УДК 621.391.

**Гордієнко С.Б.**

# СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

З огляду на інтенсивність розвитку інформаційних технології, в статті проведено аналіз сучасних проблем інформаційної безпеки. Досліджено взаємомозв'язок між рівнем інформаційної безпеки та реалізацією системи захисту інформації і інформаційних ресурсів, здійсненням організаційно-технологічних заходів по захисту інформаційних систем на об'єктах інформаційної діяльності.

***Ключові слова:*** інформаційні системи, інформаційної безпека, системи захисту інформації, цілісність інформації, сервер баз даних, зловмисник, програмний рівень захисту.

На сьогодні інформацію розглядають як один з основних ресурсів розвитку суспільства, а інформаційні системи і технології як засіб підвищення продуктивності і ефективності роботи людей. Тому інформація є цінним і дорогим ресурсом. Інформаційна технологія визначає процеси передачі і поширення, зберігання і обробки інформації, а так само її використання в певній меті. Ясно, що ці процеси мають бути швидкими, найменш витратними, максимально корисними, зручними і автоматизованими. З цієї причини основною тенденцією розвитку інформаційних технологій є їх представлення в цифровому виді, перехід до цифрових телекомунікаційних інформаційних баз, які базуються на цифровій розподіленій взаємодії комп'ютерів, розроблених по найрізноманітніших функціональних алгоритмах. Впровадження персональних комп'ютерів в інформаційну сферу і застосування телекомунікаційних засобів зв'язку визначили новий етап розвитку інформаційної технології.

Комп'ютерні телекомунікації - тип інформаційних технологій, що інтенсивно розвивається, що використовують глобальні комп'ютерні мережі, зокрема Інтернет. Інтернет і інформаційна безпека несумісні по самій природі мережі Інтернет. Ця мережа об'єднує разом з мережами з обмеженим доступом (комерційних, освітніх, державних, військових і інших організацій) і рядових користувачів, які мають можливість отримати прямий доступ в Інтернет зі своїх домашніх комп'ютерів, використовуючи модем і телефонну мережу загального користування. Первинна простота доступу в Інтернет погрожує безпеці локальної мережі і конфіденційності інформації, що міститься в ній. За допомогою програмних портів, через які і здійснюється взаємодія комп'ютера з Інтернет, що будь-який, що бажає теоретично може проникнути в саме серце комп'ютера і отримати над ним повний контроль. За результатами опитування, проведеного Computer Security Institute(CSI) серед 500 найбільш великих організацій, компаній і університетів з 1991 року число незаконних вторгнень зросло на 48,9%, а втрати, викликані цими атаками оцінюються в 66 млн. доларів США. Можливість доступу до комерційних архівних даних організації може їй дуже дорого коштувати, тому, підключаючись до мережі Інтернет, слід провести аналіз ризику і скласти план захисту інформаційної системи. Для відвертання несанкціонованого доступу до даних доцільно ставити фільтри (firewall) між внутрішньою мережею і Інтернет. Серед програм, що відносяться до класу міжмережевих екранів, популярністю користуються такі як ZoneAlarm, Outpost, KasherskyAntiHacker і інші. Таким чином, потрібний комплексний підхід до інформаційної безпеки організацій. Інформаційна безпека повинна розглядатися як складова частина загальної безпеки організації, причому як важлива і невід'ємна її частина. Необхідно розробити концепцію інформаційної безпеки, в якій слід передбачити не лише заходи, пов'язані з інформаційними технологіями (криптозахист, програмні засоби адміністрування прав користувачів, їх ідентифікації і аутентифікації, брандмауери для захисту входів-виходів мережі і т. п.), але і заходи адміністративного і технічного характеру.

