# 2 Проблеми розвитку нормативної та методичної баз системи захисту інформації. Метрологічне забезпечення систем ТЗІ. Стандартизація, сертифікація та випробування засобів ТЗІ

**УДК 681.3**

## ЗАГРОЗИ ІНФОРМАЦІЇ І КАНАЛИ ВИТОКУ

***Анатолій Антонюк, Віктор Жора****

*Інститут програмних систем Національної Академії наук України,*

**Національний технічний університет України «КПІ»*

*Анотація:* **Розглянуто основні загрози інформації в автоматизованих системах. Для кожного класу загроз проаналізовано канали витоку інформації. Подано формальні визначення каналів витоку.**

*Summary:* **The article deals with the main information threats in automated systems. Channels of information leakage are analyzed for every class of threats. The formal definitions of leakage channels are proposed.**

*Ключові слова:* **Інформація, конфіденційність, цілісність, доступність, спостереженість, захист, загроза, канал витоку.**

### І Вступ

Для захисту інформації (ЗІ) необхідно витрачати сили і кошти, отже, треба знати, які витрати ми можемо понести в разі втрати інформації. Очевидно, що витрати на захист не повинні перевищувати можливих збитків при втраті інформації. Таким чином, необхідно ввести якусь міру цінності інформації, тобто визначити, в якому сенсі слід розуміти її цінність.

Сформулюємо властивості інформації, що визначають її цінність. Такими фундаментальними властивостями захищеної інформації (ФВЗІ) є конфіденційність, цілісність, доступність і спостереженість [1–4]. Конфіденційність визначається як властивість інформації, яка полягає в тому, що вона не може бути доступною для ознайомлення користувачам і/або процесам, які не мають на це відповідних повноважень. Цілісність інформації – це властивість, яка полягає в тому, що вона не може бути доступною для модифікації користувачам і/або процесам, які не мають на це відповідних повноважень. Цілісність інформації може бути фізичною і/або логічною. Доступність інформації – це властивість, що полягає в можливості її використання за вимогами користувача, який має відповідні повноваження. Спостереженість – це властивість інформації, яка полягає в тому, що процес її обробки має безперервно знаходитися під контролем органу, що керує захистом.

Під загрозами розуміються шляхи реалізації дій, що вважаються небезпечними. Наприклад, загроза зйому інформації і перехоплення випромінювання з дисплею веде до втрати секретності або конфіденційності, загроза пожежі веде до порушення цілісності та доступності інформації, загроза розриву каналу передачі інформації може реалізувати втрату доступності.

В [1–4] констатується, що загрози інформації розглядаються з точки зору їх будь-якої небажаної дії на будь-яку з цих властивостей і можливого їх порушення. З цієї точки зору в автоматизованих системах (АС) розрізняють наступні класи загроз інформації:

- порушення конфіденційності;
- порушення цілісності;
- порушення доступності або відмова в обслуговуванні;
- порушення спостереженості або керованості.

Таким чином, загроза – це потенційно можлива несприятлива дія на інформацію, що призводить до порушень хоча б одної з наведених властивостей.

Аналіз загроз є одним з найбільш важливих питань при побудові захищених АС. Аналіз загроз має виявити можливі загрози інформації, а також показати, з якого боку і в якій точці АС слід чекати атаки. Загрози можуть реалізуватися внаслідок багатьох причин, серед яких [5]:


*ISBN 966-622-022-9*
*Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.*

- кількісна недостатність – фізична нестача компонентів АС для протидії можливим порушенням безпеки інформації;
- якісна недостатність – недосконаліть конструкції або організації компонентів АС, внаслідок чого не забезпечується протидія можливим порушенням безпеки інформації;
- відмови елементів АС – порушення працездатності елементів, яке призводить до неможливості виконання ними своїх функцій;
- збої елементів АС – тимчасове порушення працездатності елементів, яке призводить до неправильного виконання ними в деякий момент часу своїх функцій;
- помилки елементів АС – неправильне (одноразове або систематичне) виконання елементами своїх функцій внаслідок специфічного (постійного або тимчасового) їх стану;
- стихійні лиха – явища, що виникають випадково, не контролюються і призводять до фізичних зруйнувань;
- зловмисні дії – дії людей, що спеціально спрямовані на порушення безпеки інформації;
- побічні явища – явища, що супутні виконанню елементом АС своїх функцій.

