спектр проблем, щоб в Україні з'явився виважений і продискутований план дій щодо інформатизації країни і відповідна державна політика щодо використання національного інформаційного простору і ресурсу. Це треба зробити заради забезпечення: конституційних прав і свобод людини й громадянина в сфері одержання інформації; інформаційного забезпечення державної політики України в процесі розвитку сучасних інформаційних технологій і вітчизняної індустрії інформації. Її розвиток вимагає інституалізації, підпорядкування певним законам захисту національного інформаційного простору, національних інформаційних ресурсів, систем їхнього формування, поширення і використання всієї інформаційної інфраструктури заради реалізації прав громадян, суспільства і державних установ держави на інформацію. І, що головне, нові умови цивілізаційного розвитку обумовлюють обов'язкову присутність в структурі поняття «інформаційна безпека» щодо інтересів особи, суспільства і власно держави.

Нові законодавчі та директивні документи мають сполучати завдання як економічного, так і соціального розвитку України. І тут нам слід визнати, що в Україні, як і в інших пострадянських країнах може не вистачити досвіду і фахівців. Скажімо, на жаль, за час набуття незалежності ми втратили ціле покоління вчених і не є таємницею, що сьогодні молоді ми передаємо не стільки знання батьків, скільки знання і досвід дідів, а це, на наш погляд, гальмує цивілізаційний розвиток України і створює рецидиви його реверсного спрямування. Це має бути всім зрозуміло, оскільки людство хвилює одночасне зростання політичних і соціальних ризиків, пов'язаних з ворожим використанням інформації, поява принципова нових викликів і загроз безпечному життю людини, а захист інформації про розвиток соціально-економічних, політичних, оборонних напрямків стає найпершою потребою і функцією держави.

Список літератури

1. *Делягин М.Г.* Мировой кризис. Общая теория глобализации. — М.: 2003. — С. 51.

2. *Соснін О.В.* Проблеми державного управління системою національних інформаційних ресурсів з наукового потенціалу України: Монографія. — К.: Інститут держави і права ім. В.М.Корецького НАН України, 2003. — 572 с.

Надійшла 17 .11.09

УДК 004.621.391 **Павлов І.М.**

НЕФОРМАЛЬНИЙ ПІДХІД В МЕТОДИЦІ ОЦІНКИ ЕФЕКТИВНОСТІ ЕСКІЗНОГО ПРОЕКТУВАННЯ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

На сьогоднішній час мало хто уявляє собі можливість комп'ютерної обробки інформації без її захисту. Але що таке ефективний засіб захисту інформації та наскільки ефективно інформація захищається засобами захисту, які встановлюються в комп'ютерних системах (КС) – на це питання не завжди можуть відповісти як розробники таких систем, так і самі користувачі [1].

Коли мова йде про інформаційні технології, можна виділити два їх основних положення – це використання комп'ютера в особистих цілях користувача та корпоративне використання комп'ютера або службове використання. Від цього і зростають вимоги до конфіденційності, цілісності та доступності інформації, яка циркулює в цьому інформаційному просторі. Тому проведення аналізу та систематизація інформації по

побудові систем захисту інформації, які спроможні ефективно захищати інформаційні ресурси користувачів – є актуальною задачею проблеми захисту інформації та метою цієї статті.

Аналіз останніх досліджень і публікацій виявив різні підходи до проблеми створення систем захисту інформації [2-5]. В останніх публікаціях не завжди чітко виділяють етапи та підходи до проектування систем захисту інформації. Тому іноді неможливо розділити процес формального та неформального підходів до створення систем захисту інформації.

В даній статті показаний перший етап (неформальний підхід) до створення систем захисту інформації.

Система захисту інформації повинна розроблятися сумісно з КС. При побудові системи захисту можуть використовуватися існуючі засоби захисту, або розроблятися спеціально для конкретної КС (рис. 1).

