УДК 331

В. М. ФРАНКО
Хмельницький національний університет

ПРОБЛЕМИ БЕЗПЕКИ СУЧАСНИХ КОРПОРАТИВНИХ МЕРЕЖ

В статті представлені науково-технічні принципи побудови систем забезпечення безпеки інформаційних ресурсів корпоративних мереж з урахуванням сучасних тенденцій розвитку мережених інформаційних технологій. Розглянуті сучасні технології, що використовуються для побудови захищених корпоративних мереж, досліджені методи захисту від внутрішніх порушників.

The article presents the scientific and technical principles of systems safety information resources for corporate networks with current trends in information technology network. The modern technologies used to build a secure corporate networks, studied the methods of protection against internal offenders.

Нові інформаційні технології активно впроваджуються у всі сфери народного господарства. Поява локальних і глобальних мереж передачі даних надала користувачам комп'ютерів нові можливості оперативного обміну інформацією. Якщо до недавнього часу подібні мережі створювалися тільки у специфічних і вузьконаправлених цілях (академічні мережі, мережі військових відомств і так далі), то розвиток Інтернету і аналогічних систем призвів до використання глобальних мереж передачі даних у повсякденному житті практично кожної людини.

Проведення практичних робіт з інспектування, аналізу вразливостей, сертифікаці та атестації за вимогами безпеки великої кількості корпоративних мереж та автоматизованих систем, комунікаційних провайдерів (операторів зв'язку) низки головних управлінь центрального банку України, комерційних банків, Державних структур і комерційних підприємств.започаткувало основну мету концепції – визначення методів і засобів захисту і забезпечення безпеки інформації, що відповідають інтересам, вимогам та законодавству України в сучасних умовах необхідності використання ресурсів глобальних мереж передачі даних загального користування для побудови корпоративних захищених і безпечних мереж. Концепція формулює науково-технічні принципи побудови систем забезпечення безпеки інформаційних ресурсів корпоративних мереж з урахуванням сучасних тенденцій розвитку мережевих інформаційних технологій, розвитку видів мережевих протоколів, їх взаємної інкапсуляції і спільного використання.

Особливості організації корпоративних комп'ютерних мереж визначають необхідність пошуку нових рішень як на структурному рівні, так і при організації доставки повідомлень абонентам мережі та забезпеченні їх безпеки.

Побудова сучасних систем забезпечення безпеки інформаційних корпоративних мереж ґрунтується на комплексному підході, що довів свою ефективність і надійність. Комплексний підхід орієнтований на створення захищеного середовища обробки інформації в корпоративних системах. Сюди відносяться правові, морально-етичні організаційні програмні і технічні способи забезпечення інформаційної безпеки. Проте тільки математичне моделювання корпоративної мережі дозволяє забезпечити ефективність і гарантованість функціонування систем захисту. Тільки тоді, на основі математичного моделювання, можна буде побудувати обґрунтовану з гарантіями по безпеці концепцію інформаційної безпеки корпорації. Актуальність також у тому, що моделі ефективності і надійності функціонування корпоративних мереж розроблені порівняно давно і детально вивчені, а адекватні моделі безпеки поки тільки розробляються.

Актуальність і важливість проблеми забезпечення інформаційної безпеки обумовлені наступними чинниками:

1. Сучасні рівні і темпи розвитку засобів інформаційної безпеки значно відстають від рівнів і темпів розвитку інформаційних технологій.
2. Високі темпи зростання парка персональних комп'ютерів, вживаних в різноманітних сферах людської діяльності. (Згідно даним досліджень компанії Gartner Dataquest в теперішній час у світі більше мільярда персональних комп'ютерів. А наступний мільярд буде досягнутий вже в 2009 році.)
3. Різке розширення кола користувачів, що мають безпосередній доступ до обчислювальних ресурсів і масивів даних.

Доступність засобів обчислювальної техніки, і, перш за все, персональних ЕОМ, призвела до розповсюдження комп'ютерної обізнаності в широких верствах населення. Це, у свою чергу викликало численні спроби втручання у роботу державних і комерційних систем як зі злим наміром, так і з чисто «спортивного інтересу». Багато з цих спроб мали успіх і нанесли значних збитків власникам інформації і обчислювальних систем. За оцінками фахівців у сьогодення біля 80 – 95% інтелектуального капіталу компаній зберігається в цифровому вигляді – текстові файли, таблиці, бази даних.

Стрімкий розвиток інформаційних технологій відкрив нові можливості для бізнесу, що призвело до появи нових загроз. Сучасні програмні продукти із-за конкуренції потрапляють в продаж з помилками і недоробками.