Джерелами наведених причин порушення безпеки можуть бути:

- особи, що мають будь-яке відношення до функціонування АС;
- технічні засоби;
- моделі, алгоритми, програмне забезпечення (ПЗ);
- технологія функціонування – сукупність засобів, прийомів, правил, заходів і погоджень, що використовуються в процесі обробки інформації;
- зовнішнє середовище – сукупність елементів, що не входять до складу АС, але можуть впливати на захищеність інформації в АС.

Розглянемо наведені класи загроз більш докладно.

## II Загрози конфіденційності

Аналіз розвитку теорії та практики ЗІ показує, що на сьогоднішній день визначаються наступні основні шляхи порушення конфіденційності [6]:

- втрата контролю над системою захисту інформації (СЗІ);
- канали витоку інформації.

Всі інші шляхи порушення конфіденційності так чи інакше зводяться до них.

Якщо СЗІ перестає адекватно функціонувати, то, звичайно, може реалізуватися несанкціонований доступ (НСД) до інформації. Втрата керування СЗІ може бути реалізована внаслідок наведених в першому розділі причин та джерел порушень безпеки. Зрозуміло, що в реальному житті слід розглядати їх комбінації. Вони можуть бути також причиною виникнення прихованих каналів витоку інформації.

Прихований канал витоку інформації або просто канал витоку – це спосіб отримання інформації за рахунок використання шляхів передачі інформації, які присутні в АС, але не керуються або не спостерігаються СЗІ. Канали витоку характеризують ситуацію, коли або проектувальники не змогли попередити НСД, або СЗІ не в змозі розглядати такий доступ як заборонений [6].

Серед каналів витоку виділяють канали з пам’яттю і часові канали. Канал з пам’яттю реалізується шляхом прямого або непрямого запису інформації в певну область пам’яті одним процесом і прямим або непрямим читанням даної області іншим процесом. Графічно канал з пам’яттю можна зобразити наступним чином

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

тобто користувач $U_1$ активізує процес $S$, який може отримати доступ на читання ($r$) до спільного з користувачем $U_2$ ресурсу $O$, причому $U_2$ має доступ на запис ($w$) в $O$, а $U_1$ може читати ($r$) від $S$.

Приклад 1. Від $U_2$ в каталог $O$ записано імена файлів. Навіть якщо $U_1$, активізуючи процес $S$, не має доступу до самих файлів, він має інформацію про файлову систему користувача $U_2$. Отже, маємо виток частини інформації: або конкретний файл є, або його немає – 1 біт.

Захист проти витоку інформації за таким каналом базується на виборі правильної політики безпеки, а також на можливостях контролю інформаційних потоків та виводу інформації.

Іншим каналом з пам’яттю є канал типу «збирання сміття», тобто коли виток інформації здійснюється шляхом зйому залишків інформації в об’єктах після роботи користувача або процеса. Захист забезпечується очищенням об'єкта після роботи або перед її початком, а також за допомогою шифрування інформації, що міститься в об'єктах [ 3].

Часовий канал витоку – це канал, що дозволяє передавати інформацію від одного процесу до іншого шляхом модуляції першим процесом деяких часових характеристик АС, які можуть спостерігатися іншим процесом. Графічно часовий канал можна зобразити наступною схемою

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

де $U_1$ – зловмисник; $U_2$ – користувач, що працює з конфіденційною інформацією; $S_u$ – суб'єкт, з яким оперує користувач $U_2$, отже, інформація про нього є цікавою для зловмисника $U_1$; $S_m$ – суб'єкт, процес якого модулюється інформацією процесу $S_u$; $S$ – процес користувача $U_1$, що дозволяє спостерігати за процесом $S_m$.