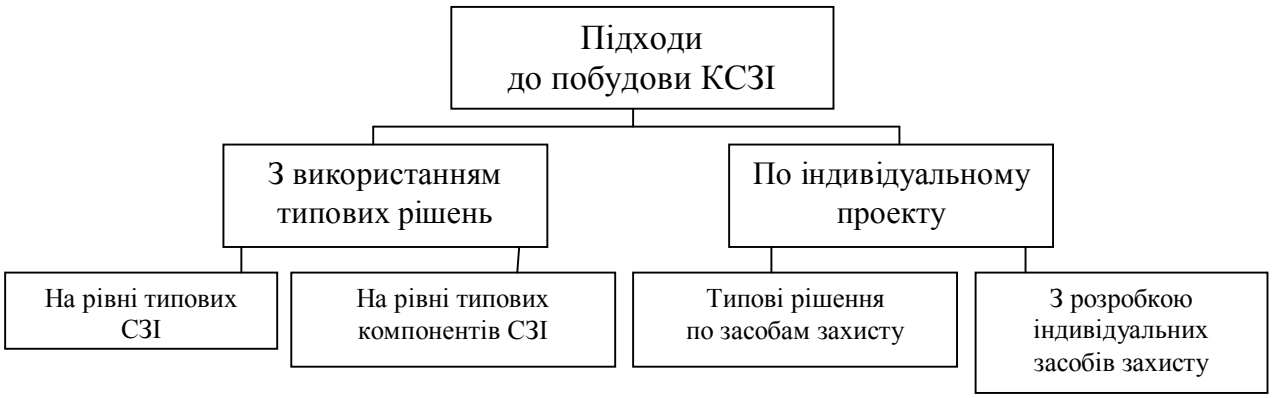

Рис. 1. Підходи до побудови комплексної системи захисту інформації

В залежності від особливостей КС, умов її експлуатації та вимог до захисту інформації процес створення КСЗІ може не мати окремих етапів або зміст їх може відрізнятися від визначених норм при розробці складних апаратно-програмних систем. Але в цілому розробка таких систем може включати наступні етапи [6]:

- розробка технічного завдання;
- ескізне проектування;
- технічне проектування;
- робоче проектування;
- вироблення дослідного зразка.

Одним з етапів розробки комплексних систем захисту інформації є етап ескізного проектування. Порядок послідовності та зміст ескізного проектування.

Ескізне проектування можна умовно розділити на 2 етапи: 1 етап неформального подання результатів та 2 етап – формального подання результатів досліджень [7].

Одна з важливих вихідних інформацій для побудови КСЗІ отримується під час аналізу комп'ютерної системи, яка захищається. Так як система захисту є підсистемою КС, то взаємодії системи захисту з КС можна визначити як внутрішнє, а взаємодію з зовнішнім середовищем – як зовнішнє [8]. Місце комплексу засобів захисту в КС представлено на рис.2.

Внутрішні умови взаємодії визначаються архітектурою КС.

При аналізі інформації визначаються важливість та ступінь конфіденційності інформації,яка повинна оброблятися, зберігатися та передаватися в КС. На основі аналізу робиться висновок про доцільність створення КСЗІ. Якщо інформація не є конфіденційною і

може швидко відновитися, то створювати КСЗІ немає потреби. В цьому випадку достатньо користуватися штатними засобами КС і можливе страхування від втрати інформації.