Розробники, включаючи в свої вироби всілякі функції, не встигають виконати якісну відладку створюваних програмних систем. Помилки і недоробки, що залишилися в цих системах, призводять до

випадкових і навмисних порушень інформаційної безпеки. Наприклад, причинами більшості випадкових втрат інформації є відмови в роботі програмно-апаратних засобів, а більшість атак на комп'ютерні системи засновані на знайдених помилках і недоробках у програмному забезпеченні. Так, наприклад, за перших 6 місяців після випуску серверної операційної системи компанії Microsoft Windows Server 2003 було виявлено 14 вразливостей, 6 з яких є критично важливими.

Не дивлячись на те, що з часом Microsoft розробляє пакети оновлення, що знімають виявлені недоробки, користувачі вже встигають постраждати від порушень інформаційної безпеки, що трапилися по причині тих, що допустили помилки. Така ж ситуація має місце і з програмними продуктами інших фірм. Поки не будуть вирішені ці проблеми недостатній рівень інформаційної безпеки буде серйозним гальмом у розвитку інформаційних технологій.

Бурхливий розвиток глобальної мережі Інтернет практично не перешкоджає порушенням безпеки систем обробки інформації у всьому світі. Подібна глобалізація дозволяє зловмисникам практично з будь-якої точки земної кулі, де є Інтернет, здійснювати напад на корпоративну мережу.

Сучасні методи накопичення, обробки і передачі інформації сприяли появі загроз, пов'язаних з можливістю втрати, спотворення і розкриття адресованих даних, або таких, що належать кінцевим користувачам.

Наприклад, в даний час в банківській сфері понад 90% всіх злочинів зв'язано з використанням автоматизованих систем обробки інформації.

Під загрозою безпеці розуміється можлива небезпека (потенційна або така, що реально існує) здійснення якого-небудь діяння (дії або бездіяльності), направленого проти об'єкту захисту (інформаційних ресурсів), що завдає збитку власникові або користувачеві, спотворення, що виявляється в небезпеці, розкриття або втрати інформації. Реалізацію загрози надалі називатимемо атакою.

Реалізація тієї або іншої загрози безпеці може переслідувати наступні цілі:

1. Порушення конфіденційності інформації. Інформація, що зберігається і оброблювана в корпоративній мережі, може мати велику цінність для її власника, її використання іншими особами наносить значний збиток інтересам власника.
2. Порушення цілісності інформації. Втрата цілісності інформації (повна або часткова компрометація, дезинформація) – загроза близька до її розкриття. Цінна інформація може бути втрачена або знецінена шляхом її несанкціонованого видалення або модифікації. Збиток від таких дій може бути багато більшим, ніж при порушенні конфіденційності.
3. Порушення (часткове або повне) працездатності корпоративної мережі (порушення доступності). Вивід з ладу або некоректна зміна режимів роботи компонентів КС, їх модифікація або підміна можуть привести до отримання невірних результатів, відмови КС від потоку інформації або відмова при обслуговуванні.

Тому забезпечення інформаційної безпеки комп'ютерних систем і мереж є одним з ведучих напрямів розвитку інформаційних технологій.

Забезпечення безпеки КС припускає організацію протидії будь-якому несанкціонованому вторгненню в процес функціонування КС, а також спробам модифікації, розкрадання, виводу з ладу або руйнування її компонентів, тобто захист всіх компонентів КС – апаратних засобів, програмного забезпечення, даних і персоналу.

Комплексний підхід ґрунтується на рішенні комплексу приватних завдань за єдиною програмою. Цей підхід в даний час є основним для створення захищеного середовища обробки інформації в корпоративних системах, що зводить воєдино різнорідні заходи протидії погрозам. Сюди відносяться правові, морально-етичні організаційні програмні і технічні способи забезпечення інформаційної безпеки. Комплексний підхід дозволив об'єднати цілий ряд автономних систем шляхом їх інтеграції в так звані інтегровані системи безпеки.

Методи рішення завдань забезпечення безпеки дуже тісно пов'язані з рівнем розвитку науки і техніки і, особливо, з рівнем технологічного забезпечення. А характерною тенденцією розвитку сучасних технологій є процес тотальної інтеграції. Цією тенденцією охоплені мікроелектроніка і техніка зв'язку, сигнали і канали системи і мережі. У якості прикладів можна привести надвеликі інтегральні схеми, інтегральні мережі передачі даних, багатофункціональні пристрої зв'язку і тому подібне.