Пропускна здатність часового каналу визначається тією долею цінної інформації про процес $S_u$, яку можна отримати шляхом модуляції процесу $S_m$.

Приклад 2. Нехай користувач $U_2$ за допомогою процесу $S_u$ використовує принтер для друкування результатів чергового циклу обробки інформації. Процес $S_m$ визначається роботою принтера, який є загальним ресурсом $U_1$ і $U_2$ з пріоритетом для $U_2$. Тоді процес $S$ регулярно з заданою частотою посилає запит на використання принтера і, звичайно, отримує відмову, коли $S_u$ друкує черговий цикл інформації. Отже, в одиницях частоти запиту користувач $U_1$ отримує інформацію про періоди роботи процесу $S_u$ з цінною інформацією, тобто маємо канал витоку. Захист від таких каналів базується на контролі інформаційних потоків в АС.

Приклад 3. Перехоплення інформації в каналі зв'язку є прикладом часового каналу витоку. Тут реалізується безпосередній (навіть без модуляції) доступ до процесу обробки (передачі) цінної інформації. Захистом від таких каналів є криптографічні засоби.

Побічні канали витоку по випромінюванню, живленню або акустиці є також часовими каналами витоку. Тут захист досягається за допомогою екранування, зашумлення, фільтрації.

Крім застосованих раніше схем графічного зображення каналів витоку, за допомогою апарату математичної логіки можливе їх більш складне формальне моделювання. Один зі способів моделювання захищених систем розглянуто в [7]. Скористаємося наведеним підходом, а також деякими результатами.

Отже, при моделюванні деякої системи вважається, що час є дискретним і приймає значення з множини $N$={1, 2,... }, тобто $t \in N$. Позначимо множину всіх видів доступів через $R$, $|R|<\infty$. Якщо $p \subseteq R$, то доступ $p$ активізованого (тобто такого, що може перетворювати інформацію) суб'єкта $S$ до об'єкта $O$ позначимо через $S \xrightarrow{p} O$, а неможливість доступу через $S \xrightarrow{-} O$. Якщо в деякий проміжок часу реалізована послідовність доступів

$$U \xrightarrow{a} S_1 \xrightarrow{a} S_2 \xrightarrow{a} \ldots \xrightarrow{a} S_k \xrightarrow{p} O,$$

то вважається, що здійснено доступ $S \xrightarrow{p} {}^{*}O$ від імені суб'єкта $S$ до об'єкта $O$ (через $a$ тут позначено процес активізації). Позначимо також через $O_t$ множину об'єктів системи в момент $t$, $|O_t|<\infty$, а також через $O_t(U)$ множину об'єктів з $O_t$, які породив користувач $U$. Звичайно, вважаємо, що $U \in O_t(U)$. Отже, за цими позначеннями для $i$-го та $j$-го користувачів запишемо наступний вираз

$$\exists t \in N, \quad \exists p \in R, \quad p \neq 0, \quad \exists U_i, \exists O \in O_t, \quad U_i \xrightarrow{p} {}^{*}O, \quad O \in O_t(U_j), \quad i \neq j,$$

який означає, що в певний момент часу існує деякий (непорожній) вид доступу, можливий для певного користувача, до об'єкта, який створив інший користувач. Саме такі доступи вважаються несприятливими (оскільки завдяки ним можуть реалізуватися загрози) і саме вони називаються каналами витоку.

