УДК 004.056

Л.М. Скачек,
кандидат технічних наук

ОЦІНКА УРАЗЛИВОСТІ ІНФОРМАЦІЇ В МЕРЕЖАХ ЗВ'ЯЗКУ

Здійснено оцінку уразливості інформації в мережах зв'язку.
Ключові слова: *оцінка, уразливість інформації, мережа зв'язку.*

Осуществлена оценка уязвимости информации в сетях связи.
Ключевые слова: *оценка, уязвимость информации, сеть связи.*

An assessment of the vulnerability of information in communication nets is carried out.
Keywords: *assessment, vulnerability information, telecommunication network.*

Одним із першочергових завдань, що передують оцінці безпеки конфіденційного зв'язку, є завдання оцінки уразливості інформації. Для дослідження і практичного вирішення завдань із захисту інформації потрібні **показники,** які характеризують найбільш несприятливі ситуації з точки зору уразливості інформації. Ними є найбільш уразливий структурний компонент мережі зв'язку (СС), найнебезпечніший дестабілізуючий чинник, найненадійніший елемент захисту, найбільш небезпечний потенційний порушник, найважливіша інформація.

Велике значення для оцінки захищеності й уразливості має часовий інтервал, відносно якого оцінюється захищеність. Попри те, що час є категорією суто безперервною, для цілей, що розглядаються тут, його як параметр захищеності можна структурувати, виділивши інтервали для аналізу й оцінки рівня захищеності або уразливості інформації.

Уразливістю інформації є подія, що виникає як результат збігу обставин, коли через певні причини використовувані в автоматизованих системах обробки даних засоби захисту не в змозі чинити достатній опір прояву дестабілізуючих чинників і небажаного його впливу на інформацію, що захищається.

При вивченні конкретних видів уразливості інформації: порушення фізичної або логічної цілісності, несанкціонованої модифікації, несанкціонованого отримання, несанкціонованого розмноження.

При деталізації загальної моделі основна увага акцентується на тому, що переважна більшість порушень фізичної цілісності інформації має місце в процесі її обробки на різних ділянках технологічних маршрутів. При цьому цілісність інформації залежить не лише від процесів, що відбуваються на об'єкті, але і від цілісності інформації, що поступає на його вхід. Основну небезпеку становлять випадкові дестабілізуючі чинники (відмови, збої і помилки компонентів автоматизованих систем обробки даних), які потенційно можуть проявитися в будь-який час, і в цьому плані можна говорити про регулярний потік цих чинників. Із

стихійних лих найбільшу небезпеку становлять пожежі, небезпека яких більшою чи меншою мірою також є постійною. Небезпека побічних явищ практично може бути зведена до нуля шляхом належного вибору місця для приміщень автоматизованої системи обробки даних та їх устаткування. Що стосується зловмисних дій, то вони пов'язані, головним чином, з несанкціонованим доступом до ресурсів автоматизованої системи обробки даних. При цьому найбільшу небезпеку являє занесення вірусів.

Відповідно до викладеного вище, загальну модель процесу порушення фізичної цілісності інформації на об'єкті автоматизованої системи обробки даних представлено на рис. 1.

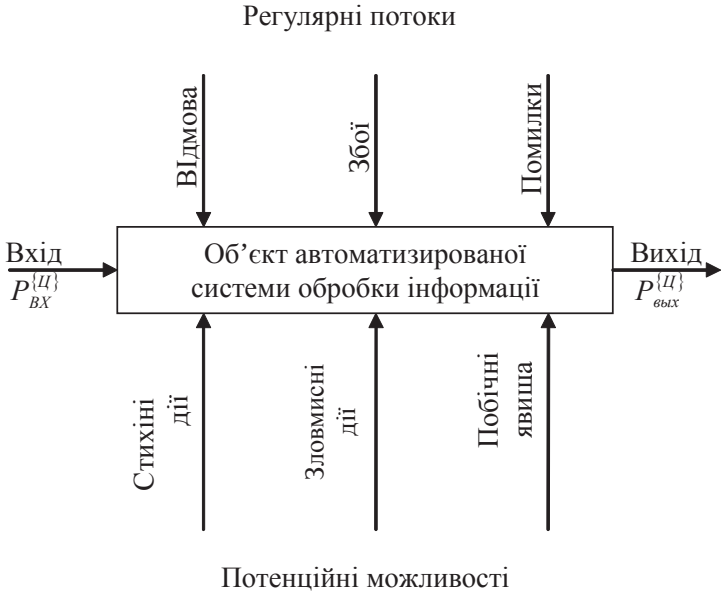

Рис. 1. Загальна модель процесу порушення фізичної цілісності інформації

З точки зору несанкціонованого отримання інформації принципово важливою є та обставина, що в сучасних автоматизованих системах обробки даних воно можливе не лише шляхом безпосереднього доступу до баз даних, але і багатьма шляхами, що не вимагають такого доступу. При цьому основну небезпеку становлять зловмисні дії людей. Дія випадкових чинників безпосередньо не призводить до несанкціонованого отримання інформації, вона лише сприяє появі каналів несанкціонованого отримання інформації, якими може скористатися зловмисник.

Розглянемо далі трансформацію загальної моделі уразливості з точки зору несанкціонованого розмноження інформації. Принциповими особливостями цього процесу є:

• будь-яке несанкціоноване розмноження є зловмисною дією;

• несанкціоноване розмноження може здійснюватися в організаціях-розробниках компонентів автоматизованої системи обробки даних, безпосередньо в автоматизованій системі обробки цих і сторонніх організацій, причому останні

можуть отримувати носій, із якого робиться спроба зняти копію як законним, так і незаконним шляхом.