Подальшим розвитком комплексного підходу або його максимальною формою є інтегральний підхід, заснований на інтеграції різних підсистем забезпечення безпеки, підсистем зв'язку у єдину інтегральну систему з загальними технічними засобами, зв'язки з програмним забезпеченням і базами даних. Інтегральний підхід направлений на досягнення інтегральної безпеки. Основний сенс поняття інтегральної безпеки полягає у необхідності забезпечити такий стан умов функціонування корпорації, при якому вона надійно захищена від всіх можливих видів погроз у ході всього безперервного виробничого процесу. Поняття інтегральної безпеки припускає обов'язкову безперервність процесу забезпечення безпеки як у часі, так і в просторі з обов'язковим обліком всіх можливих видів загроз (несанкціонований доступ знімання інформації, тероризм, пожежа, стихійні лиха і т. д.).

У якій би формі не застосовувався комплексний або інтегральний підхід, він завжди направлений на вирішення ряду приватних завдань в їх тісному взаємозв'язку з використанням загальних технічних засобів, каналів зв'язку, програмного забезпечення і т. д. Наприклад, стосовно інформаційної безпеки найбільш очевидними з них є завдання обмеження доступу до інформації технічного і криптографічного закриття

інформації, обмеження рівнів паразитних випромінювань технічних засобів, охорона від тривожної сигналізації. Проте необхідне рішення й інших, не менш важливих проблем, як-от, наприклад, стихійні лиха, аварії, тероризм і тому подібне. Тому об'єктивно забезпечити повну безпеку інформації можуть лише інтегральні системи безпеки, що індиферентні до виду загроз безпеці і забезпечують необхідний захист безперервно як в часі, так і в просторі, в ході всього процесу підготовки, обробки, передачі і зберігання інформації.

Розглянемо комплексний підхід для забезпечення інформаційної безпеки. До основних способів забезпечення інформаційної безпеки відносять:

1) законодавчі (правові);
2) морально-етичні;
3) організаційні (адміністративні);
4) технічні;
5) програмні.

Законодавчі заходи захисту визначаються законодавчими актами країни, якими регламентуються правила використання, обробки і передачі інформації обмеженого доступу і встановлюються заходи відповідальності за порушення цих правил.

Дійсно, більшість людей не здійснюють протиправних дій зовсім не тому, що це технічно складно, а тому, що це засуджується і/або карається суспільством, а також тому, що так поступати не прийнято.

Загалом сюди відносяться:

1) конституція;
2) доктрина інформаційної безпеки;
3) кодекси;
4) закони;
5) укази Президента;
6) ухвали Уряду;
7) державні стандарти в області захисту інформації;
8) ГОСТи;
9) керівні документи.

Організаційні (адміністративні) засоби захисту – це організаційно-технічні і організаційно-правові заходи здійснювані, у процесі створення і експлуатації апаратури телекомунікацій для забезпечення захисту інформації. Організаційні заходи охоплюють всі структурні елементи апаратури на всіх етапах їх життєвого циклу (будівництво приміщень, проектування системи, монтаж і наладка устаткування, випробування і експлуатація).

Організаційні заходи передбачають:

1) Обмеження доступу в приміщення де відбувається обробка конфіденційної інформації.
2) Допуск до рішення завдань на комп'ютері з обробки секретної, конфіденційної інформації перевірених посадових осіб, визначення порядку проведення робіт на комп'ютері.
3) Зберігання магнітних носіїв в ретельно закритих міцних шафах.
4) Призначення одного або декількох комп'ютерів для обробки цінної інформації і подальша робота тільки на цих комп'ютерах.
5) Установка дисплея, клавіатури і принтера так, щоб виключити перегляд сторонніми особами змісту оброблюваної інформації.
6) Постійне спостереження за роботою принтера та інших пристроїв виводу на носії цінної інформації.
7) Знищення фарбувальних стрічок або інших матеріалів, що містять фрагменти цінної інформації.
8) Заборона ведення переговорів про безпосередній зміст конфіденційної інформації особами, зайнятими її обробкою.

Організаційно-технічні заходи припускають:

1) Обмеження доступу всередину корпуса комп'ютера шляхом встановлення механічних пристроїв замикання.
2) Знищення всієї інформації на вінчестері комп'ютера при відправці в ремонт з використанням засобів низькорівневого форматування.
3) Організацію живлення комп'ютера від окремого джерела живлення або від загальної (міської) електромережі через стабілізатор напруги (мережевий фільтр) або мотор-генератор.
4) Використання для відображення інформації рідкокристалічних або плазмових дисплеїв, а для друку - струменевих або лазерних принтерів.
5) Розміщення дисплея, системного блоку, клавіатури і принтера на відстані не менше 2,5 – 3,0 метрів від пристроїв освітлення, кондиціонування повітря, зв'язку (телефону), металевих труб телевізійної і радіоапаратури, а також інших комп'ютерів, що не використовуються для обробки конфіденційної інформації.
6) Відключення комп'ютера від локальної мережі або мережі видаленого доступу при обробці на ньому конфіденційної інформації, окрім випадку передачі цієї інформації по мережі.
7) Установка принтера і клавіатури на м'яких прокладках з метою зниження просочування інформації по акустичному каналу.

