УДК 004.056.53

Черниш Л.Г. к.т.н.
Завацький С.М.

КОМБІНОВАНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

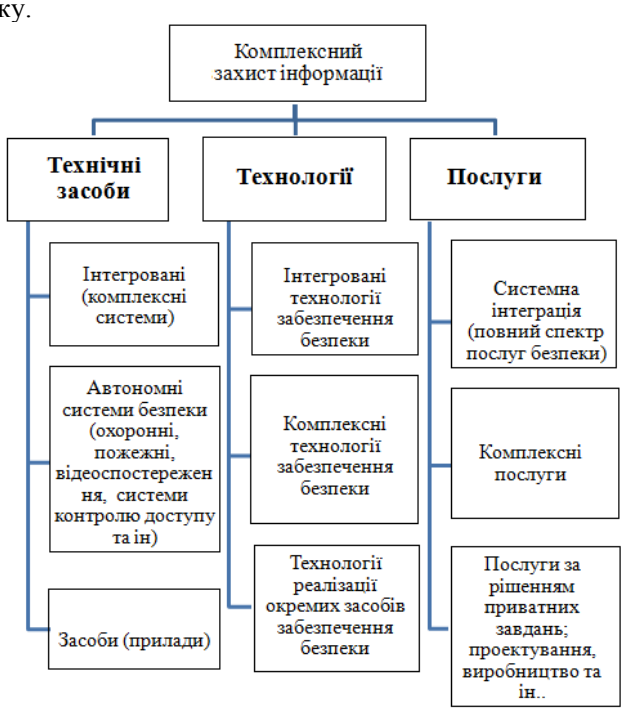
Національний авіаційний університет , e-mail: serJJJ17@yandex.ua

На сьогоднішній день основною тенденцією розвитку науки і техніки ,в тому числі і спеціальної техніки , є процес інтеграції . Цей процес необхідний для створення умов, за яких буде неможливим перехоплення, видозміна та знищення інформації, причому дія захисту повинна бути безперервна в часі і просторі.

Ключові слова:. *Інформаційна безпека. Захист інформації*

Мета статті . В наш час суттєво підвищити ефективність систем безпеки стало можливим тільки з використанням поняття інтегрованої безпеки , основний зміст якої полягає в необхідності забезпечити умови функціонування людини , об'єктів і інформації , за яких вони надійно захищені від усіх реальних видів загроз в ході безперервного виробничого процесу та життєдіяльності .

Основні матеріали дослідження . Однією з основних тенденцій розвитку науки і техніки , в тому числі і спеціальної техніки є процес інтеграції . Цей процес торкнувся таких сучасних напрямків, як електроніка , кібернетика , телекомунікації та , в тому числі технічні засоби зв'язку та захисту інформації. Кінцевою метою інтегрованого захисту інформації є створення умов , за яких буде неможливим як перехоплення , так і видозміна і знищення інформації , причому дія захисту повинна бути безперервна в часі і в просторі. Умовно процес інтегрування захисту інформації в рамках комплексної системи безпеки відображений на малюнку.



Створення систем захисту інформації в рамках комплексної системи безпеки грунтується на наступних принципах:

- Системний підхід до побудови системи захисту , що означає оптимальне поєднання взаємопов'язаних організаційних , програмних , апаратних , фізичних та інших властивостей, підтверджених практикою створення вітчизняних і зарубіжних систем захисту і застосовуються на всіх етапах технологічного циклу обробки інформації.
- Принцип безперервного розвитку системи як безперервного процесу , що полягає в обгрунтуванні та реалізації найбільш раціональних методів , способів і шляхів вдосконалення системи захисту інформації , безперервному контролі , виявленні її слабких місць , потенційних каналів витоку інформації та нових способів несанкціонованого доступу.
- Поділ і мінімізація повноважень по доступу до оброблюваної інформації та процедурам обробки, тобто надання користувачам мінімуму строго визначених повноважень , достатніх для виконання ними своїх службових обов'язків.
- Повнота контролю та реєстрації спроб несанкціонованого доступу, тобто необхідність точного встановлення ідентичності кожного користувача і протоколювання його дій для проведення можливого розслідування, а також неможливість здійснення будь-якої операції обробки інформації без її попередньої реєстрації.
- Забезпечення надійності системи захисту , тобто неможливість зниження рівня надійності при виникненні в системі збоїв , відмов , навмисних дій зломщика або ненавмисних помилок користувачів і обслуговуючого персоналу.

- Забезпечення контролю за функціонуванням системи захисту , тобто створення засобів і методів контролю працездатності механізмів захисту.
- Забезпечення всіляких засобів боротьби з шкідливими програмами.
- Забезпечення економічної доцільності використання системи захисту , що виражається в перевищенні можливого збитку інформаційних систем від реалізації загроз над вартістю розробки та експлуатації систем інформаційної безпеки.