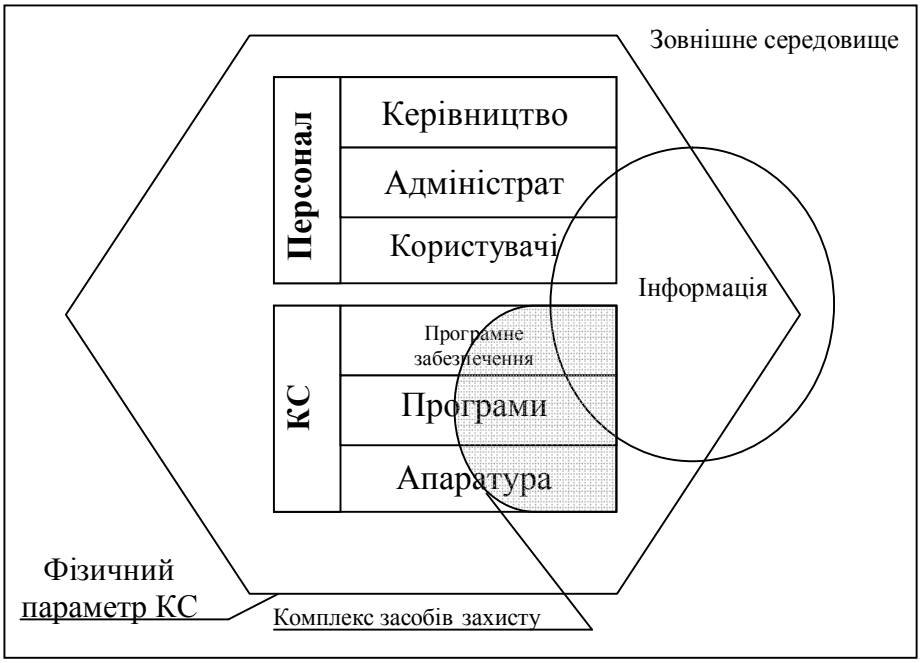

Рис. 2. Місце комплексу засобів захисту в комп'ютерній системі

При аналізі інформації визначаються потоки конфіденційної інформації, елементи КС, в яких вона зберігається і обробляється. На цьому етапі розглядаються питання розмежування доступу до інформації окремих користувачів та цілих сегментів КС. На основі аналізу інформації, нормативних документів з ТЗІ, галузевих стандартів ТЗІ визначаються вимоги до захищеності інформації. Вимоги задаються шляхом присвоєння певного грифу конфіденціальності та встановлення правил розмежування доступу.

Загальна схема методики оцінки ефективності ескізного проектування представлена на рис. 3.

Визначені вимоги до захищеності інформації обґрунтовуються шляхом видання відповідних документів та організації контролю. В результаті проведеної роботи в подальшому визначаються функції комплексної системи захисту інформації розроблюваного проекту [9].

Згідно з [10] канали впливу загроз діляться на канали несанкціонованого доступу (НСД) та загрози по технічним каналам витоку інформації. В свою чергу за ціллю використання весь масив загроз можна поділити на 3 класи [11]:

- загрози для самої комп'ютерної системи;
- загрози для КСЗІ:
- загрози для інформації.

Аналіз загроз є обов'язковою умовою побудови КСЗІ. За результатами проведеного аналізу будується модель загроз безпеки інформації в КС.