## III Загрози цілісності

Мова опису загроз цілісності інформації є аналогічною мові опису загроз конфіденційності. Однак між загрозами цим властивостям є принципова різниця. Так, для конфіденційності основна загроза – це незаконне ознайомлення з інформацією, тобто на саму інформацію активна дія відсутня. Виявилося, що для опису такої загрози достатньо поняття каналу витоку. Для цілісності ж основна загроза – це незаконна модифікація інформації, тобто активна дія на інформацію з боку порушника. Отже, замість звичайного каналу витоку зручно ввести поняття каналу дії на цілісність [6]. Формально це зводиться до заміни доступу на читання ($r$) доступом на запис ($w$).

Тоді, скориставшись формалізмом, поданим в попередньому розділі, запишемо наступний вираз для визначення каналу дії на цілісність

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

де $R'$ - підмножина доступів, за якими можлива модифікація інформації. Отже, в деякий момент часу


*ISBN 966-622-022-9*
*Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.*

існують певні види доступу до інших об'єктів, що можливі для деякого користувача. Такі доступи вважаються несприятливими.

Прикладом виникнення каналу дії на цілісність є використання програми «троянский кінь». Така програма, крім документованих функцій, може здійснювати приховані дії від того, хто її активізує, на користь розробника програми (зловмисника). Як правило, «троянский кінь» використовується для модифікації захищеної інформації.

Порушення цілісності може виникнути внаслідок створення випадкових або навмисних критичних ситуацій, зараження вірусами тощо. Всі наведені в першому розділі причини та їх джерела можуть створити порушення цілісності інформації.

Серед механізмів захисту від порушень цілісності виділяються наступні:

- своєчасне регулярне копіювання цінної інформації;
- введення надмірності в саму інформацію, тобто застосування перешкодозахищеного кодування інформації, що дозволяє контролювати її цілісність;
- введення надмірності в процес обробки інформації, тобто використання автентифікації, що дозволяє контролювати цілісність файлів, повідомлень і програм;
- введення системної надмірності, тобто, за військовою термінологією, підвищення «живучості» системи.

## IV Загрози доступності

Порушення доступності може виникнути внаслідок наведених у першому розділі причин порушень безпеки та їх джерел. Відповідно до визначення доступності, особа, використовуючи ресурси АС за правилами політики безпеки, повинна отримати інформацію в необхідному їй вигляді, місці і вчасно.

Доступність в АС забезпечується правильним використанням ресурсів, стійкістю до відмов окремих компонент, можливістю їх ефективної заміни («гаряча» заміна), здатністю до відновлення після збоїв [3].

В більшості випадків доступність в АС інформації визначається працездатністю самої АС [7], тобто її відсутність слід вважати основною загрозою. Можна виділити наступні напрямки повсякденної діяльності в АС для підтримки її працездатності:

* підтримка користувачів, тобто консультації і різного роду допомоги користувачам;
* підтримка ПЗ, тобто контроль за ПЗ, яке використовується в АС;
* конфігураційне керування, яке дозволяє контролювати зміни в програмній конфігурації;
* резервне копіювання;
* керування носіями, що забезпечує фізичний захист носіїв;
* документування;
* регламентні роботи.

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

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

тобто в деякий момент часу жоден вид доступу деякого користувача є неможливим до будь-яких об'єктів. Підкреслимо, що в даному випадку саме відсутність каналів доступу (на відміну від конфіденційності та цілісності) вважається небезпечною.

## V Загрози спостереженості

На відміну від конфіденційності або цілісності, де наявність каналів витоку є негативною обставиною, спостереженість зобов'язує мати канали спостереження. Тобто канали, за допомогою яких можна отримати доступ на читання до певної множини процесів та об'єктів, якщо вважати, що доступ на читання з об'єкта забезпечує можливість його спостерігати. Графічно це можна зобразити наступним чином

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

тобто користувач $U_1$ активізує процес $S$, який може отримати доступ на читання ($r$) до певної множини процесів та об'єктів $\{S_c, O_c\}$. Термін певна множина має на увазі обраний і фіксований перелік подій, які мають відношення до безпеки інформації в АС. Слід також звернути увагу на те, що доступ на читання ($r$) є досить сильною вимогою, оскільки для спостереженості достатньо більш слабкого доступу (який, наприклад, дозволяв би тільки визначати – була подія чи ні).

