УДК 004.056
О. А. ЛАПТЄВ, канд. техн. наук, ст. наук. співробітник,
Державний університет телекомунікацій, Київ

МОДЕЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ МАРКОВСЬКИХ ВИПАДКОВИХ ПРОЦЕСІВ

Обґрунтовано та запропоновано математичний апарат, в якому за елемент інформаційної безпеки беруть не загрози несанкціонованого знімання інформації (атаки), а загрози — можливість знімання інформації уразливості. Більшість відомих підходів до моделювання різняться тим, які параметри при моделюванні ними застосовуються як вхідна інформація, а також які характеристики модельованої системи розраховуються і надходять на вихід моделі (будуються моделі з використанням теорії ймовірностей, випадкових процесів, мереж Петрі, теорії автоматів, теорії графів, нечітких множин, теорії катастроф, ентропійного підходу і т. ін.). У таких підходах за найпростіший елемент безпеки беруть загрозу атаки на інформаційну систему [3]. Як параметри загрози уразливості розглянута інтенсивність λ виникнення уразливості і інтенсивність μ усунення уразливості. Під виникненням уразливості (тут і далі) природно розуміємо її виявлення порушником безпеки. Припускаючи, що система містить кінцеву (нехай і дуже велику) кількість не виявлених уразливостей, можемо сказати, що в даному разі процес не є марковським, оскільки виявлення та усунення уразливості кожної призводить до зміни їх кількості на кінцевому вихідної множини, тобто маємо процес із післядією.

Розглянуто математичний апарат для моделювання систем із відмовами і відновленням (виявлення каналів витоку інформації і запобігання знімання інформації по цих каналах), з характеристиками безпеки. Виконано розрахунки за зазначеною методикою для різних значень ρ (де $\rho = \lambda/\mu$, λ–виникнення уразливості і μ–усунення уразливості).

Ключові слова: математичний апарат; моделювання систем; знімання інформації; атаки; загрози; уразливості.

Вступ

Постановка завдання. На сучасному етапі розвитку науки і техніки захист інформації дедалі помітніше набуває ознак одного з найактуальніших завдань сьогодення внаслідок надзвичайно широкого розповсюдження як систем обробки інформації, так і розширення локальних та глобальних комп'ютерних мереж, якими передаються величезні обсяги інформації державного, військового, комерційного, приватного характеру. Тому важливим завданням є забезпечення безпеки та захисту інформації, що неможливо гарантувати без будування моделі захисту або схем побудов систем інформаційної безпеки. Отже, розробка методики вибору схем систем безпеки є дуже актуальною.

Основна частина

Будь-яка модель захисту інформації не може претендувати на повну гарантію від злому. Це тільки певний абстракт, мета якого описати загальну термінологію і критерії системи безпеки. Модель не дає відповіді на питання, як безпечніше будувати систему, як нарощувати окремі компоненти і конфігурацію в цілому.

Починаючи з 1977 року, було запропоновано величезну кількість абстрактних моделей захисту інформації. Найпопулярніші з них — модель Біба (1977 р.), Сазерландская модель (1986 р.), модель Гогена-Мезігера (1982 р.), модель Кларка-Вілсона (1987 і 1989 рр.).

Відмінною особливістю пропонованого математичного апарату є використання як елемента інформаційної безпеки не загрози несанкціонованого знімання інформації (атаки), а загрози — можливості знімання інформації уразливості.

Під ***загрозою інформаційної безпеки*** розуміється сукупність умов і чинників, що створюють потенційну або реально існуючу небезпеку отримання несанкціонованого доступу до інформації порушником. Під ***уразливістю***, що є джерелом загрози — різні канали доступу до інформаційної системи, що зумовлює виникнення загрози безпеки інформації, під ***атакою*** — спроба подолання системи захисту інформаційної системи [1], тобто спроба реалізації загрози, створюваної уразливістю. Природно, що атака передбачає використання (експлуатацію) уразливостей.

