В.В. Шорошев,
А.Ю. Ільніцький

Інформаційно-аналітична модель первинного захисту від загроз несанкціонованого доступу

Згідно з вимогами стандартів технічного захисту інформації (ТЗІ) України однією з найважливіших задач управління комплексною системою ТЗІ ОВС України є контроль, перевірка та експертна оцінка ефективності організаційно-технічних заходів захисту, що використовуються. Досягається це реалізацією комплексу заходів, серед яких проблема створення інформаційно-аналітичних моделей захисту від загроз несанкціонованого доступу (НСД) до інформації займає досить суттєве місце. Такі моделі дозволяють не тільки дати оцінку заходів захисту, що використовуються, але і прогнозувати наслідки прояву нових загроз НСД, які постійно змінюються та удосконалюються. Розглянемо інформаційно-аналітичну модель експертної оцінки виявлення та блокувння загроз НСД до інформації автоматизованих систем (АС) і засобів обчислювальної техніки (ЗОТ)[1].

Згідно з вимогами стандартів ТЗІ України об'єктом захисту є інформація з обмеженим доступом, що становить державну або іншу передбачену законодавством України таємницю, конфіденційна інформація, що є державною власністю чи передана державі у володіння, користування, розпорядження (далі – інформація з обмеженим доступом (ІзОД)).

Основними носіями ІзОД в інформаційно-аналітичних підсистемах (ІАП) ОВС України засоби, які показані на рис. 1.

Як бачимо, носії різних видів інформації ОВС здебільшого знаходяться в приміщеннях, за винятком телекомунікаційних засобів, що можуть розміщуватись як в приміщеннях, так і на великих територіях. Але в усіх випадках навколо них, як об"єктів захисту, створюються так звані перешкоди (фізичні, режимні організаційні, апаратні, технічні, програмні, віртуальні і т. ін.).

Шорошев В'ячеслав Вікторович — кандидат технічних наук, провідний науковий співробітник НДІ НАВСУ.

Ільніцький Анатолій Юхимович — начальник лабораторії захисту інформаційних технологій НДІ НАВСУ, полковник міліції.