8) У час обробки цінної інформації на комп'ютері рекомендується виключати пристрої, що створюють додатковий шумовий фон (кондиціонери вентилятори), а також обробляти іншу інформацію на комп'ютерах, що стоять поряд. Ці пристрої повинні бути розташовані на відстані не менше 2,5 – 3,0 метрів.

9) Знищення інформації безпосередньо після її використання.

Технічні засоби реалізуються у вигляді механічних, електричних, електромеханічних і електронних пристроїв, призначених для перешкоди на можливих шляхах проникнення і доступу потенційного порушника до компонентів захисту.

Програмні засоби представляють з себе програмне забезпечення, спеціально призначене для виконання функцій захисту інформації.

Програмні засоби складали основу механізмів захисту на першій фазі розвитку технології забезпечення безпеки зв'язку в каналах телекомунікацій. При цьому вважалося, що основними засобами захисту є програмні. Спочатку програмні механізми захисту включалися, як правило, до складу операційних систем ЕОМ, або систем управління базами даних. Практика показала, що надійність подібних механізмів захисту є явно недостатньою. Особливо слабкою ланкою виявився захист через пароль. Тому надалі механізми захисту ставали все більш складними, із залученням інших засобів забезпечення безпеки.

До данного класу засобів захисту відносяться антивірусні, криптографічні засоби системи розмежування доступу, міжмережеві екрани, системи виявлення вторгнень і тому подібне.

Згідно з результатами дослідження компанії «Ibas», проведеного у січні 2004 року, 70% співробітників крадуть конфіденційну інформацію з робочих місць**.** Більше всього з роботи беруть такі речі, як книги електронних адрес бази даних клієнтів, а також комерційні пропозиції і презентації. І більше того, 72% опитаних не страждають етичними проблемами, вважаючи, що мають законні права на нематеріальне майно компанії. З іншого боку, згідно з існуючою статистикою, в колективах людей, зайнятих тією або іншою діяльністю, як правило, тільки близько 85% є цілком лояльними (чесними), а останні 15% діляться приблизно так: 5% можуть зробити що-небудь протиправне, якщо по їх уявленнях, вірогідність заслуженого покарання мала; 5% готові ризикнути на протиправні дії, навіть якщо шанси бути викритим і покараним складають 50% на 50%; 5% готові піти на протизаконний вчинок, навіть якщо вони майже упевнені в тому, що будуть викриті і покарані. Така статистика в тій чи іншій мірі може бути застосовна до колективів, що беруть участь в розробці і експлуатації інформаційно-технічних комп'ютерних систем. Таким чином, можна припустити, що не менш 5% персоналу, який бере участь у розробці і експлуатації програмних комплексів, здатні здійснити дії кримінальної характеру з корисливих спонукань або під впливом яких-небудь інших обставин. Отже, висвітлена у роботі проблема цілком актуальна. І лише останнім часом компанії, що спеціалізуються на розробці засобів захисту, усвідомили необхідність в розробці засобів захисту від внутрішніх порушників. Одну з перших систем подібного напряму випустила вітчизняна компанія «Праймтек» у кінці 2005 року. Система призначена для контролю політики безпеки організації.

Важливим є той факт, що для скоєння високотехнологічного злочину зловмисникові необов'язково бути фахівцем з інформаційних технологій. Це означає, що практично будь-який співробітник організації потенційно в змозі нанести серйозний збиток компанії з використанням програмних засобів. Конкретні приклади ілюструють, що в мережі Інтернет можна знайти величезне число повчальних матеріалів і готових програмних продуктів для реалізації несанкціонованого доступу до комп'ютерів у локальних обчислювальних мережах. Багато статей написано доступною мовою і забезпечено докладними інструкціями по реалізації атак. Проте проблема, звичайно, не у наявності таких матеріалів, а у слабкості сучасних технологій захисту мереж.

Список використаних джерел

1. Биячуев Т. А. Безопасность корпоративных сетей / [под ред. Л. Г. Осовецкого]. – СПб. : СПб ГУ ИТМО, 2004. – 161 с.