Із урахуванням того, що під безпекою інформації розуміється [1] стан захищеності інформації, при якому забезпечені її конфіденційність, доступність і цілісність, має сенс відповідно класифікувати загрози (конфіденційність, цілісність і доступність інформації) і атаки (за реалізованими цілями здійснення несанкціонованого доступу).

Несанкціонований доступ — це доступ до інформації або до ресурсів інформаційної системи, здійснюваний із порушенням встановлених прав і/або правил доступу [2]. Тобто, несанкціонований доступ — це результат атаки, що реалізовується з деякою метою, тобто з метою розкриття конфіденційності інформації, порушення її цілісності або доступності.

Більшість відомих підходів до моделювання різняться тим, які параметри при моделюванні

ними використовуються як вхідна інформація і які характеристики модельованої системи розраховуються і надходять на вихід моделі (моделі з використанням теорії ймовірностей, випадкових процесів, мереж Петрі, теорії автоматів, теорії графів, нечітких множин, теорії катастроф, ентропійного підходу та ін.). У таких підходах за найпростіший елемент безпеки беруть загрозу атаки на інформаційну систему [3].

Практична застосовність подібних моделей вкрай ускладнюється необхідністю експертного завдання ключової характеристики безпеки — імовірності виникнення загрози атаки.

При моделюванні, в якому за найпростіший елемент безпеки беруть загрози атаки, виникнення різних загроз атак розглядається як незалежні події, а отже, використовуються відповідні розрахункові формули. Однак таке вихідне посилання некоректне, оскільки реальні загрози атак стають у системі уразливими, при цьому події виникнення загроз атак, як правило, залежні уразливості через використання багатьма атаками одних і тих самих уразливостей. Оскільки виникнення і усунення уразливостей із певними застереженнями можна інтерпретувати як виникнення й усунення відмови (у даному разі характеристики безпеки інформаційної системи), можна припустити, що для вирішення завдань моделювання відмов і відновлень характеристики безпеки може бути використано математичний апарат теорії надійності. Проте в теорії надійності завдання моделювання власне у своєму трактуванні принципово різниться. Там немає поняття порушника інформаційної безпеки, що здійснює цілеспрямований вплив на систему, немає відмінностей у цілях такого впливу, як порушення конфіденційності, цілісності і доступності оброблюваної інформації і т. ін. Отже, з огляду на те, що і в теорії надійності, і в теорії інформаційної безпеки існують у чомусь схожі поняття відмов, потенційно математичний апарат теорії надійності може бути використаний у теорії інформаційної безпеки для розглядуваних задач моделювання, але з істотною адаптацією під особливості вирішуваних завдань із виявлення й усунення каналів витоку інформації.

Статистика щодо виявлення та усунення уразливості ведеться безперервно. Вона відома і доступна, їх стохастичні параметри можуть бути визначені, дає змогу проводити стосовно загроз уразливостей відповідний імовірнісний аналіз. Таким чином, оцінка актуальності уразливості, яка визначається мірою критичності уразливості, сформованою відомими підходами до оцінювання, з огляду на складність її виявлення, використання і цілі експлуатації зловмисником, дозволяє дійти висновків про необхідність і екстреність прийняття будь-яких заходів щодо виявленої уразливості, зокрема будь-яких організаційних заходів. Але при цьому у жодному разі не йдеться про стохастичні властивості виявлення й усунення уразливостей, що не дає змоги спрогнозувати подальше виявлення будь-яких видів уразливостей, тим самим уможливлюючи реалізацію атак відповідних типів у процесі функціонування системи.

Уразливості (канали витоку інформації) за своєю суттю різнорідні. Деякі у разі їх виявлення не створюють реальної загрози доти, доки порушником не вжито відповідних дій, що призведуть до реальної загрози, наприклад відсутність обладнання, здатного здійснити атаку на виявлену уразливість.

