УДК 681.3.06

Труш О.В., Хахлюк О.А.

ЦІЛІСНІСТЬ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ: ЗАГРОЗИ ТА МЕТОДИ ЗАХИСТУ

У статті приведено класифікацію загроз цілісності інформації в інформаційно-телекомунікаційних системах спеціального призначення та проведено їх аналіз. Визначено можливі методи захисту від порушень цілісності при передачі інформації.

Ключові слова: цілісність інформації, загрози, технічний захист інформації.

Сучасні інформаційно-телекомунікаційні системи спеціального призначення є орієнтованими, в першу чергу, на обробку інформації з обмеженим доступом, яка є власністю держави. Відповідно до вимог законодавства для забезпечення конфіденційності, доступності, цілісності та спостереженості інформації в таких ІТС повинна створюватися система захисту інформації (СЗІ), як невід'ємна їх складова. СЗІ являє собою складну організаційно-технічну, економічну й інформаційну систему, і, як правило, складається з організаційних та інженерних заходів, фізичних засобів захисту, комплексу технічного захисту інформації (ТЗІ) та комплексу засобів захисту від несанкціонованого доступу.

Метою технічного захисту інформації є запобігання витоку технічними каналами або порушення *цілісності інформації* з обмеженим доступом. Аналіз наукових праць та публікацій, присвячених забезпеченню ефективного захисту інформації свідчить про те, що підвищення безпеки інформації в ІТС СП можливе лише при *комплексному підході до аналізу можливих загроз й удосконалення засобів захисту від них*.

Загрозами будемо називати шляхи реалізацій дій, які вважаються небезпечними з погляду забезпечення захищеності інформації. Таким чином, загроза – це потенційно можливий несприятливий вплив на інформацію, що призводить до порушення конфіденційності, цілісності, доступності інформації, відмови в обслуговуванні тощо.

Оцінка ефективності функціонування СЗІ можлива на підставі аналізу узагальненої моделі її взаємодії з навколишнім середовищем. Причому узагальнена модель повинна відображати процес захисту інформації як взаємодію дестабілізуючих факторів і засобів захисту.

В даний час широко використовується узагальнена ймовірнісна модель процесу захисту інформації, представлена на рис. 1. У відповідності до неї обробка інформації на об'єкті O_i здійснюється в умовах впливу на інформацію різних загроз $\{З_j\}$. Для забезпечення інформаційної безпеки об'єкту СЗІ повинна здійснювати нейтралізуючий вплив на дестабілізуючі фактори та загрози. Ймовірність ефективного захисту інформації від *j*-ї загрози $P_{зij}$ можна визначити наступним чином:

$$P_{зij} = 1 - P_{зj}(1 - P_{нj}),$$

де $P_{зj}$ – ймовірність впливу *j*-ї загрози на *i*-й об'єкт, $P_{нj}$ – ймовірність нейтралізації впливу *j*-ї загрози. Тоді загальну ефективність СЗІ $P_{сзі}$ (ймовірність захисту інформації від усіх можливих загроз *n*) запишемо, як

$$P_{сзі} = \prod_{j=1}^{n} P_{зij} .$$

Тому *метою статті є аналіз можливих загроз цілісності інформації в ІТС СП та визначення методів захисту від них.*

Цілісність забезпечується шляхом дотримання вимог політики безпеки по переміщенню інформації від відправника до отримувача. Під повнотою захисту при обміні, варто розуміти врахування багатьох можливих типів загроз, від яких забезпечується захист.

Серед способів захисту від порушень цілісності можна виділити наступні:

- введення надмірності в саму інформацію (використання коригувальних кодів);
- введення надмірності в процес обробки інформації (використання процедури

аутентифікації);

- введення системної надмірності (підвищення живучості системи).

