УДК 681.3.004

Хамула С.В.

ОЦІНКА ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ ТЕХНІЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

Захист інформації, що обробляється в автоматизованих системах (АС), полягає в створенні і підтримці в дієздатному стані системи заходів, як технічних (інженерних, програмно-апаратних), так і нетехнічних (правових, організаційних), що дозволяють запобігти або ускладнити можливість реалізації загроз, а також знизити потенційні збитки у разі їх здійснення. Іншими словами, захист інформації повинний спрямовуватись на забезпечення безпеки оброблюваної інформації і АС в цілому, тобто такого стану, який забезпечує збереження заданих властивостей інформації і АС, що її обробляє. Система зазначених заходів називається комплексною системою захисту інформації (КСЗІ) [1].

Одним з основних завдань управління КСЗІ є контроль, перевірка та оцінка ефективності застосування технічних засобів захисту, які входять до її складу. Досягається це завдяки реалізації комплексу заходів, базовим з яких є процес побудови інформаційно-аналітичних моделей захисту інформації від загроз несанкціонованого доступу (НСД), які дозволяють оцінити ефективність використання засобів захисту і надають можливість прогнозувати наслідки прояву нових загроз НСД, які постійно змінюються і удосконалюються.

В даній роботі буде розглянуто інформаційно-аналітичну модель первинного базового захисту інформації, яка запропонована в наукових працях [2,3,4], де система технічного захисту інформації (ТЗІ) представлена у вигляді замкненої однорідної захисної оболонки, так званої перешкоди ТЗІ.

Якщо позначити імовірність не подолання системи захисту інформації через $P_{сзі}$, термін життєвого циклу інформації – $t_ж$, очікуваний термін подолання перешкоди зловмисником – $t_п$, імовірність обходу перешкоди зловмисником – $P_{обх}$, імовірність подолання перешкоди зловмисником - $P_п$, то умову достатності захисту можливо записати у вигляді співвідношень:

$$P_{сзі} = 1, \text{ якщо } t_ж < t_п \text{ і } P_{обх} = 0, \qquad (1)$$

де $P_{обх} = 0$ відображає необхідність замкнення перешкоди навколо об'єкту захисту

Відомо [5], що сума імовірностей двох несумісних подій, які утворюють повну групу, дорівнює 1, тобто в даному випадку:

$$P_{сзі} + P_П = 1. \qquad (2)$$

Якщо $t_ж > t_п$, а $P_{обх} = 0$, то

$$P_{сзі} = 1 - P_П, \qquad (3)$$

де $P_п$ - імовірність подолання перешкоди зловмисником за термін, менший за $t_ж$.

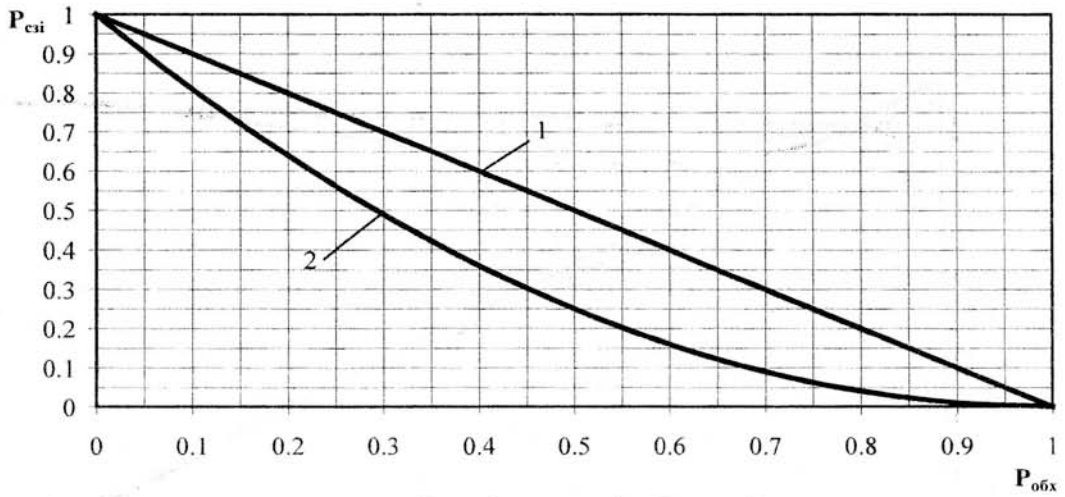
Для випадку, коли $t_ж > t_п$ і $P_{обх} = 0$, стійкість захисту можливо оцінити за допомогою виразу:

$$P_{сзі} = (1 - P_П)(1 - P_{обх}), \qquad (4)$$

де $P_п = 0$, якщо $t_ж < t_п$; $P_п > 0$, якщо $t_ж > t_п$.