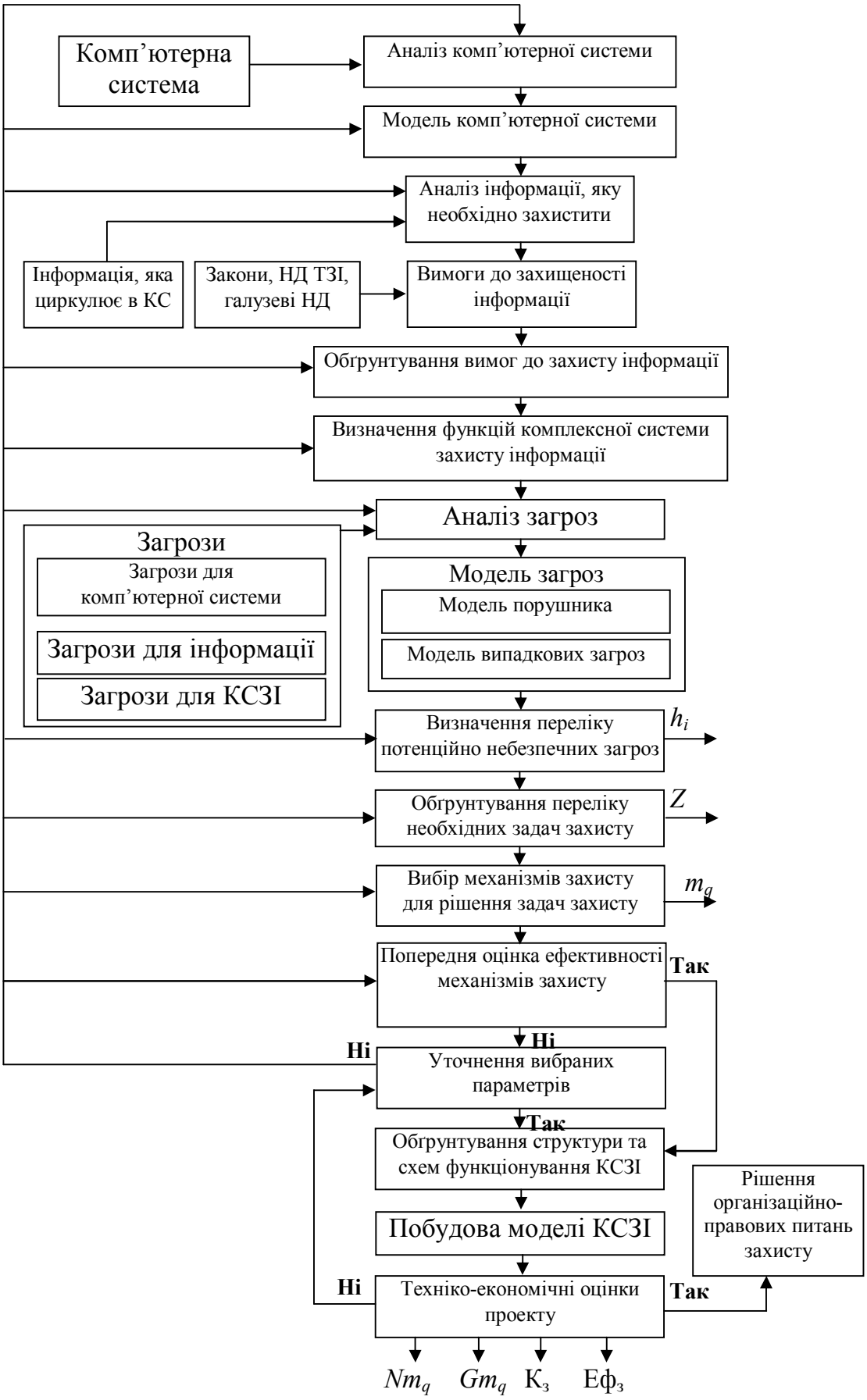

Рис. 3. Схема методики оцінки ефективності ескізного проектування КСЗІ

Загрози для КС можна поділити на загрози загальні і специфічні. Під загальними загрозами розуміються фізичні загрози для КС (знищення, пошкодження носіїв інформації, впровадження засобів перехоплення, крадіжка апаратних та програмних ключів тощо) та програмно-математичні загрози (помилки проектування КС, КСЗІ, впровадження закладних програм тощо).

Загрози для КСЗІ можна розподілити на 3 класи: атаки (напади), відмови в обладнанні, програмах, діях та аварії елементів КСЗІ.

Атака (напад) створює потенційно зашкоджуючі події в КСЗІ, які ініціюються противником (хакером). Атака включає в себе наступні фази: вторгнення, дослідження та експлуатацію. Атаки, як основний клас загроз для КСЗІ, враховуються при розрахунках живучості КСЗІ [12].

В табл.1 надані загальні загрози для КСЗІ ІТС.