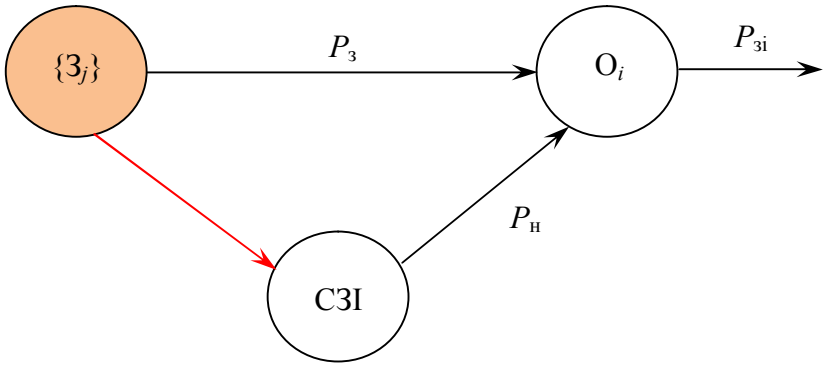

Рис. 1. Узагальнена модель процесу захисту інформації

Розглянемо загрози, які спрямовані, в першу чергу, на індивідуальні повідомлення, передані в ІТС. Типовим об'єктом нападу може служити інформаційний обмін між двома (або більше) користувачами системи.

Такими загрозами є наступні:

- перехоплення;
- несанкціоноване відтворення інформації;
- маскування;
- маніпуляції даними;
- радіоелектронне подавлення (РЕП).

Загальна класифікація загроз повідомленням, які передаються в ІТС спеціального призначення, представлена на рис. 2.

Розглянемо ці загрози докладніше з погляду порушення цілісності переданої інформації.

Перехоплення. Перехоплення являє собою ситуацію несанкціонованого вивчення або відтворення інформації, переданої або збереженої в ІТС, і відноситься до всіх мереж і до всіх видів інформаційного трафіку.

Ефективність загроз такого виду залежить від виду інформації, яка може бути перехоплена. У випадку перехоплення мовних повідомлень або даних зловмисникам стає відома конфіденційна інформація. При перехопленні покажчиків управління зловмисник може одержати доступ до даних ідентифікації користувача або групи користувачів, даних про його місце розташування або рівні пріоритету, місця розташування терміналу, що використовується, переліку необхідного обслуговування і т.д.

Результати перехоплення можуть використовуватися для підтримки інших нападів, зокрема при маскуванні під іншого користувача або для управління деякими даними.

Несанкціоноване перехоплення даних на інтерфейсі між користувачами ІТС ніколи не може бути виявлене або повністю відвернене механізмами системної безпеки. Основними способами боротьби з перехопленням є:

- взаємна аутентифікація через інтерфейс між користувачами;
- шифрування інтерфейсу між користувачами;
- шифрування між кінцевими точками;
- механізм передачі ключів шифрування по інтерфейсу між користувачами;
- використання методів підвищення прихованості зв'язку (наприклад, застосування шумоподібних сигналів).

Маскування. Для маскування існують такі можливості:

- маскування під іншого користувача (або термінал) з метою отримання призначеної йому інформації;

- маскування під ретрансляційну станцію (РС) для одержання окремих викликів від користувачів.