У теорії надійності для моделювання систем із відмовами і відновленням (у даному разі — виявлення аналога витоку інформації і запобігання знімання інформації по цих каналах) об'єктів — характеристики надійності, як правило, використовується апарат марковських випадкових процесів за припущень про пуассонівський характер потоку заявок і про показовий розподіл часу обслуговування [3]. Як відомо, процес, що відбувається в фізичній системі, називається марковским (або процесом без післядії), якщо для кожного моменту часу ймовірність будь-якого стану системи в майбутньому залежить тільки від стану системи в даний момент часу і не залежить від того, у який спосіб система дійшла до цього стану. Розглянемо, чи може використовуватися (чи коректне використання, а якщо коректне, то як можуть інтерпретуватися здобуті при моделюванні результати) даний математичний апарат у нашому випадку — для моделювання систем з відмовами і відновленням (виявлення каналів витоку інформації і запобігання зніманню інформації по цих каналах), але вже з характеристиками безпеки.

Проаналізуємо, що являють собою уразливості, виявлення яких у системі створює реальну загрозу атак. Виникнення уразливості в інформаційній системі може бути спричинено або відсутністю чи некоректністю вирішення відповідної задачі захисту, або помилками у реалізації засобів інформаційного захисту, які можуть експлуатуватися порушником задля уникнення захисту. Як параметри загрози уразливості розглядаємо інтенсивність λ виникнення уразливості та інтенсивність μ усунення уразливості. Під виникненням уразливості (тут і далі) природно розуміємо її виявлення порушником безпеки. Припускаючи що система містить кінцеву (нехай і дуже велику) кількість не виявлених уразливостей, можемо сказати, що в даному разі процес не є марковським, оскільки виявлення та усунення уразливості кожної призводить до зміни їх кількості на кінцевій

вихідній множині, тобто маємо процес із післядією. При цьому вхідний потік не буде пуассонівським, оскільки в цих припущеннях $\lambda \neq \text{const}$. Далі оцінимо, як будуть змінюватися параметри уразливості в процесі експлуатації інформаційної системи. Вочевидь, що в загальному випадку інтенсивність λ виникнення уразливості через деякий час буде знижуватися, оскільки насамперед порушник буде вишукувати найбільш прості недоліки функціональної реалізації захисту (збільшення складності виявлення уразливості природно призведе до зниження інтенсивності λ). Стосовно параметра μ можна сказати, що він ніяк не пов'язаний зі складністю виявлення уразливості порушником безпеки і визначається виключно типом уразливості (наприклад, помилки у виборі систем захисту за віброакустичним каналом вимагають різної трудомісткості усунення), тобто для кожного типу уразливості можемо взяти: $\mu = \text{const}$.

Припустимо, що ми спроектували систему захисту, застосувавши формальну екстраполяцію (прогнозна екстраполяція тут мало застосовна з огляду на високу інтенсивність переходів на нові види захисту в сучасних інформаційних системах) із використанням марковської моделі. Тим самим при моделюванні ми припустили, що потік без післядії, тобто інтенсивності λ виникнення уразливості і μ усунення уразливості будуть незмінні в процесі подальшої експлуатації захищеної інформаційної системи. Очевидно, що значення λ буде тільки зменшуватися, а μ залишиться тим самим у подальшій експлуатації системи. Використовуючи таку модель, ми знайдемо граничні (за найгірших для системи умов) значення необхідних характеристик, облік яких гарантує, що «гірше не буде». Отже, можна дійти дуже важливого висновку: при моделюванні характеристик загрози безпеки інформаційної системи можна використовувати марковські моделі, які дозволяють у даному разі визначати граничні значення характеристик безпеки, що і мають бути застосовані під час проектування системи захисту в припущенні неможливості побудови коректного прогнозу щодо зміни значень параметрів загроз, уразливостей у часі. Беручи до уваги, що ймовірністю одночасної появи в системі кількох однотипних уразливостей (не одночасної присутності, саме виникнення реальних загроз, уразливостей) можемо знехтувати, процес виникнення та усунення в системі загрози уразливості може бути описаний схемою «загибелі і розмноження» [3].