Вираз (4) справедливий для випадку, коли зловмисників двоє, тобто коли один долає перешкоду, а інший її обходить.

Проаналізуємо формулу (4) функціональною залежністю $P_{сзі} = f(P_{обх})$ при $P_п = 0$ і $P_п > 0$. Графік такої залежності має наступний вигляд: (рис.1)



1 – дії одного зловмисника ($P_п = 0$ - *const*, $0 \le P_{обх} \le 1$);
2 – дії двох зловмисників ($0 \le P_п \le 1$, $0 \le P_{обх} \le 1$).

Рис. 1. Графік залежності імовірності не подолання СЗІ від імовірностей подолання і обходу перешкоди ТЗІ зловмисником.

Припустимо, що одному із зловмисників відома стійкість і складність перешкоди. Тоді він вибере один з варіантів подолання перешкоди ТЗІ за схемою "або". Вираз для визначення стійкості захисту матиме вигляд:

$$P_{сзі} = (1 - P_П) Y (1 - P_{обх}), \qquad (5)$$

У відповідності з виразом (5), стійкість перешкоди ТЗІ після визначення шляху її подолання зловмисником, дорівнюватиме найменшому значенню однієї з подій.

Вибір та визначення величини $P_{обх}$ можливо проводити експертним шляхом. Звичайно, за умов, коли $P_{обх} = 1$ заходи захисту втрачають всілякий зміст.

Якщо припустити, що у однієї перешкоди ТЗІ може бути кілька шляхів обходу, тоді вираз (5) набуває наступного вигляду:

$$P_{сзі} = (1 - P_П) Y (1 - P_{обх_1}) Y (1 - P_{обх_2}) Y \ldots Y (1 - P_{обх_k}), \qquad (6)$$

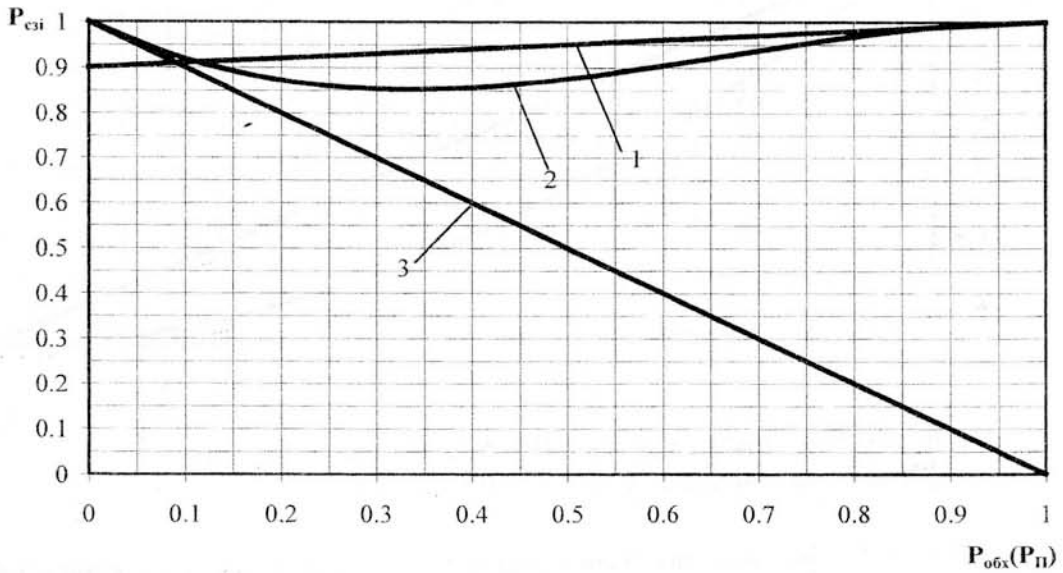
де k – кількість шляхів обходу перешкоди.