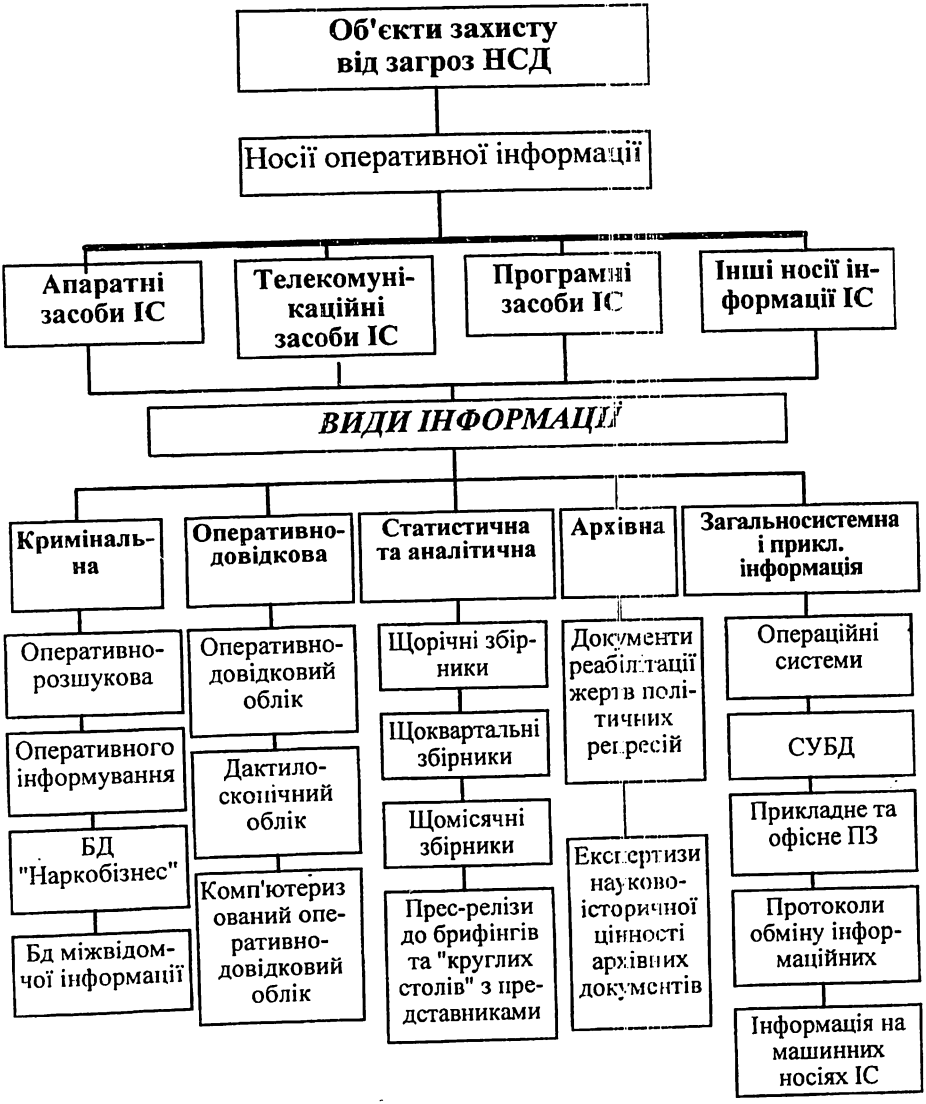

Рис. 1 Носії оперативної інформації та її основні види як об'єкти захисту від загроз НСД в ІС ОВС України

Таким чином, об'єкт захисту знаходиться, так би мовити, в замкненій та однорідній оболонці, яка зветься перешкодою. Стійкість захисту залежить від властивостей перешкоди. Принципову роль відіграє здатність перешкоди протистояти спробам подолання її порушником ТЗІ. Властивість об'єкту захисту – здатність приваблювати його власника та потенційного порушника ТЗІ. Привабливість об'єкта захисту полягає в його цінності (ціні). Ця властивість об'єкта захисту широко використовується при експертній оцінці захищеності інформації у будь-яких обчислювальних системах. Можна сформулювати два правила ТЗІ і моделі поведінки порушника ТЗІ.

Правило 1 – враховується, що стійкість створеної перешкоди ТЗІ достатня, якщо вартість очікуваних витрат на її подолання потенційним порушником перевищує вартість інформації, що захищається.

Але можливий інший підхід. Відомо, що інформація з часом втрачає свою цінність і починає старіти, а в окремих випадках її ціна може впасти до нуля. Звідси слідує друге правило.

Правило 2 – за умову достатності перешкоди ТЗІ доцільно прийняти перевищення витрат часу на подолання цієї перешкоди порушником ТЗІ над часом життєвого циклу (старіння, цінності) інформації, що захищається.

У загальному випадку найпростіша модель первинного, тобто одноланкового і однорівневого захисту будь-якого об'єкта від загроз НСД може бути у вигляді, що показаний на рис. 2.

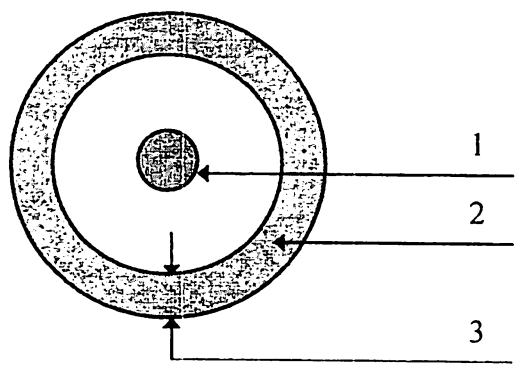

Рис. 2 Модель первинного базового захисту ПЕОМ від загроз НСД:
1 – об'єкт захисту від НСД;
2 – перешкода ТЗІ; 3 – стійкість перешкоди ТЗІ

Якщо позначити імовірність неподолання системи захисту інформації (СЗІ) через $P_{сзі}$, термін життєвого циклу (старіння, цінності) інформації через $t_ж$, очікуваний термін подолання перешкоди порушником через $t_п$, імовірність обходу перешкоди порушником через $P_{обх}$, то для випадку старіння інформації умову достатності захисту одержимо у вигляді таких відношень:

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

де $P_{обх}$, що дорівнює нулю, відображає необхідність замкнення перешкоди навколо об'єкта захисту. Якщо $t_ж > t_п$, а $P_{обх} = 0$, тоді

$$P_{сзі} = (1 - P_{под}),$$

де $P_{под}$ – імовірність подолання перешкоди порушником за термін, менший $t_ж$.

Для реального випадку, коли $t_ж > t_п$ і $P_{обх} = 0$, стійкість захисту можна записати у вигляді:

$$P_{сзі} = (1 - P_{под})(1 - P_{обх}),$$

де $P_{под} = 0$, якщо $t_ж < t_п$; $P_{под} > 0$, якщо $t_ж > t_п$.

