УДК 621.391

ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ ФУНКЦІОНУВАННЯ НА КАНАЛЬНОМУ РІВНІ ВІДКРИТИХ МЕРЕЖ ПЕРЕДАЧІ ДАНИХ В УМОВАХ ЗАГРОЗ

Володимир Тарасенко, Сергій Коваль*

Національний технічний університет України "КПІ"

**Управління охорони державної таємниці СБ України*

Анотація: **Розглянуто імітаційну модель функціонування на канальному рівні в умовах інформаційних загроз мережі передачі даних відкритої системи обміну даними, приведено залежність ймовірності порушення цілісності інформації від ймовірності дії інформаційної загрози.**

Summary: **Functioning of imitation model on channel level under information threat conditions in open data exchange networks was investigated. Provided dependence of breaking integrity of the information and probability of information threat.**

Ключові слова: **Безпека інформації, інформаційне протиборство, загроза.**

I Вступ

Сучасність характерна стрімким впровадженням у всі сфери діяльності (науково-виробничу, фінансову, військово-технічну та інші) суспільства мереж передачі даних, побудованих на основі стандартів, протоколів та процедур відкритих систем обміну даними (OSI). Однією з вимог до функціонування таких мереж є забезпечення безпеки інформації, яка циркулює в них, в умовах інформаційного протиборства за наявності загроз, що викликають деструктивні зміни в інформації [1]. Зазначені деструктивні зміни в інформації можуть призводити до порушень у функціонуванні мереж, що визначає актуальність проблеми визначення впливу загроз на основні характеристики мереж передачі даних.

II Постановка задачи

Відомо, що загрози являють собою сукупність факторів ризику, що призводять до порушення цілісності, конфіденційності та доступності інформації, та характеризуються імовірнісними законами виникнення та впливу на інформацію [2]. Зважаючи на те, що інформація, яка циркулює в мережах передачі даних, з точки зору можливості реалізації загрози та внесення деструктивних змін, найбільш вразлива на канальному рівні виникає проблема вивчення функціонування мережі передачі даних на цьому рівні. Складність (розгалуженість за територією, часом, випадковість подій та обробки інформації та інше) побудови систем передачі даних обумовлює їх модельне дослідження з метою визначення основних показників функціонування цих систем.

Процес здійснення спеціального впливу на технічні засоби системи передачі даних, що призводить до реалізації загроз для інформації, складає інформаційне протиборство [1, 3]. При цьому під спеціальним впливом мається на увазі вплив на технічні засоби системи передачі даних, який призводить до здійснення загрози для інформації, яка циркулює в зазначеній системі [4].

З точки зору доступності до технічних засобів цифрової системи передачі даних найбільш доцільним є врахування припущення, що реалізація спеціального впливу відбувається в зовнішньому середовищі функціонування зазначеної системи, в якому неможливо забезпечити контроль за несанкціонованим доступом до її технічних засобів. Виходячи з цього реалізація спеціального впливу найбільш можлива на канальному рівні системи передачі даних. При цьому зовнішнє середовище розглядається як сукупність штучних та природних впливів з особливим визначенням штучних впливів на елементи та технічні засоби канального обладнання.

Розглянемо один з підходів до визначення впливу загроз на функціонування мережі передачі даних на канальному рівні.

III Основна частина

Одним із шляхів визначення впливу загроз на функціонування мережі передачі даних на канальному рівні є створення імітаційної моделі мережі передачі даних відкритої системи обміну даними, яка функціонує в умовах загроз. Зазначене припущення ґрунтується на тому, що імітаційне моделювання використовується як інструмент експериментального дослідження технічних систем, до яких відносяться системи передачі даних,

і застосовується у випадках складності цих систем, наявності випадкових факторів , які змінюються з часом, неможливості отримання результатів без використання електронно-обчислювальних машин.

Відомо [3], що у відкритих системах обміну даними, згідно з рекомендаціями МСЕ (Міжнародного Союзу Електрозв'язку), використовується семирівнева архітектура. Канальний рівень обміну даними є другим рівнем в такій ієрархії, який об'єднує правила та процедури з встановлення зв'язку між двома кінцями каналу (в прикладному розумінні – модемами, мережевими картами, тощо) та забезпечує високорівневе управління іншими протоколами. Протоколи канального рівня (ADCCP, SDLS та інші) забезпечують безпомилкову (з деякими граничними обмеженнями) передачу даних вищого рівня (мережевого) та процедуру завершення зв'язку, якщо в каналі зв'язку з'являються ушкодження або завади, які неприпустимі в роботі системи обміну даними. Передача даних на канальному рівні здійснюється кадрами, до складу яких входять службові поля та поля даних вищого рівня.

Стандартний формат кадру складається з полів поміток (на початку та в кінці кадру), адреси, сигналів контролю та управління, інформаційного поля та поля перевірки. Для обробки інформаційного потоку, контрольних сигналів та сигналів управління у відкритих системах обміну даними існують кадри інформаційного формату (кадри I), формату контролю та управління (кадри K) та формату N (невизначеного формату). Зазначені формати відрізняються наявністю інформаційного поля та поля перевірки (в форматах K та N вони відсутні), ознаками і завданнями того чи іншого символу відповідного розряду поля контролю та управління. Кадри K, в свою чергу, розподіляються на кадри готовності до приймання (позначимо як K1), неготовності до приймання (K2) та кадри відмови (K3) приймання всіх кадрів, починаючи з N(R).