Спроби несанкціонованого розмноження інформації в розробника й у автоматизованій системі обробки даних є одним із видів зловмисних дій з метою несанкціонованого її отримання, й тому імітуються наведеною моделлю. Якщо ж носій з інформацією, що захищається, яким-небудь шляхом (законним або незаконним) потрапив до сторонньої організації, то для його несанкціонованого копіювання можуть використовуватися будь-які засоби і методи, включаючи й такі, які носять характер наукових досліджень і дослідно-конструкторських розробок.

Як правило, моделі дозволяють визначати поточні і прогнозувати майбутні значення всіх показників уразливості інформації для будь-яких компонентів автоматизованої системи обробки даних, будь-якої їх комбінації і для будь-яких умов життєдіяльності автоматизованої системи обробки даних.

Деякі зауваження щодо використання

1. Практично всі моделі будуються на припущенні незалежності тих випадкових подій, сукупності яких утворюють складні процеси захисту інформації в сучасних автоматизованих системах обробки даних.

2. Для забезпечення роботи моделей потрібні великі обсяги таких початкових даних, переважна більшість яких нині відсутня, а формування пов'язане зі значними труднощами.

Визначимо: зауваження перше – допущення незалежності випадкових подій, що відбуваються в системах захисту інформації. Основними подіями, імітованими в моделях визначення показників уразливості, є: прояв дестабілізуючих чинників, дія дестабілізуючих чинників, що проявилися, на інформацію, що захищається, і дію використовуваних засобів захисту на дестабілізуючі чинники. При цьому зазвичай робляться наступні допущення.

1. Потенційні можливості прояву кожного дестабілізуючого чинника не залежать від прояву інших.

2. Кожен зі зловмисників діє незалежно від інших, тобто не враховуються можливості формування коаліції зловмисників.

3. Негативна дія на інформацію кожного з дестабілізуючих чинників, що проявилися, не залежить від такої ж дії інших чинників, що проявилися.

4. Негативна дія дестабілізуючих чинників на інформацію в одному якому-небудь компоненті автоматизованої системи обробки даних може привести лише до вступу на входи пов'язаних з ним компонентів інформації з порушеною захищеністю і не чинить впливу на таку ж дію на інформацію в самих цих компонентах.

5. Кожен з використовуваних засобів захисту чинить нейтралізуючу дію на дестабілізуючі чинники і поновлюючу дію на інформацію незалежно від такої ж дії інших.

6. Сприятлива дія засобів захисту в одному компоненті автоматизованої системи обробки даних лише знижує вірогідність вступу на входи пов'язаних з ним компонентів інформації з порушеною захищеністю і не впливає на рівень захищеності інформації в самих цих компонентах.

Насправді ж події, перелічені вище, є залежними, хоча міра залежності різна: від незначної, якою цілком можна нехтувати, до істотної, яку слід враховувати.

Проте для вирішення цього завдання нині немає необхідних передумов, тому залишаються лише методи експертних оцінок.

Друге зауваження торкається забезпечення моделей необхідними початковими даними. Раніше вже неодноразово відзначалося, що для практичного використання моделей визначення показників уразливості потрібні великі обсяги різноманітних даних, причому переважна більшість з них нині відсутня.

Сформулюємо тепер рекомендації з використання моделей, розроблених у рамках розглянутих раніше допущень, маючи на увазі, що це використання, забезпечуючи рішення завдань аналізу, синтезу і управління в системах захисту інформації, не повинне призводити до істотних погрішностей.

Перша і основна рекомендація зводиться до того, що моделями повинні користуватися кваліфіковані фахівці у сфері захисту інформації, які могли б у кожній конкретній ситуації обрати найбільш ефективну модель і критично оцінити міру адекватності отримуваних рішенні.

Друга рекомендація полягає в тому, що моделі потрібно використовувати не просто для набуття конкретних значень показників уразливості, а для оцінки поведінки цих значень при варіюванні істотно значимих початкових даних у можливих діапазонах їх змін. У цьому плані моделі визначення значень показників уразливості можуть служити дуже цінним інструментом при проведенні ділових ігор із захисту інформації.

Третя рекомендація зводиться до того, що для оцінки адекватності моделей, початкових даних і отримуваних рішень потрібно якомога ширше притягати кваліфікованих і досвідчених експертів.

Четверта рекомендація полягає в тому, що для ефективного використання моделей потрібно безперервно проявляти турботу про початкові дані, необхідні для забезпечення моделей при вирішенні завдань захисту. Істотно важливою при цьому є та обставина, що переважна кількість початкових даних має високий ступінь невизначеності. Тому потрібно не просто формувати необхідні дані, а перманентно їх оцінювати й уточнювати.

Модель уразливості інформації в мережах зв'язку в загальному вигляді деталізується при вивченні конкретних видів уразливості інформації, які ґрунтуються на базі сформульованих зауважень із їх використання. Причому вони сформульовані з урахуванням допущень, які дозволяють вирішення завдань аналізу, синтезу й управління в системах захисту мереж зв'язку, але не повинні призводити до істотних погрішностей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про захист інформацій в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР.

2. ДСТУ ISO/IES TR 13335-3:2003 "Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій".

3. Хореев П.Б. Методы и средства защиты информации в компьютерных системах / П.Б. Хореев. – М. : Изд. "Академия", 2005. – 256 с.

Отримано 11.10.2013.