Однак ця формула справедлива для випадку, коли порушників двоє, тобто коли один переборює перешкоду, а другий її обходить. Але у вихідній моделі поведінки потенційного порушника допускаємо, що розглядається поодинокий порушник і йому відома стійкість перешкоди та складність шляхів її обходу. Оскільки одночасно по двом шляхам він долати перешкоду не зможе, то вибере один з них – найбільш простіший, тобто по формулі "або". Тоді формульне вираження стійкості захисту в цілому для даного випадку буде відповідати формулі:

$$P_{сзі} = (1 - P_{под}) \, U \, (1 - P_{обх}),$$

де U – знак "або".

Таким чином, стійкість перешкоди після визначення і порівняння величин $(1 - P_{под})$ і $(1 - P_{обх})$ буде дорівнювати найменшому значенню однієї із них.

Як приклад первинного захисту, що вираховується за формулою (1), може бути криптографічний захист інформації, де величина $P_{под}$ може визначатись шляхом оцінки імовірності підбору коду ключа, за допомогою якого можна дешифрувати закриту

таким способом інформацію. Згідно (Л1) цю величину можна визначити за формулою:

$$P_{под} = n/A^{S}, \quad (2)$$

де n – кількість спроб підбору коду; A – кількість символів у вибраному алфавіті коду ключа; S – довжина коду ключа в кількості символів.

Величина $P_{обх}$ буде залежати від відібраного методу шифрування, способу застосування, повноти перекриття змісту інформації, існуючих методів криптоаналізу, а також способу зберігання дійсного значення коду ключа та періодичності його зміни на нове значення, якщо інформація, що закрита даним способом, постійно зберігається у її власника. Можливі й інші обставини, що впливають на імовірність обходу криптографічного захисту.

Вибір та визначення конкретної величини $P_{обх}$ спочатку можна проводити експертним шляхом на основі досвіду фахівців. Величина $P_{обх}$ повинна приймати значення від 0 до 1. При

$P_{обх} = 1$ захист втрачає усякий сенс.

Можливо також, що для однієї перешкоди може бути декілька шляхів обходу. Тоді формула (2) буде мати вигляд:

$$P_{сзі} = (1 - P_{под}) \, U \, (1 - P_{обх1}) \, U \, (1 - P_{обх2}) \, U(1 - P_{обх\text{-}к}), \quad (3)$$

де к – кількість шляхів обходу перешкоди, тобто стійкість перешкоди дорівнює найменшому значенню, що одержано після визначення та порівняння величин:

$(1 - P_{под}), (1 - P_{обх1}), (1 - P_{обх2}), (1 - P_{обх\text{-}к})$.

При масованих атаках ТЗІ, тобто при можливій одночасності подолання первинної перешкоди ТЗІ й одночасності обходу всіх її каналів формулу (3) можна подати у вигляді (максимальна загроза НСД через первинну перешкоду ТЗІ):

$$P_{сзі} = 1 - (1 - P_{под}) \prod_{1}^{K} P_{обх1} \, P_{обх2} \, P_{обх\text{-}к},$$

де $P_{сзі}$ оцінюється ймовірністю неподолання та необходу перешкоди ТЗІ по жодному із каналів НСД.

У тому разі, коли інформація, що підлягає захисту, не старіє або періодично оновлюється, тобто коли нерівність $t_{ж} > t_{п}$ постійна або ж коли забезпечити $t_{п} > t_{ж}$ по будь-яким причинам

неможливо, звичайно використовується постійно діюча перешкода ТЗІ, яка має властивості виявлення та блокування доступу порушника ТЗІ до об'єкта захисту. Таким захистом можуть бути людина або спеціальна автоматизована система виявлення під управлінням адміністратора безпеки (автоматизована першкода ТЗІ).

Очевидно, що параметри цієї перешкоди будуть впливати на її стійкість.

Здатність перешкоди виявляти та блокувати НСД повинна враховуватись при експертній оцінці її стійкості шляхом введення в формулу (3) замість $(1 - P_{под})$ величини $P_{бл}$ – імовірності виявлення та блокування загроз НСД.

Принцип роботи автоматизованої перешкоди ТЗІ заснований на тому, що в ній блоком управління здійснюється періодичний контроль датчиків виявлення порушника ТЗІ. Результати контролю спостерігаються адміністратором безпеки. Періодичність опитування датчиків автоматом може досягати тисячних долей секунди та менше. У цьому випадку очікуваний час подолання перешкоди порушником значно перевищує період опитування датчиків. Саме тому такий контроль часто вважають постійним. Але для виявлення порушника адміністратором безпеки, що керує автоматом контролю, тільки малого періоду опитування датчиків недостатньо.