Розглянемо основні складові інтегрованої системи захисту інформації комплексної системи безпеки об'єкта

Засоби виявлення прихованих закладок. Нелінійні локатори . Для виявлення будь-яких непрацюючих електронних засобів найбільш ефективним є застосування нелінійних радіолокаторів . Принцип дії таких пристроїв заснований на тому факті , що при опроміненні радіоелектронних пристроїв, що містять нелінійні елементи , такі як діоди , транзистори і т.д. , відбувається відображення сигналу на вищих кратних гармоніках . Відбиті сигнали реєструються локатором незалежно від режиму роботи радіоелектронного пристрою (ввімкнено-вимкнено).

Блокіратор мобільних телефонів. Стрімкий розвиток технологій мобільної телефонії породило цілий ряд проблем. У сфері інформаційної безпеки, зокрема захисту інформації від несанкціонованого доступу , з'явилися зовсім нові задачі визначення роботи стільникового телефону в захищається зоні і блокування його роботи з метою запобігання несанкціонованої передачі інформації , яка може носити конфіденційний характер. Це стосується як приватного бізнесу , так і державних структур , оскільки потенційно стільниковий телефон є готовим під слуховим пристроєм , що передає інформацію в каналі трафіку відповідного стандарту . Крім того , масове застосування мобільних телефонів породило ряд проблем як етичного , так і правового характеру , стосуються різних аспектів їх використання.

Засоби захисту від силових деструктивних впливів. В даний час в силу обставин, що склалися (тероризм , кримінал і т.п.) особливе значення надається засобам захисту від силових деструктивних впливів. Ці засоби , по суті є електромагнітною зброєю , яке здатні дистанційно і без зайвого шуму вразити практично будь-яку систему безпеки. Головне – забезпечити відповідну потужність електромагнітного імпульсу. Істотно підвищує скритність нападу то обставина , що аналіз ушкоджень у знищеному обладнанні не дозволяє однозначно ідентифікувати причину виникнення пошкодження , тому що причиною може бути як навмисне (напад) , так і ненавмисне (наприклад , індукція від блискавки) силовий вплив . Ця обставина дозволяє зловмисникові успішно використовувати технічні засоби силового деструктивного впливу неодноразово . В даний час встановлено , що комп'ютер або будь-яке інше електронне обладнання системи безпеки з урахуванням середовища передачі енергії деградації можуть бути піддані силовому деструктивному впливу за трьома основними каналами силового деструктивного впливу: по мережі живлення , по дротових каналах і по ефіру .

Організаційні засоби захисту . До організаційних засобів захисту можна віднести організаційно - технічні та організаційно-правові заходи , здійснювані в процесі створення і експлуатації об'єкта з метою забезпечення захисту інформації. Організаційні заходи охоплюють всі структурні елементи об'єкта та системи захисту на всіх етапах їх життєвого циклу: будівництво приміщень , проектування системи, монтаж і налагодження устаткування , випробування і перевірка в експлуатації комп'ютерної системи. При цьому організаційні заходи відіграють двояку роль у механізмі захисту : з одного боку , дозволяють повністю або частково перекривати значну частину каналів витоку інформації , а з іншого - забезпечують об'єднання всіх використовуваних в інформаційній системі засобів в цілісний механізм захисту . Організаційні заходи захисту базуються на законодавчих і нормативних документах з безпеки інформації.

Апаратні засоби захисту . Апаратними засобами захисту називаються різні електронні та електронно-механічні пристрої , які включаються до складу технічних засобів комп'ютерної системи і виконують самостійно або в комплексі з іншими засобами деякі функції захисту .

У даний час застосовується значне число різних апаратних засобів , причому вони можуть включатися практично в усі пристрої комп'ютерної системи : термінали користувачів , пристрої групового введення-виведення даних , центральні процесори , зовнішні запам'ятовуючі пристрої , інше периферійне устаткування. Так , наприклад , в терміналах користувачів найбільшого поширення отримали пристрої, призначені для попередження несанкціонованого включення терміналу в роботу (різного роду замки і блокатори) , забезпечення ідентифікації терміналу (схеми генерування ідентифікаційного коду) і ідентифікації користувача (магнітні індивідуальні картки , дактилоскопічні та акустичні пристрої впізнання тощо).

Криптографічні засоби захисту . Криптографічними засобами захисту називаються спеціальні засоби і методи перетворення інформації , що призводять до маскування її змісту. основними видами криптографічного закриття є шифрування та кодування даних, що захищаються . При цьому шифрування є такий вид закриття , при якому самостійного перетворенню піддається кожен символ закриваються даних;

при кодуванні захищаються дані діляться на блоки , що мають смислове значення , і кожен такий блок замінюється цифровим , буквеним або комбінованим кодом. Для криптографічного закриття інформації в комп'ютерних системах найбільшого поширення набуло шифрування . При цьому використовується кілька різних систем шифрування: заміною , перестановкою , гаммуванням, аналітичним перетворенням шифрованих даних . Також широко застосовуються комбіновані шифри , коли початковий текст перетворюється з використанням двох або навіть трьох різних шифрів .