Темпи зростання українського сегменту Internet в останні роки не поступаються і навіть перевершують середньоєвропейські. В той же час використовувані "засоби захисту інформації" не задовольняють сьогоднішнім потребам в першу чергу з чисто організаційно-технологічних причин. Визначальним чинником інтеграції в єдиний інформаційний простір

різних інформаційних систем і ресурсів є забезпечення належного рівня інформаційної безпеки, яка включає наступний комплекс заходів і технічних рішень по захисту інформації:

- від порушення функціонування мережі шляхом дії на інформаційні канали, канали сигналізації, управління і видалене завантаження баз даних, комунікаційне устаткування, системне і прикладне програмне забезпечення;
- від несанкціонованого доступу до інформації шляхом виявлення і ліквідації спроб використання ресурсів мережі, що призводять до порушення цілісності мережі і інформації, зміни функціонування підсистем розподіли інформації;
- від руйнування вбудовуваних засобів захисту з можливістю доказу не правомірності дій користувачів і обслуговуючого персоналу мережі;
- від впровадження програмних "вірусів" і "закладок" в програмні продукти і технічні засоби.

Побудова системи безпеки комп'ютерної мережі має своїй на меті відвертання або зниження можливого збитку, який може бути нанесений в результаті атаки на мережу. Цінні файли або інформація можуть бути знищені, сервери або інше устаткування можуть бути приведені в неробочий стан так, що на їх повне відновлення може знадобитися декілька днів. Крім того, захист мережі має на меті захист репутації організації від збитку внаслідок, наприклад, несанкціонованої зміни вмісту сторінок її WWW- сервера третіми особами, публікації інформації третіми особами під чужим авторством або поява в публічному доступі інформації, небажаної для широкого поширення (чи секретною). Інформаційна безпека в глобальній мережі має свою специфіку, що відрізняє її від проблеми інформаційної безпеки в локальних мережах. Найважливішою відмітною особливістю завдання захисту інформації в глобальній мережі є той факт, що захист інформації покладається повністю на програмно-апаратні засоби, і не може бути вирішена шляхом фізичного обмеження доступу користувачів до комп'ютерів або до устаткування, як це може бути зроблено для обмеження доступу до інформації у рамках окремої організації. У глобальній мережі потенційну можливість доступу до ресурсів має будь-який користувач мережі, що знаходиться у будь-якій точці Земної кулі, і момент доступу до тієї або іншої інформації не може бути передбачений заздалегідь. Іншою особливістю проблеми є величезна швидкість розвитку в Internet програмного забезпечення і технологій. Нові технології подолання систем захисту інформації з'являються кожні півроку, і їх арсенал може мінятися кожні 2-3 місяці. Internet з гнітючою періодичністю приголомшують скандали, суть яких полягає в розкраданні або псуванні інформації.

Стосовно Internet, то він не був би самим собою, якби в його надрах не народилося рішення, що відповідає проблемам, що виставляються життям. Причому, технічні ідеї пропонованих рішень мають спільність, що дозволяє говорити про те, що Internet після їх впровадження по мірі безпеки може перевершити навіть спеціалізовані закриті корпоративні мережі. Інформаційна безпека Internet визначається особливостями базових платформ - комунікаційною (TCP/IP) і операційною (UNIX). TCP/IP має високу сумісність як з різними по фізичній природі і швидкісним характеристикам каналами, так і з широким колом апаратних платформ. Крім того, цей протокол в рівній мірі ефективно працює як в локальних мережах, так і в регіональних і глобальних мережах. Сукупність цих характеристик робить Internet-технології унікальним засобом для створення і інтеграції великих розподілених гетерогенних інформаційних систем. У Internet інформаційних системах в порівнянні з класичними системами архітектури "клієнт-сервер" питання інформаційної безпеки вирішуються набагато простіше. Це пов'язано передусім з наступними особливостями:

- набагато більша частина інформаційних ресурсів централізована - їх надає сервер, а централізованими ресурсами не лише легше управляти, але їх і легше захищати;
- для обміну інформацією між робочими станціями і сервером використовується протокол TCP/IP, для якого розроблена система захисних засобів, включаючи криптографічні;

- на робочих станціях виконується тільки WWW переглядач і програми інтерпретації Web- документів сервера, які завантажуються безпосередньо з сервера.