Таблиця 1

Загрози для комплексних систем захисту інформації

№ з/п	**Назва загрози**
1.	Порушення технології роботи із засобами технічного захисту інформації.
2.	Впровадження в апаратні і програмні засоби систем захисту інформації компонентів, що реалізують функції, які не визначені документацією на ці засоби.
3.	Розробка і розповсюдження програм, які порушують нормальне функціонування систем інформаційних систем, в тому числі систем захисту інформації.
4.	Вплив на парольно-ключові системи захисту КСЗІ.
5.	Компрометація ключів і засобів криптографічного захисту.
6.	Блокування роботи засобів захисту інформації.
7.	Впровадження електронних пристроїв для перехоплення інформації в технічні засоби обробки, зберігання і передачі інформації по каналах зв'язку і автоматизації.
8.	Використання несертифікованих вітчизняних і закордонних технологій засобів захисту інформації при проектуванні та розробці елементів КСЗІ та КС.
9.	НСД до інформації в обхід системи захисту, яка знаходиться в банках та базах даних.

Відмови – потенційно зашкоджуючі події, які пов'язані з недоліками в елементах КСЗІ або в зовнішньому елементі, від якого залежить КСЗІ. Відмови можуть бути наслідком програмних помилок проектування, апаратних засобів, помилок людини і є згенерованими подіями. Відмови враховуються при розрахунках надійності КСЗІ [13].

Аварії (випадковості) описують велику кількість різних випадкових і потенційно зашкоджуючих подій, таких як стихійне лихо (форс-мажор). Аварії визначаються як зовнішньо згенеровані події (тобто за межами КСЗІ). Аварії враховуються при розрахунках живучості КСЗІ [14].

Враховуючи все зазначене вище, розглянемо вплив атак на КСЗІ.

Розглядається 3 чітких фази впливу загроз на КСЗІ: вторгнення, дослідження і експлуатацію.

Фаза вторгнення. В цій фазі зловмисник дотримується доступу до системи через різні сценарії атаки (нападу). Ці сценарії коливаються від спроб хакерських атак любителів до високо спланованих атак (нападів) професійних зловмисників. Ці спроби призначені для отримання вигоди з уразливих місць областей КСЗІ.

Фаза дослідження. В цій фазі система зламана і зловмисник вивчає внутрішню системну організацію і можливості КСЗІ. Вивчаючи, зловмисник дізнається як краще отримати і використати доступ для досягнення мети вторгнення.

Фаза експлуатації. В цій фазі, зловмисник отримав доступ в необхідну підсистему КСЗІ і виконує необхідні операції зі знищення підсистем (функцій) КСЗІ.

Вторгнення, дослідження і експлуатація створюють спіраль роботи зловмисника. Наприклад, проникаючи в систему на рівні користувача зловмисник використовує звичайні засоби для визначення уразливих місць. Наприкінці, використовуючи отриману інформацію, зловмисник проникає в захищені підсистеми.

Такий підхід дозволяє оцінити вплив усієї сукупності загроз на КСЗІ як в мирний час, так і під час використання КС, коли вона знаходиться під впливом противника.

Загрози для інформації по каналам НСД визначаються [15] і поділяються на загрози конфіденційності, цілісності, доступності спостережності та гарантій безпеки. Для протидії цим загрозам в КСЗІ та елементах СІТС під час проектування та розробки повинні враховуватися критерії безпеки інформації.

Загрози конфіденційності.

Аналіз розвитку КС показує, що на сьогоднішній час визначаються наступні шляхи порушень конфіденційності:

- втрата контролю над системою захисту інформації;
- канали витоку інформації.

Всі інші шляхи порушень конфіденційності повторюють вищезазначені шляхи.

Коли СЗІ перестає адекватно функціонувати, то стає вірогідною реалізація НСД до інформації. Втрата управління СЗІ може бути реалізована внаслідок порушень безпеки персоналу та керівництва.

Серед каналів витоку інформації виділяють канали з пам'яттю та тимчасові канали.