Програмні засоби захисту . Програмними засобами захисту називаються спеціальні програми , які включаються до складу програмного забезпечення комп'ютерної системи спеціально для здійснення функцій захисту . Програмні засоби є найважливішою і неодмінною частиною механізму захисту сучасних комп'ютерних систем , що зумовлено такими їх перевагами, як універсальність , простота реалізації , гнучкість , практично необмежені можливості зміни розвитку . До недоліків програмних засобів відноситься необхідність витрачання ресурсів процесора на їх функціонування і можливість несанкціонованого (зловмисного) зміни , а також той факт , що програмні засоби захисту можна реалізувати тільки в тих структурних елементах комп'ютерної системи , в складі яких є процесор , хоча функції захисту програмними засобами можуть здійснюватися і в інтересах інших структурних елементів . Тому програмні засоби захисту застосовуються в центральних процесорах , пристроях групового управління введенням висновком даних , а також в апаратурі зв'язку в тих випадках , коли в їх складі є процесори.

Відомі на сьогоднішній день програми захисту можна розділити на наступні групи відповідно до виконуваними ними функціями :

- Програми ідентифікації ; програми регулювання роботи (технічних засобів , користувачів , функціональних завдань , елементів баз даних тощо) ;
- Програми шифрування даних, що захищаються ; програми захисту програм (операційних систем , систем управління базами даних , програм користувачів та ін..);
- Допоміжні програми (знищення залишкової інформації, формування грифа секретності видаваних документів, ведення реєстраційних журналів, імітація роботи з порушником, тестовий контроль механізму захисту і деякі інші).

Фізичні засоби захисту . До фізичних засобів захисту відносяться фізичні об'єкти , механічні, електричні та електронні пристрої , елементи конструкції будівель , засоби пожежогасіння і цілий ряд інших засобів , які забезпечують виконання наступних завдань : захист території і приміщень комп'ютерної системи об'єкта від проникнення зловмисників ; захист апаратури і носіїв інформації від пошкодження або розкрадання ; запобігання можливості спостереження за роботою персоналу і функціонуванням обладнання з-за меж території або через вікна; запобігання можливості перехоплення електромагнітних випромінювань працюючого обладнання та ліній передачі даних; контроль за режимом роботи персоналу; організація доступу в приміщення співробітників; контроль за переміщенням в різних робочих зонах; протипожежний захист приміщень ; мінімізація матеріального збитку і втрат інформації , які можуть виникнути в результаті стихійного лиха.

Фізичні засоби захисту є найбільш традиційними засобами охорони автоматизованої системи обробки даних. В принципі , вони нічим не відрізняються від давно використовуваних засобів охорони банків , музеїв , магазинів і інших об'єктів , які потенційно можуть залучити зловмисників.

Для реалізації систем фізичного захисту можуть бути використані найрізноманітніші засоби і методи , наприклад організація озброєної охорони ; ведення спостереження за всіма принципово можливими шляхами проникнення в приміщення комп'ютерної системи; організація пропускної системи і т.д.

Фізичним заходам захисту традиційно надається велике значення. Конкретна структура фізичної системи захисту , як і будь-який інший захисту , визначається важливістю матеріального , інформаційного або іншого ресурсу , що підлягає захисту , а також рівнем необхідної секретності , матеріальними можливостями організації , можливостями проведення різних організаційних заходів , існуючим законодавством і цілим рядом інших, не менш значущих чинників .

Висновки. Застосування розглянутих методів і засобів, а саме виявлення прихованих закладок, блокіратор мобільних телефонів, захист від силових деструктивних впливів , організаційні засоби захисту, апаратні засоби захисту, криптографічні засоби захисту, програмні засоби захисту, фізичні засоби захисту у рамках інтегрованого захисту інформації дозволяють істотно підвищити безпеку об'єктів та інформації, що обробляється.

Список використаних джерел

1. Герасименко В. А. Защита информации в автоматизированных системах обработки данных / В.А. Герасименко: в 2 кн.: Кн. 1.— М.: Энергоатомиздат, 1994.

2. Анин Б. Защита компьютерной информации. — СПб.: БХВ-Петербург, 2000.

3. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учеб. пособие. – М.: Горячая линия – Телеком, 2004.

4. Проектування інформаційних систем. Посібник / Заред. Пономаренка В.С. - К.: Видавничий центр "Академія", 2002. - 486с.

5. Дибкова Л.М. Інформатика та комп'ютерна техніка. Посібник. - К.: Академвидав, 2002 - 318с.