Необхідний ще й термін на виробку сигналу тривожної сигналізації, тобто термін спрацювання автоматизованої перешкоди, оскільки він часто значно перевищує період опитування датчиків і, тим самим, збільшує термін виявлення порушника ТЗІ. Практика показує, що звичайно сигналу такої тривожної сигналізації достатньо для призупинення дій порушника ТЗІ, якщо цей сигнал до нього дійшов. Але оскільки фізичний або логічний доступ до об'єкта захисту поки що відкритий, подальші дії адміністратора безпеки (охорони) зводяться до визначення місця та організації блокування доступу порушника ТЗІ, на що також потрібний час.

Таким чином, умову стійкості автоматизованої перешкоди ТЗІ з виявленням та блокуванням загроз НСД можна показати у вигляді співвідношення:

$$(T_g + t_{спр} + t_{вм} + t_{бл}) / t_{п} < 1,$$

де T_g – період опитування датчиків автоматизованої перешкоди ТЗІ; $t_{спр}$ – термін спрацювання тривожної сигналізації; $t_{вм}$ – термін визначення місця загрози НСД; $t_{бл}$ – термін блокування загрози НСД.

Якщо позначимо суму (T_g + $t_{спр}$ + $t_{вм}$ + $t_{бл}$) через $T_{вбл}$, одержимо співвідношення:

$$T_{вбл} / t_п < 1,$$

де $T_{вбл}$ – термін виявлення і блокування НСД.

Процес контролю НСД та несанкціонованих дій порушника щодо його терміну показано на рис.3. З діаграми видно, що порушник може бути невиявленим у двох випадках:

а) коли $t_п < T$;

б) коли $T < t_п < T_{вбл}$.

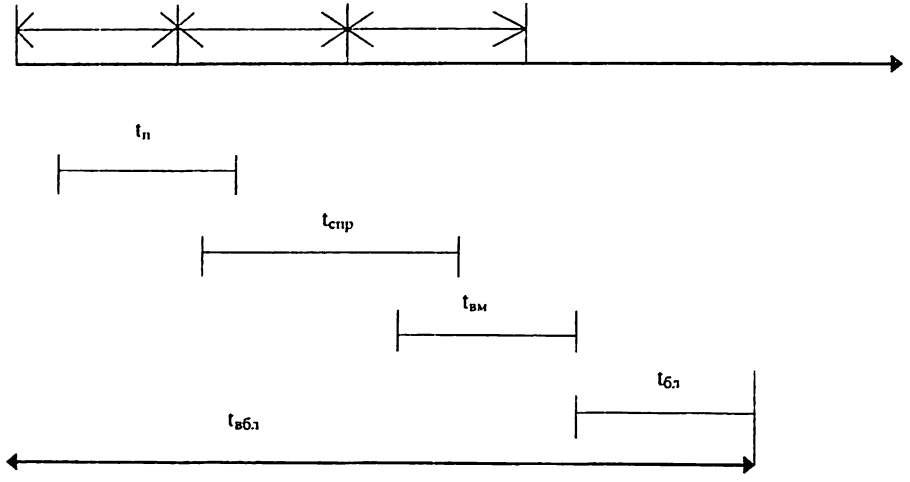

Рис. 3 Модель почасової діаграми контролю загроз НСД

У першому випадку потрібно додаткова умова попадання інтервалу часу $t_п$ в інтервал Т, тобто необхідна синхронізація дій порушника ТЗІ з частотою опитування датчиків виявлення загроз НСД. Для вирішення цієї задачі порушнику ТЗІ потрібно таємно підключити вимірювальну апаратуру в момент НСД до інформації, що являє собою досить складну задачу для стороннього порушника. Саме тому вважаємо, що свої дії з частотою опитування датчиків автоматизованої перешкоди ТЗІ він синхронізувати не зможе і може розраховувати лише на деяку ймовірність успіху, яка визначається в імовірності попадання відрізка часу $t_п$ в проміжок часу між моментами (запитами, імпульсами) опитування датчиків ТЗІ, що дорівнює Т.