Канал з пам'яттю реалізується шляхом прямого або непрямого запису інформації в визначену область пам'яті одним процесом та прямим або непрямим читанням цієї області іншим процессом. Графічно канал с пам'яттю можна зобразити наступним чином:

$$U_1 \xrightarrow{(r,exe)} S \xrightarrow{r} O \xleftarrow{w} U_2 , \qquad (1)$$

тобто користувач U_1 активізує процес S, який може отримати доступ на читання (r) загального з користувачем U_2 ресурсу O, причому U_2 має доступ на запис (w) в O, а U_1 може читати (r) з S [16].

Приклад 1. Від U_2 в каталог O записані імена файлів. Навіть коли U_1, активує процес S, на який не має доступу, він має інформацію про файлову систему користувача U_2. Тобто, є виток частини інформації: або конкретна інформація є або її немає – 1 біт.

Захист від витоку інформації по цьому каналу оснований на виборі правильної політики безпеки а також на можливостях контролю інформаційних потоків і виводу інформації.

Іншим каналом з пам'яттю є канал типу "збір сміття", тобто виток інформації використовується шляхом контролю залишкової інформації в об'єктах після роботи користувача або процесу. Захист забезпечується зачищенням об'єкту після роботи або перед її початком, а також за допомогою шифрування інформації, яка розміщується в об'єктах.

Тимчасовий канал – це канал, який дозволяє передавати інформацію від одного процесу до іншого шляхом модуляції першим процесом деяких тимчасових характеристик інформаційної системи, які можуть спостерігатися іншим процесом. Графічно тимчасовий канал можна зобразити наступною схемою:

$$U_1 \xrightarrow{(r,exe)} S \xrightarrow{r} S_m \xleftarrow{w} S_ц \xleftarrow{w} U_2 , \qquad (2)$$

де U_1 – зловмисник, U_2 – користувач, який працює з конфіденційною інформацією $S_ц$ – суб'єкт, яким оперує користувач U_2, тобто, інформація про нього має користь для

зловмисника U_1, S_m – суб'єкт, процес якого модулюється інформацією процесу $S_ц$; S – процес користувача U_1, який дозволяє спостерігати за процесом S_m.

Пропускна спроможність тимчасового каналу визначається тією частиною цінної інформації про процес $S_ц$, яку можна отримати шляхом модуляції процесу S_m.

Приклад 2. Користувач U_2 за допомогою процесу $S_ц$ використовує принтер для розмноження інформації. Процес S_m визначається роботою принтеру, який є загальним ресурсом U_1 і U_2 з пріоритетом для U_2. Тоді процес S регулярно із заданою частотою посилає запит на використання принтеру і, отримує відмову, коли $S_ц$ друкує черговий цикл інформації. Відповідно витікає, що, в одиницях частоти запиту користувач U_1 отримує інформацію про періоди роботи процесу $S_ц$ з цінною інформацією, тобто, є канал витоку. Захист від таких каналів базується на контролі інформаційних потоків в системі.

Побічні канали витоку інформації по випромінюванню, живленню або акустиці також є каналами витоку. В цьому випадку захист досягається за допомогою екранування, зашумлення, фільтрації.

Крім використаних раніше схем графічного зображення каналів витоку можливе інше формалізоване моделювання за допомогою апарату математичної логіки.

Загрози цілісності

Мова опису загроз цілісності інформації аналогічна до мови опису загроз конфіденційності. Однак є різниця. Так для конфіденційності основна загроза – це ознайомлення з інформацією, тобто на саму інформацію активний вплив відсутній. Таким чином для опису цієї загрози достатньо поняття каналу витоку. Для цілісності основна загроза – це незаконна модифікація інформації, тобто активний вплив на інформацію з боку порушника. Замість звичайного каналу витоку можна ввести поняття каналу впливу на цілісність. Формально це призводить до заміни доступу на читання (r) доступом на запис (w).