Відомо [2], що в разі, коли система передачі даних зазнає на канальному рівні впливу загроз, які складають множину $A=\{\alpha_1, \alpha_2, ..., \alpha_n\}$, n – число, яке визначає максимальну кількість загроз. Кожна з загроз α_i, $i=\overline{1,n}$ змінює символи (у прикладному розумінні – інвертує їх) у відповідних розрядах полів кадру, що призводить, в свою чергу, до порушення цілісності інформації. Зміна (інверсія) символів носить ймовірносний характер, тому кожну з загроз α_i можна характеризувати відповідними ймовірностями впливу p_a на символи відповідних розрядів полів кадрів. Ймовірність порушення цілісності інформації в конкретному полі кадру I, N або K буде дорівнювати $P(A)=m/M$ для достатньо великих M , де m – довжина поля (байт), M – довжина кадру, за умови нормування $\sum_{j=1}^{L} P(A)_j = 1$, де L – загальна кількість полів в кадрах. В свою чергу порушення цілісності інформації призведе до помилки, виявлення якої передбачено протоколом канального рівня відкритої системи обміну даними. Якщо визначити подію виявлення помилки через B, ймовірність якої буде залежати від реалізації конкретних процедур підвищення достовірності інформації, то :

- в разі виявлення помилки з ймовірністю $P(B)$ - здійснюється її виправлення та, одночасно, збільшення часу передачі кадру;
- в разі невиявлення помилки з ймовірністю $1 - P(B)$ – вона призводить до множини наслідків порушень $\{W_к\}$, $k=\overline{1,Q}$, де Q – загальна кількість наслідків порушень цілісності інформації на канальному рівні відкритої системи обміну даними.

З врахуванням вищевикладеного було розроблено імітаційну модель функціонування мережі передачі даних на канальному рівні, реалізовану програмою з використанням мови програмування PASCAL для операційної системи Windows.

Особливістю імітаційної моделі є її універсальність з точки зору застосування для встановлення взаємозалежностей між ймовірностями порушення цілісності інформації, дії загрози, довжиною кадрів та їх кількістю, необхідною для передачі повідомлення. В моделі також враховано дію загрози на кадри контролю та управління, що дозволило здійснити імітування умов функціонування мережі передачі даних на канальному рівні, найбільш наближених до реальних.

Як приклад можливості експериментального дослідження імітаційна модель була використана для встановлення співвідношення між ймовірністю дії загрози $P(A)$ та ймовірністю порушення цілісності інформації в полях інформаційного кадру $P(B)$ (рис. 1).

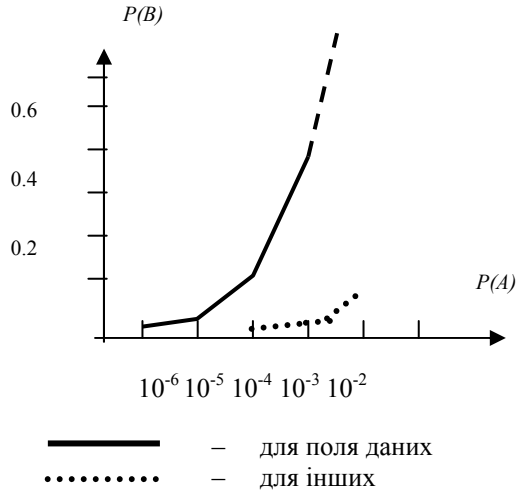

Рисунок 1– Залежність ймовірності порушення цілісності інформації в полях інформаційного кадру *P(B)* від ймовірності дії загрози *P(A)*

IV Висновок

Запропонована імітаційна модель дозволяє здійснювати прогнозування порушень безпеки інформації, яка циркулює в мережі передачі даних на канальному рівні відкритої системи обміну даними, за наявності апріорно заданих інформаційних загроз.

Література : 1. Гаценко О. Ю. Об оптимизации пакетов передачи данных в условиях информационного противоборства. // Электронное моделирование.—2000. Т. 22.– № 5.— С. 115 – 119. 2. Тарасенко В. П., Коваль С. М. Модельне прогнозування на канальному рівні характеристик відкритих систем обміну даними в умовах загроз. // Реєстрація, зберігання і обробка даних. – 2000, Т. 2.– № 4. – С. 82 – 90. 3. НД ТЗІ 1.1-003-99. Нормативний документ системи технічного захисту інформації. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. 4. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни і визначення. 5. Шварц М. Сети связи: протоколы, моделирование и анализ. – М.: Наука, 1992. – Ч. 1. – 336 с.

УДК 681.3.06

ИНТЕГРИРОВАННЫЕ МОДУЛИ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

Геннадий Гулак*, Виталий Вервейко, Юрий Горбенко, Сергей Полчанинов
**ДСТСЗИ СБУ, ХНУРЭ*

Анотація: **Розглядається задача створення інтегрованих модулів криптографічного перетворення та їх застосування.**
Summary: **The task of integrated crypto modules development and implementation is considered.**
Ключевые слова: **Система защиты информации, криптопровайдер, модуль криптографических преобразований.**

Введение

В настоящее время быстро расширяется спектр программного обеспечения, использующего средства криптографической защиты информации. Криптографические средства все более усложняются, что приводит к резкому усложнению программных продуктов, которые их используют. При появлении новых криптографических алгоритмов и стандартов приходится переделывать значительный объем программного обеспечения в соответствии с требованиями новых стандартов. В результате возникает задача упрощения применения средств криптографической защиты информации и упрощения перехода от использования одних