованих на постійне теоретичне і практичне навчання з систем безпеки системних адміністраторів.

Аналіз ризиків – один з найважливіших етапів вироблення політики безпеки. При оцінці ризиків, що загрожують Intranet системам, слід враховувати такі обставини:
- нові загрози відносно старих сервісів, що грунтуються на можливості пасивного чи активного прослуховування мережі. Пасивне прослуховування означає читання мережового трафіка, а активне – його зміну (модифікацію даних, що передаються). Як правило, в Intranet системах потрібно дотримуватися принципу "все, що не дозволено, заборонено", оскільки "зайвий" мережовий сервіс може створити канал для проникнення в корпоративне середовище.

Висновки. Для побудови надійної захищеної мережі потрібно чітко визначити стратегію її захисту від зовнішніх і внутрішніх посягань на її ресурси. Захист повинен складатися не тільки з програмних засобів, таких, як міжмережові екрани FireWall, а й з

комплексу адміністративних заходів. Потрібно уникати створення в локальній мережі "зайвих" надлишкових сервісів, що можуть стати причиною несанкціонованого доступу до ресурсів мережі. Система, що відповідає за захист мережі, має бути максимально простою, оскільки чим простіша система, тим вона надійніша в керуванні і, як наслідок, забезпеченавід зовнішнього доступу.

The technical and program aspects of the information protection in the Internet are parsed. Is otined, as by diverse program, hardware and administrative resources it is possible to improve protection of the information and to improve reliability of local intelligence systems, which connect to the Internet.

Література

1. Браун С. "Мозаика" и "Всемирная паутина" для доступа к Internet / Пер. с англ. - М.: Мир: Малип: СК Пресс, 1996. - 167с.
2. Гайкович В., Першин А. Безопасность электронных банковских систем. - М.: Единая Европа, 1994. - 264 с.
3. Гилстер П. Новый навигатор Internet / Пер с англ. -Киев: Диалектика, 1996. - 495 с.
4. Игер Б. Работа в Internet / Под ред. А. Тихонова / Пер. с англ. - М.: БИНОМ, 1996. - 313 с.
5. Кент П. Internet / Пер. с англ. В.Л. Григорьева. - М.: Компьютер, ЮНИТИ, 1996. - 267 с.
6. Колесников О.Э. Интернет для делового человека. - М.: МЦФ. Издат. фирма "Яуза", 1996. - 281 с.
7. Крол Эд. Все об Internet: Руководство и каталог / Пер. с англ. С.М. Тимачева. - Киев: BNV, 1995. - 591 с.
8. Левин В.К. Защита информации в информационно-вычислительных системах и сетях // Программирование. - 1994. - N5. - С. 5-16.
9. Нольден М. Ваш первый выход в Internet: Для начинающих пользователей Internet и широкого круга пользователей PC / Гл. ред. Е.В. Кондукова / Пер с нем. К.А. Шиндер. - Спб.: ИКС, 1996. - 238 с.
10. Продукты года // LAN - русское издание. - 1995. - Том 1. - № 1. - С. 6-25.
11. Об информации, информатизации и защите информации: Федеральный Закон // Российская газета. - 1995. - 22 февраля. - С. 4.
12. Фролов А.В., Фролов Г.В. Глобальные сети компьютеров: Практическое введение в Internet, E-mail, FTP, WWW, и HTML, программирование для Windiws Sockets. - М. - МИФИ, 1996. - 283 с.
13. Хоникат Д. Internet Windows 95: Руководство пользователя / Пер. с англ. В. Неклюдова. - М.: БИНОМ, 1996. - 334 с.
14. Cheswick W.R., Bellovin S.M. Firewalls and Internet Security: Repelling the Wily Hacker. - Addison-Wesley, 1994. - 275 с.
15. An Introduction to Computer Security: The NIST Handbook. Draft. - National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 1994. - 310 с.

Одержано 14.01.2000 р.