Принципи захисту ком'ютерної інформації від неправомірного втручання

Греков І. П., Логвин Ю.С.
Сумський державний університет, юридичний факультет;
к.ю.н., ст. викладач кафедри АГП ФЕБ;студентка гр. Ю-74
e-mail: kafedrapravasumdu@ukr.net

The author examines the issue of information security in computer systems, types of threats to computer systems, exploring ways of malicious harmful impact on computer systems and technology management information security.

ВСТУП

Питання захисту інформації в комп'ютерних системах (КС) не втрачають своєї актуальності вже понад 30 років. Це пояснюється тим, що інформація, яка знаходиться в тому чи іншому комп'ютері, є достатньо вразливою для неправомірного втручання. З відносно недавнього часу законодавством України передбачена кримінальна відповідальність за вчинення комп'ютерного злочину у такий спосіб (ст. 361 Кримінального кодексу України), але в ній застосовується термін «несанкціоноване втручання».

ОСНОВНИЙ ТЕКСТ

У розуміння розглядуваного способу вчинення злочину певні труднощі вносить, по-перше, визначення поняття «втручання», а по-друге, окреслення в рамках цього поняття дій, які є неправомірними. У коментарі до ст. 361 КК України під цим поняттям маються на увазі будь-які дії винного, що впливають на обробку електронно-обчислювальних машин (ЕОМ) інформації, яка в ній зберігається або яка передається за допомогою комп'ютерних мереж. Для того щоб уточнити перелік таких дій, звернемося до теорії захисту інформації [1].

У теорії захисту інформації як «загрозу комп'ютерній системі» розуміють реально або потенційно можливі дії чи умови навмисного або випадкового (ненавмисного) порушення режиму функціонування комп'ютерної системи. Наслідком загрози можуть бути небажані впливи на інформацію. Відповідно до КК України шкідливими впливами на комп'ютерну інформацію є витік, втрата, підробка, блокування, спотворення процесу її обробки або порушення встановленого порядку її маршрутизації (ст. 361 КК України). Загрози комп'ютерній системі залежать від її структури і конфігурації, технології обробки інформації, стану навколишнього фізичного середовища, дій персоналу і структури комп'ютерної інформації, що оброблюється в ній.

Виходячи з теорії захисту інформації, до основних типів реалізації загроз комп'ютерним системам належать:

а) стихійні лиха;
б) зловмисні дії;
в) побічні явища;
г) відмови і збої, помилки елементів системи.

Необхідно звернути увагу на зловмисні дії. За способами реалізації зловмисний шкідливий вплив на комп'ютерну систему може здійснюватися:

1. По технічних каналах, включаючи канали побічних електромагнітних випромінювань і наведень, акустичні, оптичні, радіо-, радіотехнічні та інші канали проникнення інформації.
2. По каналах спеціальної дії за рахунок формування спеціальних полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації.

3. Несанкціонованим доступом (НСД) у результаті підключення до апаратури і ліній зв'язку, маскування під зареєстрованих (законних) користувачів, подолання заходів захисту для отримання (використання) інформації або нав'язування помилкової, вживання закладних пристроїв і упровадження шкідливих програм [2].

На практиці виникають труднощі при кваліфікації дій особи, доступ якої до комп'ютерної інформації був санкціонований, але був використаний з неправомірною метою. Такий доступ потрібно називати неправомірним. Тобто він санкціонований, але використаний протиправно, отже – неправомірний доступ.

Ст. 361 КК України у початковій редакції від 2001 р. передбачала відповідальність за «незаконне втручання» в комп'ютерну систему. Але Законом України від 24 грудня 2004 р. законодавцем було замінено цей термін на «несанкціоноване втручання». Крім того, законодавець у ст. 362 КК України окремо виділяє несанкціоновані дії з комп'ютерною інформацією особою, що мала право доступу до неї. Але виникає проблема: якщо доступ і дії особи були санкціоновані, але результат дій був злочинним, то таке діяння не є кримінально караним за новою редакцією розділу XVI КК України, що, на нашу думку, неприпустиме.

Таким чином, неправомірний доступ включає такі дії злочинця:

1. Несанкціонований доступ.
2. Санкціонований доступ, але несанкціоновані дії.
3. Санкціонований доступ, санкціоновані, але неправомірні дії. Третій вид дій злочинця не охоплюється ст. 361 КК України, що неприпустиме і повинно бути виправлене законодавцем. Отже, по суті, правильніше було б у КК України передбачити відповідальність за неправомірний доступ до інформації замість «несанкціонованого втручання».

Для виключення неправомірного втручання в комп'ютерну інформацію та попередження злочинів з його використанням необхідно створити належну систему захисту цієї інформації. Це завдання не може бути вирішене ефективно без дотримання певних принципів.