Дія будь-якої загрози спостереженості зводиться до неможливості її реалізувати або до відсутності будь-яких каналів доступу, що формально виражється наступним чином

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

де $R'$ - підмножина доступів, за якими можливо спостерігати за процесами або об'єктами. Тобто в деякий момент часу відсутня жодна можливість користувачу спостерігати за будь-якими об'єктами.

Отже, загрози спостереженості зводяться до ушкодження або навіть знищення каналів спостереження, а головна задача спостереженості в АС – їх підтримувати. Вона реалізується за допомогою наступних послуг [3]: реєстрація (аудит), ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність комплексу засобів захисту, самотестування, ідентифікація і автентифікація при обміні, автентифікація відправника, автентифікація отримувача.

Найбільш розповсюдженою практикою реалізації спостереженості є протоколювання та аудит. Протоколювання - це збір і накопичування інформації про події, що відбуваються в АС. Аудит – це аналіз накопиченої інформації. Протоколювання та аудит організуються для виконання наступних цілей:

* забезпечення звітності користувачів та адміністраторів;
* забезпечення можливості реконструювання послідовності подій;
* виявлення спроб порушення інформаційної безпеки;
* представлення інформації для виявлення та аналізу проблем інформаційної безпеки.

## VI Висновки

Подано основне поняття інформаційної безпеки – загрози інформації. Сформульовані властивості захищеної інформації, які визначають її цінність. Кожна властивість обговорюється на предмет загроз і механізмів захисту від них. Визначаються канали витоку інформації і подається деякий формальний опис загроз, що пов'язані з ними.

Отримані формальні визначення загроз ФВЗІ можна використати для дослідження політики безпеки та захищеності АС, а також дослідження профілів захищеності в АС.

*Література: 1. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.-НД ТЗІ 1.1-002-98, ДСТСЗІ СБ України, Київ, 1998. 2. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.-НД ТЗІ 1.1-001-98, ДСТСЗІ СБ України, Київ, 1998. 3. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.-НД ТЗІ 2.2-001-98, ДСТСЗІ СБ України, Київ, 1998. 4. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.-НД ТЗІ 2.2.-002 -98, ДСТСЗІ СБ України, Київ, 1998. 5. Герасименко В. А. Защита информации в автоматизированных системах обработки данных.-М.: Энергоатомиздат.-1994.-тт. 1,2. 6. Грушо А. А., Тимонина Е. Е. Теоретические основы защиты информации. М.: «Яхтсмен», 1996. 7. Галатенко В. А. Информационная безопасность: практический подход.-М.: Наука, 1998. 301 с.*

**УДК 519.724.681**

# МЕТОДИ ВИЗНАЧЕННЯ ЦІННОСТІ ІНФОРМАЦІЇ ДЛЯ ОРГАНІЗАЦІЇ ЇЇ ЗАХИСТУ

***Борис Мороз, Олег Молотков, Юлія Ульяновська***
*Академія митної служби України*

*Анотація:* **Розглянуто взаємозв'язок у визначенні цінності і старіння інформації при її обробці і використанні з метою її захисту. Визначено взаємозалежність захисту інформації з її цінністю та старінням. Особлива увага приділяється методам визначення цінності інформації з метою визначення заходів її захисту в мережах передачі даних.**

*Summary:* **The correlation in definition of value and deterioration of information is considered at to handling and use with the purpose it of guards. The interdependence of a guard of the information with it value and aging is defined. The special attention is given to methods of definition of value of the information with the purpose of definition of measures on it to a guard in data networks.**

*Ключові слова:* **Інформація, цінність та старіння інформації, захист.**

## I Вступ


*ISBN 966-622-022-9*
*Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.*