За умов здійснення масованих атак (організованих групою зловмисників), тобто за наявності можливості одночасного подолання первинної перешкоди ТЗІ і використання усіх шляхів її обходу вираз (6) набуває вигляду:

$$P_{сзі} = 1 - P_П \prod_{i=1}^{k} (1 - P_{обх_i}), \qquad (7)$$

де $P_{сзі}$ оцінюється імовірністю не подолання та не обходу перешкоди ТЗІ жодним з каналів НСД.

Графік залежності імовірності не подолання СЗІ від імовірностей подолання і обходу перешкоди ТЗІ зловмисником за умов здійснення масованих атак на об'єкт захисту має наступний вигляд: (рис. 2)



1 – ($P_п$ = 0,1 - *const*, $P_{обх1} = 0$, $0 \le P_{обх2} \le 1$);
2 – ($0 \le P_п \le 1$, $0 \le P_{обх1,2} \le 1$);
3 – ($0 \le P_п \le 1$, $P_{обх1,2} = 0$).

Рис. 2. Графік залежності імовірності не подолання СЗІ від імовірностей подолання і обходу перешкоди ТЗІ зловмисником за умов здійснення масованих атак на об'єкт захисту

У випадку, коли інформація, що підлягає захисту, періодично оновлюється (виконується умова $t_ж > t_п$, або коли, з будь-яких причин, забезпечити $t_п > t_ж$ неможливо), використовується постійна перешкода ТЗІ, яка виявляє і блокує доступ порушника до об'єкту захисту. Виконання зазначених заходів забезпечує служба захисту інформації, функції якої визначені нормативним документом технічного захисту інформації [6].

Вираз для визначення стійкості перешкоди ТЗІ з автоматизованим виявленням та блокуванням загроз НСД можливо записати у вигляді:

$$\left(T_{од} + t_{спр} + t_{вм} + t_{бл}\right) / t_п < 1, \qquad (8)$$

де $T_{од}$ - період опитування датчиків автоматизованої перешкоди ТЗІ;
$t_{спр}$ - термін спрацьовування спеціальної сигналізації;
$t_{вм}$ - термін визначення місця загрози НСД;
$t_{бл}$ - термін блокування загрози НСД;
$t_п$ - термін подолання перешкоди зловмисником.

Якщо термін виявлення і блокування загроз НСД позначити як $T_{вбл}$, отримаємо:

$$T_{вбл} = T_{од} + t_{спр} + t_{вм} + t_{бл}. \qquad (9)$$

Аналіз представленої в роботах [2,3,4] часової діаграми процесу контролю і виявлення НСД вказує на те, що умову стійкості перешкоди ТЗІ з автоматизованим виявленням і блокуванням загроз НСД можливо записати у вигляді:

$$T_{вбл} / t_{П} < 1. \qquad (10)$$

Зловмисник ТЗІ може бути невиявлений у двох випадках:

1. Якщо $t_{п} < T$;
2. Якщо $T < t_{п} < T_{вбл}$.

У першому випадку необхідна додаткова умова попадання інтервалу часу $t_{п}$ в інтервал Т (проміжок часу опитування датчиків ТЗІ). Для розв'язання цієї задачі зловмиснику необхідно під'єднати спеціальну апаратуру в момент здійснення НСД до інформації, що для сторонньої особи є складним завданням.