Вирішення проблеми інформаційної безпеки полягає у використанні організаційно-технологічних (адміністративних), технічних і програмних заходів, а так само в профілактичній роботі серед користувачів для зменшення можливостей несанкціонованого доступу до інформації. Вцілому інформаційна безпека будується на:

- конверсії технологій інформаційної безпеки і захисту інформації, інформаційних систем та телекомунікаційного середовища від несанкціонованого використання і дій;
- забезпеченні захисту ресурсів за рахунок паралельного доступу до баз даних і перевірки повноважень при зверненні до ресурсів мережі;
- реконфігурації мереж, вузлів і каналів зв'язку;
- організації замкнутих підмереж і адресних груп;
- розвитку спеціалізованих захищених комп'ютерів, локальних обчислювальних мереж і корпоративних мережних сегментів (що особливо важливе для розробників інформаційних систем);
- забезпеченні захисту технічних засобів і приміщень від просочування інформації по побічних каналах і від можливого впровадження в них електронних облаштувань знімання інформації;
- розвитку і використанні технологій підтвердження достовірності об'єктів даних, користувачів і джерел повідомлень;
- використанні протоколів шифрування IP пакетів, систем шифрування облікових даних і прав доступу до інформації, передача інформації з використанням секретних ключів;
- застосуванні технологій виявлення цілісності об'єктів даних.

Таким чином, реалізація системи захисту інформації і інформаційних ресурсів розпадається на три незалежні завдання:

1. Забезпечення системи цілісності інформації і інформаційних систем.
2. Організація авторизованого доступу до інформації.
3. Неприпустимість появи у відкритому доступі інформації, що становить державну таємницю, або, що має конфіденційний характер.

Розглянемо детальніше підходи до рішення перших двох завдань. У даної проблеми відсутні готові рецепти рішень. У кожному конкретному випадку, розглядаючи той або інший мережний ресурс, слід приймати рішення виходячи із співвідношення ризику і можливого збитку, від атаки при використанням цього ресурсу, з потреби в цьому ресурсі, а також витрат на освоєння і підтримку того або іншого рішення. Будь-яка інформаційна система, побудована на основі клієнт-серверних Інтернет технологій з обліком системи безпеки, повинна містити наступні серверні компоненти:

- шлюз-сервер, що управляє правами доступу до інформаційної системи;
- WWW- сервер;
- сервер баз даних;
- сервер додатків і (чи) сервер обробки транзакцій.

При цьому серед організаційно-технологічних заходів по захисту інформаційних систем можна виділити три основних:

- організація системи захисту на рівні IP пакетів (технологічний рівень Модель OSI);
- адміністративний рівень захисту - контекстна перевірка і перегляд пакетів з метою ухвалення рішення;
- програмний рівень захисту (шлюз виступає проміжною ланкою між Інформаційною системою і клієнтом).

У разі розміщення інформаційної системи на різних машинах, що знаходяться в різних локальних мережах (розподіленої інформаційної системи), необхідно будувати довірчі бази з обов'язковим застосуванням шлюзів для забезпечення прав доступу.

Організація доступу до інформаційних ресурсів через машину-«посередник» є найнадійнішим і найпростішим способом вирішення проблеми цілісності даних, що

зберігається в інформаційній системі. У цій ситуації сама інформаційна система, знаходиться на машині недоступною з глобальної мережі і відповідає тільки на запити з локальної мережі організації, і не може бути схильна до зовнішніх атак. Машина-«посередник» не обробляє зовнішні запити, а отримуючи запит після перевірки його правильності звертається до необхідного ресурсу і відправляє відповідь користувачеві. У цій ситуації зловмисник може зламати тільки машину-шлюз, відновлення якої не займе багато часу.

Належний стан інформаційної безпеки неможливий без чіткого адміністративного керівництва мережею, та управління інформаційною безпекою. Він включає в себе створення умов і забезпечення взаємодії усіх служб мережі, центру управління мережею і адміністраторів підмереж для досягнення високої швидкості реагування на спроби несанкціонованого доступу, швидкого сповіщення усіх зацікавлених сторін про нові технології і методи подолання систем захисту і обміну досвідом.

## ЛІТЕРАТУРА

1. Федотов А.М. Новые информационные технологии. //Материалы научно-практической конференции "Проблемы информатизации региона" / Федотов А.М. - Красноярск. 1993. С. 32-48.

2. Замкова Т.В. Проблемы защиты информации в совремкнных информационных системах / Замкова Т.В. // Современные наукоемкие технологии. – 2005. – № 3 – С. 58-59.

Надійшла: 02.09.2012р.

Рецензент: д.т.н., проф. Щербак Л.М.