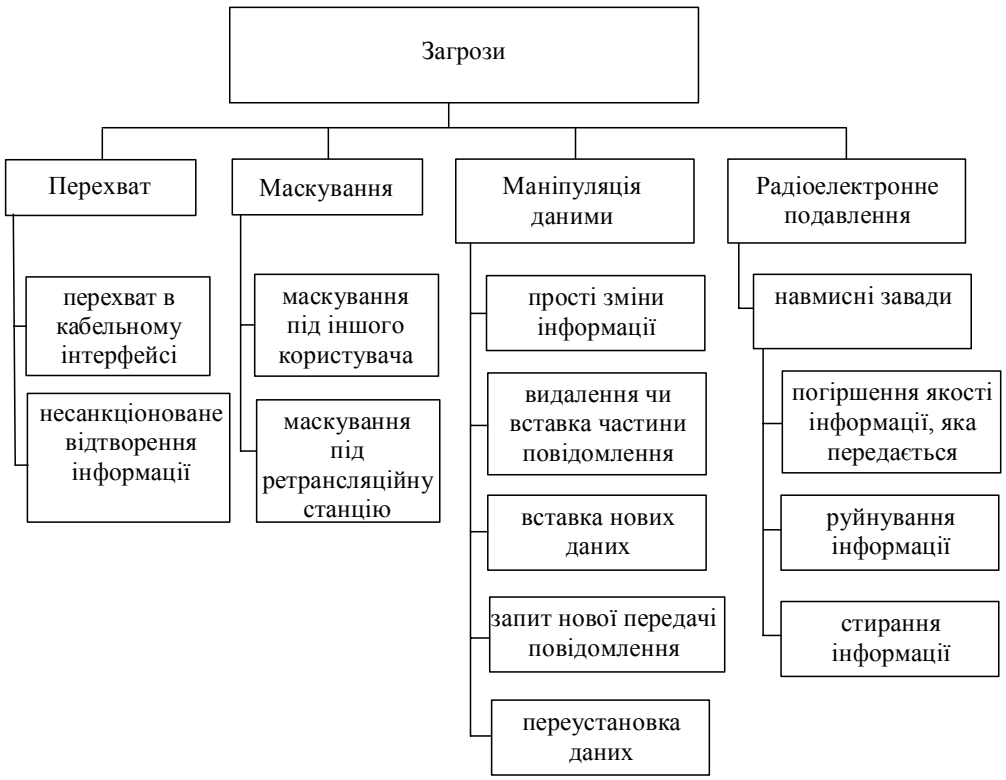

Рис. 2. Класифікація загроз повідомленням, які передаються в ІТС СП

Маскування під іншого користувача може здійснюватися як на радіо- так і на провідному інтерфейсі. Спеціальним випадком маскування виступає маскування під об'єкт системи на інтерфейсі, який не постійно встановлює з'єднання, типу міжсистемного інтерфейсу між двома системами доступу різних стандартів, зв'язаних через транзитну мережу. Важливо відзначити, що при маскуванні інтерес для зловмисника представляють, насамперед, службові дані, які відповідають за безпеку системи, тобто дані аутентифікації користувачів.

Можливими контрзаходами проти обох типів маскувань є ті ж самі процедури, що й у випадку перехоплення, тобто механізми шифрування й аутентифікаційні механізми. До того ж маскування під іншого користувача може бути виявлене за допомогою переустановлення даних.

До основних способів боротьби з маскуванням відносяться:

- взаємна аутентифікація через інтерфейс між РС і користувачем (кінцевим терміналом);
- шифрування інтерфейсу між РС і користувачем;
- шифрування між кінцевими точками;
- механізм передачі ключів;
- використання методів підвищення прихованості зв'язку.

Маніпуляції даними. У загальному випадку маніпуляції є видом загроз, які полягають у можливості несанкціонованої зміни інформації в системі. Це відноситься до всіх мереж зв'язку і до усіх видів переданої інформації.

У залежності від технічних можливостей зловмисника модифікація може досягати дуже високого рівня.

При цьому навіть не обов'язково розшифровувати повідомлення, можна просто їх відтворювати зі вставками.

Типовими об'єктами модифікацій стають дані управління, наприклад, дані ідентифікації відправника і (або) одержувача, місце його розташування, дані ідентифікації рівня

пріоритету, заголовки деяких даних. Ці модифікації можуть використовуватися для порушення інформації про маршрутизацію або з метою маскування під іншого користувача. При цьому зловмисник може змінювати дані управління, наприклад, організовувати ізоляцію деяких системних вузлів.

Загрози маніпуляції не можуть бути відвернені застосуванням алгоритмічних методів безпеки. У випадку таких загроз необхідно застосовувати методи, які можуть дозволити одержувачу інформації виявляти маніпуляції даними з високою ймовірністю.

Радіоелектронне подавлення. Однією з найважливіших вимог до ІТС СП є здатність успішно функціонувати в умовах впливу навмисних завад, ефект впливу яких позначається в погіршенні якості обробки інформації в результаті її руйнування або старіння, що збільшує ступінь невизначеності при прийнятті рішень.

У загальному випадку радіоелектронне подавлення (РЕП) включає два послідовних етапи – радіотехнічну розвідку і радіопротидію. Метою радіотехнічної розвідки є установлення факту роботи (випромінювання) системи і визначення її параметрів, необхідних для організації радіопротидії. Метою радіопротидії є постановка завад, дія яких максимально утрудняє роботу системи взагалі або призводить до порушення її нормального функціонування. Очевидно, що постановка завад буде тим ефективнішою, чим більше інформації про систему, яка подавлюється, буде виявлено на етапі розвідки.

Впливаючи на приймальні пристрої, завади імітують або спотворюють спостережувані апаратурою сигнали або зображення, затрудняють або виключають виділення корисної інформації, ведення переговорів, знижують дальність дії й точність роботи автоматичних систем управління. Під дією завад електронні засоби й системи можуть перестати бути джерелами інформації, незважаючи на їхню повну справність і працездатність.