Тоді, користуючись формалізованим підходом, який представлений в першому підрозділі, справедливий наступний вираз для визначення каналу впливу на цілісність:

$$\exists t \in N, \quad \exists p \in R' \subseteq R, \quad p \neq 0, \quad \exists U_i, \exists O \in O_t, \quad U_i \xrightarrow{p} {}^{*} O, \quad O \in O_t(U_j), \quad \exists j \quad , \qquad (3)$$

де R' – підмножина доступів, після яких можлива модифікація інформації. Тобто в деякий час існують деякі види доступу до інших об'єктів. Ці доступи є негативними. Прикладом виникнення каналу впливу на цілісність є використання програми «троянський кінь». Ця програма, крім документованих функцій, може робити приховані дії від імені того, хто її активізує, на користь розробника програми (зловмисника).

Порушення цілісності може виникати внаслідок створення випадкових або критичних ситуацій, зараження вірусами тощо.

Серед механізмів захисту від порушень цілісності виділяють наступні:

- своєчасне регулярне копіювання цінної інформації;
- введення надмірності в саму інформацію, тобто застосування кодування інформації, яке дозволяє контролювати цілісність;
- введення надмірності в процес обробки інформації, тобто використання автентифікації, яке дозволяє контролювати цілісність файлів, повідомлень та програм;
- введення системної надмірності, тобто підвищення живучості системи.

Загрози доступності

Згідно [13] особа, яка використовує ресурси КС по правилам політики безпеки, повинно отримати інформацію в необхідному для нього вигляді, визначеному місці та своєчасно.

Доступність в КС забезпечується правильним використанням ресурсів, стійкістю до відмов окремих компонентів (надійністю), можливістю їх ефективної заміни («гаряча заміна»), спроможністю до відновлення після збоїв.

В більшості випадків доступність інформації в КС визначається працеспроможністю самої КС, тобто її відсутність є основною загрозою. Можна виділити наступні напрямки повсякденної діяльності для підтримки працездатності КС:

-підтримка користувачів, тобто консультації та різного плану допомога;

-підтримка програмного забезпечення (ПЗ), тобто контроль за ПЗ, яке використовується в КС;

-конфігураційне управління, яке дозволяє контролювати зміни в програмній конфігурації;

-резервне копіювання;

-управління носіями, яке забезпечує фізичний захист носіїв;

-документування;

-регламентовані роботи.

Оскільки результатом дії будь-якої загрози доступності є відсутність будь-яких каналів доступу, то формально це можна виразити наступним чином:

$$\exists t \in N, \quad \forall p \in R, \quad \exists U_i, \exists O \in O_t, \quad U_i \xrightarrow{-}{}^{*} O, \quad O \in O_t(U_j), \quad \forall j \quad , \tag{4}$$

тобто в деякий момент часу жоден вид доступу будь-якого користувача не можливий до будь-якого об'єкту (на відміну до конфіденційності і цілісності) і є небезпечним.

Загрози спостережності

На відміну від конфіденційності або цілісності, де наявність каналів витоку є негативною обставиною, при спостережності повинні бути канали нагляду за інформацією, тобто канали, за допомогою яких можна отримати доступ на читання визначеної множини процесів та об'єктів, коли доступ до читання з об'єкту який забезпечує можливість його спостерігати. Графічно це можна зобразити наступним чином:

$$U_1 \xrightarrow{(r,exe)} S \xrightarrow{r} \{S_c, O_c\} \quad , \tag{5}$$

тобто є користувач U_1 який активізує процес S, та може отримати доступ на читання (r) до визначеної множини процесів та об'єктів $\{S_c, O_c\}$. Доступ на читання (r) є вагомою вимогою, оскільки для спостережності достатньо більш слабкого доступу (який, наприклад, дозволяв би тільки визначати – була подія чи ні).