Імовірність успіху зловмисника ТЗІ можливо представити наступним чином:

$$P_{П} = (T - t_{П}) / T = 1 - t_{П} / T. \qquad (11)$$

Тоді імовірність виявлення НСД зловмисника буде визначатись:

$$P_{вбл} = 1 - P_{П}, \qquad (12)$$

або, з урахуванням (11):

$$P_{вбл} = t_{П} / T. \qquad (13)$$

За умов, коли $t_{п} > T$, а $P_{вбл} = 1$ зловмисник буде виявлений своєчасно, у противному випадку ($T < t_{п} < T_{вбл}$) імовірність успіху зловмисника визначатиметься виразом:

$$P_{П} = 1 - t_{П} / T_{вбл}. \qquad (14)$$

Імовірність виявлення і блокування несанкціонованих дій зловмисника ТЗІ має вигляд:

$$P_{вбл} = 1 - P_{П}, \qquad (15)$$

або, з врахуванням (14):

$$P_{вбл} = t_{П} / T_{вбл}. \qquad (16)$$

Аналізуючи (16) можливо зробити висновок, що за умови $t_{п} > T_{вбл}$ спроба НСД буде виявлена, оскільки $T_{вбл} = 1$.

Таким чином, розрахунок стійкості базової первинної перешкоди ТЗІ, з властивостями виявлення та блокування загроз НСД, визначається наступним чином:

$$P_{сзі} = P_{вбл} \, Y \left(1 - P_{обх_1}\right) Y \left(1 - P_{обх_2}\right) Y \ldots Y \left(1 - P_{обх_j}\right), \qquad (17)$$

де j - кількість шляхів обходу перешкоди ТЗІ

Для більш повного визначення стійкості перешкоди ТЗІ необхідно також враховувати надійність її функціонування.

Імовірність відмови елементів системи визначається формулою:

$$P_{\text{від}}(t) = e^{-\lambda t}, \qquad (18)$$

де λ - інтенсивність відмов групи технічних засобів, що складають систему виявлення та блокування загроз НСД;

t - час функціонування системи виявлення та блокування НСД, що розглядається

З урахуванням можливої відмови елементів автоматизованої системи контролю, стійкість перешкоди ТЗІ, з врахуванням (16) і (18), визначається наступним чином:

$$P_{\text{сзі}_k} = P_{\text{вбл}}\left(1 - P_{\text{від}}\right) Y \left(1 - P_{\text{обх}_1}\right) Y \left(1 - P_{\text{обх}_2}\right) Y \ldots Y \left(1 - P_{\text{обх}_j}\right) =$$

$$= t_{\text{П}} / T_{\text{вбл}} \left(1 - e^{-\lambda t}\right) Y \left(1 - P_{\text{обх}_1}\right) Y \left(1 - P_{\text{обх}_2}\right) Y \ldots Y \left(1 - P_{\text{обх}_j}\right). \qquad (19)$$

Значення імовірностей обходу перешкод ТЗІ ($P_{\text{обх1}}$, $P_{\text{обх2}}$ ... $P_{\text{обхj}}$) визначаються методом експертних оцінок.

Результатом аналізу моделі первинного базового захисту АСОІ від загроз НСД є вирази (6) і (19) за допомогою яких можливо визначити стійкість перешкод ТЗІ (неконтрольованої - за формулою (6), контрольованої – за формулою (19)), тобто оцінити ефективність застосування технічних засобів захисту, що входять до їх складу.

Аналізуючи ці співвідношення можливо сформулювати узагальнене правило захисту будь-якого об'єкту від загроз НСД: стійкість захисної перешкоди ТЗІ об'єкту захисту від загроз НСД є достатньою, якщо очікуваний термін подолання її зловмисником є тривалішим за термін життєвого циклу інформації, або тривалішим за термін виявлення і блокування несанкціонованого доступу до неї та її носіїв за умов відсутності шляхів обходу цієї перешкоди.

Література:

1. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-002-99 // Безопасность информации. – 1999. - № 1. – С. 8-18.
2. Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика, 1997. – 368 с.
3. Мельников В.В. Основы теории защиты информации в автоматизированных системах // Вопросы защиты информации. – 2000. - № 3. – С. 39-49.
4. Вертузаев М.С., Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу: навч. посібник. – К.: Вид. Європейського університету, 2001. – 322 с.
5. Вентцель Е.С. Теория вероятностей. – М.: Изд. физико-математической литературы, 1962. – 564 с.
6. Типове положення про службу захисту інформації в автоматизованій системі: НД ТЗІ 1.4-001-2000. – К., ДСТСЗІ СБ України, 2000. – 28 с.

Надійшла 27.03.2003