А.А. Малюк вважає, що до основоположних принципів захисту комп'ютерної інформації необхідно відносити:

- принцип обґрунтованості доступу;
- принцип персональної відповідальності;
- принцип цілісності засобів захисту;
- принцип глибини контролю доступу [3, с. 35-36].

Розглянувши загальні принципи захисту інформації в комп'ютерних системах, потрібно зазначити, що для забезпечення безпеки інформації, що зберігається й оброблюється в КС, необхідне узгоджене застосування різноманітних заходів захисту. Тільки в цьому випадку існує потенційна можливість надійно захистити інформацію від різноманітних загроз. Розумне поєднання цих заходів для досягнення надійного захисту інформації одержало назву «комплексного підходу до забезпечення безпеки інформації».

Незважаючи на всю зовнішню принадність і явну теоретичну слушність комплексного підходу, його реалізація на практиці для реально функціонуючої КС утруднена існуванням ряду об'єктивних причин.

При розробці політики безпеки виникає проблема невідповідності динаміки змін політики безпеки змінам, які відбуваються в комп'ютерній системі. Як правило, для сучасних КС цей процес займає декілька місяців. Як показує практика, за час розробки цих документів стан КС змінюється, й іноді досить істотно, а отже, зміст розроблених документів не буде повною мірою відповідати дійсності.

В основу технології, яка може вирішити ці проблеми, можна покласти такі основні принципи:

1. Дворівневий опис стану засобів захисту КС. Для успішного вирішення задач, покладених на технологію забезпечення інформаційної безпеки, для КС, яка захищається, необхідно зберігати таку інформацію:

- дані про зміни значень реальних настроювань засобів захисту – рівень керування «як є насправді»;
- значення абстрактних дозволів і еталонних настроювань засобів захисту – рівень керування «як повинно бути».

2. Зміна номенклатури об'єктів керування доступом. Для формування рівня «як повинно бути» необхідно використання об'єктів рівня абстрактних дозволів політики безпеки. До їх числа належать такі об'єкти, як «співробітник», «підрозділ», «розв'язувані задачі» та ін.

3. Застосування документоорієнтованого підходу для керування доступом. Документований підхід до керування доступом означає:

- первинне призначення доступу і визначення прав доступу співробітників організації до ресурсів КС за допомогою формалізованих електронних документів (заявок, службових записок);
- контроль за станом інформаційної безпеки КС за допомогою типових формалізованих звітних документів у вигляді, прийнятому в організації (формуляри автоматизованих робочих місць, формуляри задач, переліки користувачів та їхніх повноважень, переліки порушень тощо).

4. Наявність механізму перевірки стану контрольованих настроювань.

5. Використання активних агентів на комп'ютерах, що захищаються. Спеціальні агенти забезпечують моніторинг зміни заданих настроювань та мають відношення до забезпечення інформаційної безпеки. Реалізація технології керування інформаційною безпекою, заснованої на зазначених принципах, дозволить:

- вирішити проблему контролю за змінами реальних настроювань засобів захисту;
- об'єднати різноманітні підсистеми, відповідальні за забезпечення безпеки організації, у єдину систему керування безпекою організації;
- постійно одержувати як актуальну інформацію про реальний стан захищеності КС, так і оцінки його відповідності вимогам, що існують в організації;
- контролювати діяльність системних і мережних адміністраторів, адміністраторів баз даних, а також інших користувачів, що мають розширені права щодо доступу до КС і керуванню нею;
- спростити керування доступом співробітників організації до ресурсів КС за рахунок уніфікації номенклатури об'єктів і прав доступу до них [4].

Висновки

У вище розглянутий спосіб реально об'єднати різні засоби забезпечення безпеки – засоби криптографічного захисту інформації, засоби аналізу захищеності і оповіщення про мережеві атаки та інші засоби захисту інформації від неправомірного втручання – в єдину систему та звести до мінімуму вчинення злочину.

Література

[1] .Кримінальний кодекс України: науково-практичний коментар / Ю. В. Баулін, В. І. Борисов, С. Б. Гавриш та ін., за заг. ред. В. В. Сташиса, В. Я. Тація. – К.: Концерн "Видавничий Дім "Ін Юре", 2006. – 1184 с.

Державний стандарт України 3396.0-96. Захист інформації. Технічний захист інформації: основні положення. – К., 1996.

Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автома-тизированых системах. – М., 2001.
Козаченко І.П., Голубєв В.О. Загальні принципи захисту інформації в банківських автоматизованих системах [Електронний ресурс]. – Режим доступу: http://bezpeka.com/ru/lib/spec/art92.html.

09