Марковський неперервний ланцюг називається «процесом загибелі і розмноження», якщо його граф станів витягнути в один ланцюжок, у якому кожне із середніх станів (S_2, …, S_{n-1}) пов'язано прямим і зворотним зв'язком із кожним із сусідніх станів, а крайні стану (S_1, S_n) — тільки з одним сусіднім станом. Тоді для випадку одного об'єкта обстеження шукана характеристика безпеки — стаціонарний коефіцієнт готовності (у цьому разі готовність до безпечної експлуатації стосовно загрози, уразливості) визначається так: $P_{oy} = 1 - \rho$, де $\rho = \lambda/\mu$, а ймовірність наявності в системі одночасно R не усунених недоліків (реальних загроз, уразливостей): $P_{Ry} = \rho^R(1 - \rho)$. За групу фахівців, що перевіряють приміщення, у нашому випадку було взято колектив фахівців, які усувають виявлену уразливість у системі з інтенсивністю μ. На практиці одночасно можна усунути кілька уразливостей, тобто в загальному випадку слід розглядати схему «загибелі і розмноження». Для такої моделі шукана характеристика обчислюється за формулою [2]

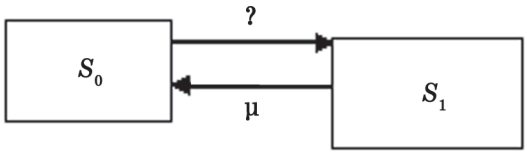
$$P_{oy} = \left(1 + \rho + \frac{\rho^2}{2!} + \ldots + \frac{\rho^C}{C!}\right)^{-1},$$

а ймовірність наявності в системі одночасно R не усунених недоліків визначатиметься як $P_{Ry} = \frac{\rho^C}{C!} P_{oy}$.

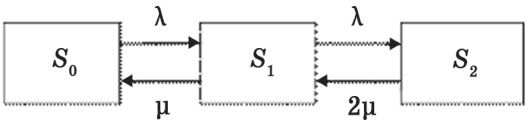
Зазначимо, що загроза уразливості в даному випадку моделюється як найпростіший або базовий елемент безпеки інформаційної системи. Далі потрібно моделювання вже більш складного елемента — загрози атаки, створюваної погрозами уразливості, а зрештою — загрози безпеки інформаційної системи в цілому, створюваної погрозами атак. З урахуванням цього, для спрощення подальших моделей оцінимо, яка кількість обслуговувальних приладів слід розглядати при моделюванні загрози уразливості і за яких умов. Можна припустити, що за умови $\rho = \lambda/\mu << 1$ значення ймовірності $P_{R>1y}$ мале і їм можна знехтувати. Оцінимо вплив на результати моделювання характеристики P_{Ry}, для чого розглянемо залежність значень характеристики P_{Ry} від зміни значень параметра ρ для одноканальної $C = 1$ та двоканальної $C = 2$ систем. Графи станів випадкового процесу виявлення і усунення уразливостей (марковського процесу з дискретними станами і неперервним часом), які нами далі будуть використовуватися, зображено на рисунку, де S_0 — початковий стан системи; S_1 — у системі виявлено і не усунено одну з уразливостей; S_2 — у системі виявлено і не усунуто дві уразливості.

Розрахункові дані для розглянутих систем наведено відповідно в табл. 1 і табл. 2.

Проаналізувавши результати, наведені в таблицях, доходимо таких висновків. За умови $\rho \leq 0{,}2$ при моделюванні загрози уразливості може використовуватися одноканальна система безпеки інформації, а за умови $\rho > 0{,}2$ має застосовуватися двоканальна система безпеки інформації.