Згідно з визначенням геометричної ймовірності одержимо формулу для визначення ймовірності успіху порушника ТЗІ:

$$P_{под} = (T - t_п) / T = 1 - t_п / T.$$

Тоді ймовірність виявлення несанкціонованих дій порушника буде визначатися:

$$P_{вбл} = 1 - P_{под},$$

$$\text{або } P_{вбл} = t_п / T. \qquad (4)$$

При $t_п > T$ порушник ТЗІ буде виявленим обов'язково, тобто $P_{вбл} = 1$.

У другому випадку, коли $T < t_п < T_{вбл}$, імовірність успіху порушника буде визначатись по аналогії з попереднім співвідношенням:

$$P_{под} = 1 - t_п / T_{вбл}.$$

Імовірність виявлення та блокування несанкціонованих дій порушника ТЗІ:

$$P_{вбл} = (1 - P_{под}),$$

$$P_{вбл} = t_п / T_{вбл}. \qquad (5)$$

При $t_п > T_{вбл}$ спроба НСД не має сенсу, оскільки вона буде виявлена обов'язково. У цьому разі $P_{вбл} = 1$.

Таким чином, стійкість первинної перешкоди ТЗІ з властивостями виявлення та блокування загроз НСД можна розрахувати за формулою:

$$P_{сзі} = P_{вбл} \cup (1 - P_{обх1}) \cup (1 - P_{обх2}) \cup (1 - P_{обхj}),$$

де j – кількість шляхів обходу цієї перешкоди; U – знак "або".

Ця формула справедлива також і для організаційного заходу захисту у вигляді періодичного контролю заданого об'єкта адміністратором безпеки. При цьому вважаємо, що виявлення, місця НСД та його блокування відбувається одночасно – в момент контролю об'єкта адміністратором безпеки, тобто $t_{спр} = t_{вм} = t_{бл} = 0$, $T_{вбл} = T$, де T – період контролю адміністратором безпеки об'єкта захисту. Імовірність виявлення та блокування дій порушника буде визначатись за формулою (4).

Для більш повного уявлення стійкості перешкоди у вигляді автоматизованої системи виявлення та блокування загроз НСД необхідно враховувати надійність її функціонування та шляхи можливого обходу її порушником ТЗІ.

Імовірність відмови системи визначається за формулою:

$$P_{відк}(t) = e^{-\lambda t}, \qquad (6)$$

де λ – інтенсивність відмов групи технічних засобів, що складають систему виявлення та блокування загроз НСД; t – інтервал терміну функціонування системи виявлення та блокування НСД.

З урахуванням можливої відмови автоматизованої системи контролю стійкість такої перешкоди ТЗІ буде визначатись за формулою:

$$P_{сзі} = P_{вбл}(1 - P_{відк})U(1-P_{обх1})U(1-P_{обх2})U(1-P_{обхj}), \quad (7)$$

де $P_{вбл}$ і $P_{відк}$ визначаються відповідно за формулами (5) і (6).

Величина $P_{обх}$ і кількість шляхів обходу визначаються експертним шляхом на основі аналізу принципів побудови автоматизованої системи контролю та блокування загроз НСД.

Одним із можливих шляхів обходу автоматизованої системи виявлення та блокування загроз НСД може бути можливість потайного відключення порушником цієї системи (наприклад, шляхом обривання або замкнення контрольних ланок, підключення імітатора контрольного сигналу, зміни програми збору сигналів тощо.) Імовірність такого роду подій визначається у межах від 0 до 1 методом експертних оцінок на основі аналізу принципів створення і роботи системи. При відсутності можливості несанкціонованого відключення системи величина його імовірності дорівнює нулю.

Таким чином, первинні захисні перешкоди доцільно використовувати двох видів: контрольовані і неконтрольовані адміністратором безпеки (оператором). Стійкість неконтрольованої перешкоди оцінюється за формулою (3), контрольованої – за формулою (7). Аналіз даних формул дозволяє сформулювати узагальнене концептуальне правило захисту будь-якого об'єкту ТЗІ з таким змістом.

Стійкість захисної перешкоди ТЗІ є достатньою, якщо очікуваний термін подолання її порушником ТЗІ є тривалішим за термін життєвого циклу (старіння, цінності) захищуваної інформації або триваліший терміну виявлення та блокування несанкціонованого доступу до неї та її носіїв при відсутності шляхів потайного обходу цієї перешкоди.

У більшості випадків на практиці захисна оболонка об"єкта ТЗІ складається із декількох "з'єднаних" між собою первинних перешкод ТЗІ з різною стійкістю та декількох рівнів або контурів ТЗІ.

---

[1] Див.: *Мельников В.В.* Защита информации в компьютерных системах. – М.: Финансы и статистика, Электронинформ, 1997.