Оскільки подавити різноманітні засоби зв'язку завадами одного виду неможливо, застосовують спеціальні види завад.

Для кожного виду завади слід вибрати спосіб передачі повідомлення, що забезпечує задану цілісність інформації (наприклад, інший вид передачі, направлену антену, дублювання напрямку декількома видами радіозв'язку і т.д.). Необхідно розрізняти забезпечення цілісності, обумовлене технічними можливостями каналів зв'язку протистояти навмисним і взаємним завадам, і забезпечення цілісності, що визначається організаційними заходами щодо радіоелектронного захисту системи в цілому.

Відповідно до функцій РЕП завадозахищеність системи передачі визначається її прихованістю і завадостійкістю. Прихованість системи передачі – це її здатність протистояти дії радіорозвідки. Радіотехнічна розвідка передбачає послідовне виконання трьох основних задач: виявлення факту роботи системи передачі (виявлення сигналу); визначення структури виявленого сигналу і його основних параметрів; розкриття інформації, яка міститься в сигналі. Відповідно до цих задач можна визначити три види прихованості: енергетичну, структурну та інформаційну. Завадостійкість – це здатність системи передачі протистояти шкідливому впливу завад. Аналіз завадостійкості здійснюється незалежно від причин появи завад у системі передачі.

Таким чином, для підвищення завадозахищеності систем передачі необхідно підвищувати їх прихованість і завадостійкість.

Застосовують наступні основні методи підвищення енергетичної і структурної прихованості системи передачі:

1. робота з мінімально необхідною потужністю випромінювання, достатньою для забезпечення необхідної якості зв'язку, використання радіосистем з адаптацією за потужністю випромінювання;

2. використання оптимальних способів приймання сигналів і пристроїв захисту (подавлення) від навмисних завад;

3. використання складних шумоподібних сигналів з великою базою. Такі сигнали, на відміну від простих, мають більш високу завадостійкість і прихованість, а отже і ефективність при забезпеченні цілісності переданої інформації;

4. використання частотно-адаптивних ліній зв'язку.

Таким чином, проведений аналіз дозволяє зробити наступні *висновки*.

В інформаційно-телекомунікаційних системах спеціального призначення основними загрозами канальній цілісності інформації є перехоплення, несанкціоноване відтворення інформації, маскування, маніпуляції даними та радіоелектронне подавлення.

Для захисту від порушень цілісності інформації необхідно застосовувати введення надмірності в саму інформацію, у процес її обробки, а також введення системної надмірності.

Поряд з криптографічними методами захисту інформації як один з основних напрямків забезпечення цілісності інформації в інформаційно-телекомунікаційних системах спеціального призначення заслуговує на увагу застосування методів підвищення прихованості зв'язку. Серед цих методів особливе місце займають шумоподібні сигнали, що дозволяють одночасно підвищити достовірність і прихованість передачі інформації. Застосування в інформаційно-телекомунікаційних системах спеціального призначення шумоподібних сигналів та інших методів забезпечення прихованості передачі сигналів дозволить підвищити рівень захищеності інформації від порушень цілісності та інших загроз.

ЛІТЕРАТУРА

1. Закон України „Про захист інформації в інформаційно-телекомунікаційних системах".
2. Постанова КМ України № 373 від 26.03.2006 „Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах".
3. Постанова КМ України №180 від 16.02.1997 „Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах".
4. Грушо А. А. Теоретические основы защиты информации / А. А. Грушо, Е. Е. Тимонина. – М.: Яхтсмен. – 1996. – 301 с.
5. Антонюк А. Загрози інформації і канали витоку / А. Антонюк, В. Жора // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. – Вип. 2. – С. 42–46.
6. Домарев В. В. Безопасность информационных технологий. Системний поход / В. В. Домарев. – К.: ООО „ТИД" „ДС", 2004. – 992 с.
7. Поповский В. В. Защита информации в телекоммуникационных системах: Учебник/ В. В. Поповский, А. В. Персиков. – Х.: ООО „Компания СМИТ", 2006. – 238 с.
8. Варакин Л. Е. Системы связи с шумоподобными сигналами / Л. Е. Варакин. – М.: Радио и связь, 1985. – 384 с.

Надійшла: 22.03.2013 р.

Рецензент: д.т.н., проф. Щербак Л.М.