За умови $\rho \le 0,2$



За умови $\rho > 0,2$

Графи системи станів випадкового процесу для загрози уразливості

Таблиця 1

Характеристики одноканальної системи ($C = 1$)

P_{Ry}	ρ							
	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8
P_{0y}	0,90	0,80	0,70	0,60	0,50	0,40	0,30	0,20
P_{1y}	0,09	0,16	0,21	0,24	0,25	0,24	0,21	0,16
$P_{R\ge 3y}$	0,01	0,04	0,09	0,16	0,25	0,36	0,49	0,64

Таблиця 2

Характеристики двоканальної системи ($C = 2$)

P_{Ry}	ρ						
	0,3	0,4	0,5	0,6	0,7	0,8	0,9
P_{0y}	0,74	0,68	0,62	0,56	0,51	0,47	0,43
P_{1y}	0,22	0,27	0,31	0,34	0,36	0,38	0,39
P_{2y}	0,03	0,05	0,07	0,10	0,13	0,15	0,18
$P_{R\ge 3y}$	0	0	0	0	0	0	0

Висновки

Здійснивши обчислення за зазначеною методикою для різних значень ρ (де $\rho = \lambda/\mu$, λ — виникнення уразливості і μ — усунення уразливості), дійшли висновків, що для забезпечення безпеки інформації при $\rho \le 0,2$ може використовуватися одноканальна система, а для $\rho > 0,2$ — двоканальна. Таким чином, використовуючи наведений підхід до моделювання, а саме, якщо за елемент інформаційної безпеки беруть не загрози несанкціонованого знімання інформації — атаки, а загрози — можливості отримання інформації уразливості, із застосовуваними нами допущеннями з використанням теорії на основі марковських випадкових процесів, можна визначити структуру системи з необхідним рівнем інформаційної безпеки ще на першому підготовчому етапі.

Список використаної літератури

*1. **Щеглов К. А., Щеглов А. Ю.** Эксплуатационные характеристики риска нарушений безопасности информационной системы // Научно-технический вестник информационных технологий, механики и оптики. 2014. №1(89). С. 129–139.*

*2. **Щеглов К. А., Щеглов А. Ю.** Математические модели эксплуатационной информационной безопасности // Вопросы защиты информации. 2014. Вып. 106. № 3. С. 52–65.*

*3. **Вентцель Е. С.** Исследование операций. Москва, 1972. 566 с.*

Рецензент: канд. техн. наук, доцент **С. В. Довбешко**, Державний університет телекомунікацій, Київ.

А. А. Лаптев

МОДЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ МАРКОВСКИХ СЛУЧАЙНЫХ ПРОЦЕССОВ

Обосновано и предложено математический аппарат, в котором в качестве элемента информационной безопасности принимают не угрозы несанкционированного съема информации (атаки), а угрозы — возможности съема информации уязвимости. Большинство известных подходов к моделированию, отличающиеся тем, какие параметры при моделировании ими используются как входная информация, а также какие характеристики моделируемой системы рассчитываются и поступают на выход модели (строятся модели с использованием теории вероятностей, случайных процессов, сетей Петри, теории автоматов, теории графов, нечетких множеств, теории катастроф, энтропийного подхода и т. д.), предусматривает использование в качестве простейшего элемента безопасности угрозу атаки на информационную систему [3]. В качестве параметров угрозы уязвимости рассматриваем интенсивность λ возникновения уязвимости и интенсивность μ устранения уязвимости. Под возникновением уязвимости (здесь и далее) естественно понимаем ее обнаружение нарушителем безопасности. Предполагая, что система содержит конечное (пусть и очень большое) количество не обнаруженных уязвимостей, можем сказать, что в данном случае процесс не марковский, поскольку выявление и устранение уязвимости каждой приводит к изменению их числа на конечном исходного множества, то есть наблюдается процесс с последействием.

Рассмотрен математический аппарат для моделирования систем с отказами и восстановлением (выявление каналов утечки информации и предотвращения съема информации по этим каналам), с характеристиками безопасности. Проведены расчеты по указанной методике для различных значений ρ (где $\rho = \lambda/\mu$, λ — возникновения уязвимости и μ — устранение уязвимости).

Ключевые слова: математический аппарат; моделирование систем; съем информации; атаки; угрозы; уязвимости.