Дії будь-якої загрози спостережності зводяться до неможливості її реалізувати або до відсутності будь-яких каналів доступу, які формально можна визначити як:

$$\exists t \in N, \quad \forall p \in R' \subseteq R, \quad \exists U_i, \exists O \in O_t, \quad U_i \xrightarrow{-}{}^{*} O, \quad O \in O_t(U_j), \quad \forall j \quad , \tag{6}$$

де R' - підмножина доступів, за допомогою яких можна спостерігати за процесами або об'єктами, тобто у користувача в деякий час відсутня можливість спостерігати за будь-якими об'єктами.

Таким чином, загрози спостережності зводяться до порушення або знищення каналів спостережності, а головна задача спостережності в КС – їх підтримка. Вона реалізується за допомогою наступних послуг: реєстрація (аудит), ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність комплексу засобів захисту, самотестування, ідентифікація та автентифікація при обміні, автентифікація відправника, автентифікація отримувача. [13].

Висновки

Під час розгляду питань неформального підходу до методики оцінки ефективності комплексних систем захисту інформації було розглянуто загальну структуру методики ескізного проектування комплексних систем захисту інформації комп'ютерних систем.

Було виділено в окремий етап та розглянуто основні існуючі підходи до аналізу самої комп'ютерної системи, інформації, яка в ній циркулює, аналіз загроз, які були проранжовані за цілями застосування та визначені етапи подальшої оцінки ефективності комплексних систем захисту інформації під час ескізного проектування.

Список літератури

1. *Зуев О.В., Хмелько Ю.М., Чирков Д.В.* Критерий оценки качества функционирования средств защиты информации // Захист інформації. – К.: 2001. – № 1. – С. 17-22.

2. *Астахов О.В.* Анализ защищённости корпоративних систем // Открытые системы. – М.: 2002. - № 7-8. – С. 16 – 23.

3. Абалмазов Э.И. Методы и инженерно-технические средства противодействия информационным угрозам. // - М.: Компания "Гротек", 1997.

4. Герасименко В.А. Защита информации в автоматизированных системах обработки данных: // в 2-х кн. - М.: Энергоатомиздат, 1994. - 176 с.

5. Гундарь К.Ю. Защита информации в компьютерных системах - К.: «Корнейчук», 2006.

6. Девянин П.Н. Теоретические основы компьютерной безопасности. // Учебное пособие для вузов - М.: Радио и связь, 2007.

7. *Мещеряков В.А.* Методическое обеспечение обоснования требований к системам защиты информации от программно- математического воздействия в автоматизированных информационных системах критического применения // Безопасность информационных технологий Выпуск 2, 1996, МИФИ.

8. *Загальні* положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу // НД ТЗІ 1.1 – 001 – 98. – Київ, 1998.

9. *Широчин В.П., Мухин В.Е., Кулик А.В.* Вопросы проектирования средств защиты информации в компьютерных системах и сетях. // – К.: Наукова думка, 2000. – 111 с.

10. *Порядок* проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційної системі // НД ТЗІ 3.7 – 003 – 05. – Київ, 2005. – 35 с.

11. *Павлов И.Н.* Проектирование систем защиты информации. Формальный подход // "Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні". – Київ, 2005. – Вып. 11. – С. 54 – 59.

12. *Павлов І.М.* Модель процесу роботи комплексної системи захисту інформації в спеціальних інформаційно-телекомунікаційних системах та вимоги до неї по захищеності інформації // Збірник наукових праць ВІТІ НТУУ "КПІ". – Київ, 2006. – № 3. – С. 82 – 91.

13. *Мещеряков В.А.* К вопросу идентификации компьютерных преступлений. Прикладные вопросы цифровой обработки и защиты информации. // Межвузовский сборник научных трудов ВВШМ и ВГТУ. Воронеж 1997.

14. *Домарев В.В.* Безопасность информационных технологий. Методология создания систем защиты. – К.: Свифт, 2001. – 680 с.

15. *Малюк А.А.* Информационная безопасность: Концептуальные и методологические основы защиты информации. – М.: Высшая школа, 2004. – 280 с.

Надійшла 8.12.09