A. A. Laptev

THE MODEL OF INFORMATION SECURITY BASED ON MARKOV RANDOM PROCESSES

In this article rotary and propozed mathematical apparatus which as part of the information security are not the threat of unauthorized removal of information — attack and threats — the possibility of eavesdropping vulnerability. Most of the known modelling approaches that differ in which parameters in the simulation they are used as the input information and the characteristics of the simulated system are calculated and sent to the model (models are Built using probability theory, stochastic processes, Petri nets, automata theory, graph theory, fuzzy sets, catastrophe theory, entropy approach, etc.), provides for the use as a simple safety feature the threat of an attack on an information system [3].

The practical applicability of such models is extremely complicated through the necessity of the expert of the task key characteristics of safety — probability of threat of attack.

In the simulation, based on the use of as the simplest element of security threats attacks threats attacks is regarded as independent events; therefore, use appropriate calculation formulas. However, this original promise is wrong, because the real threats of attack created in the system are vulnerable, while the events of the threats of attacks, as a rule, dependent sensitivity because many attacks use the same vulnerability. Because of emergence and elimination of sensitivity with certain reservations, can be interpreted as the occurrence and elimination of failures (in this case, the security characteristics of the information system), we can assume that to solve these problems, modeling simulation of failures and recoveries safety features — can be used mathematical apparatus of reliability theory. As parameters in the vulnerability threat considering the intensity of occurrence of vulnerability λ and intensity of vulnerability μ. Under the appearance of vulnerability (here and beyond) naturally understand its detection by the security breach. On the one hand, assuming that the system contains a finite (albeit very large) number of undiscovered vulnerabilities, I can say that in this case, the process is not Markov, since the identification and elimination of vulnerabilities of each leads to change their numbers on a finite initial set, i. e. have a process with aftereffect.

Will sight, the mathematical apparatus for simulation of systems with refusals and restoration (identifying channels of information leakage and prevention of information acquisition through these channels), with the safety features. Had calculated on this method for different values of ρ (where $\rho = \lambda/\mu$, λ — the emergence of vulnerability and μ — vulnerability).

Keywords: mathematical apparatus; systems modeling; information retrieval; attack; threat; vulnerability.

УДК 621.391.8

В. Л. ПАРХОМЕНКО, канд. техн. наук, доцент;
М. С. ІЛЬЄНКО, магістр;
В. В. ПАРХОМЕНКО, здобувач;
В. С. КРИВОБОК, магістр;
О. А. ОГОРОДНІК, магістр,
Державний університет телекомунікацій, Київ

ДОСЛІДЖЕННЯ ПОБУДОВИ ТА МЕТОДУ РОЗРАХУНКУ ПЕРЕДВИХІДНОГО КАСКАДУ ЦИФРОВОГО ПЕРЕДАВАЧА

Запропоновано побудову підсилювача потужності цифрового передавача з високими якісними характеристиками. Наведено схеми передвихідного і вихідного каскадів. Розрахунок режимів підсилювачів дозволяє домогтися заданих якісних показників підсилювача потужності при високому ККД.

Ключові слова: підсилювач потужності; схеми передвихідного каскада; схема вихідного каскада; ККД; режими підсилювачів.

Вступ

Упровадження цифрового телебачення та радіомовлення вимагає від передавального обладнання більш високих якісних характеристик порівняно з аналоговим мовленням. Усе жорсткіші вимоги висуваються до якісних характеристик підсилювачів потужності, а саме до нелінійних спотворень, АЧХ та ФЧХ. Досягти цього можна, здійснивши розрахунки передвихідного та вихідного каскадів.

Вихідний каскад

Вихідний каскад побудовано на двох модулях, потужності яких складаються за допомогою мостової схеми. Кожний із модулів містить підсилювач телевізійних радіочастотних коливань, побудований за схемою Догерті. Беручи до уваги, що симетрична схема Догерті будується як двоканальна, то вельми доцільним є використання балансного транзистора MRFE6VP8600HR6, який складається з сформованих на одному кристалі двох польових транзисторів і віддає у навантаження корисну середню потужність 125 Вт.

Принципову схему модуля вихідного каскаду наведено на рис. 1.