симметричные и асимметрические алгоритмы шифрования, обеспечивающие аутентичность и целостность сообщений. Разработанные математические модели позволяют оценить степень эффективности основных типов атак, что облегчает выбор необходимых средств и методов защиты информации в ВПБС. Перспективным направлением дальнейших исследований является разработка методики оценки экономического ущерба, нанесенного в результате реализации угроз на информационные ресурсы ВПБС.

СПИСОК ЛИТЕРАТУРЫ

1. Украинский ресурс по безопасности [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://kiev-security.org.ua. – Загл. с экрана.
2. Дело [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://delo.ua/wiki/Glossary/vnutribankovskaja-platezhnaja-sistema-130342. – Загл. с экрана.
3. *Кузнецов А. А.* Анализ механизмов обеспечения безопасности банковской информации во внутриплатежных системах коммерческого банка / А. А. Кузнецов, О. Г. Король, А. М. Ткачов // Матеріали І міжнародної науково-практичної конференції «Безпека та захист інформації в інформаційних і телекомунікаційних системах», 28–29 травня 2008 р. Зб. наук. статей «Управління розвитком». – Х. : ХНЕУ, 2008. – № 6. – С. 28–35.
4. *В. Столлингс.* Криптография и защита сетей: принципы и практика : пер. с англ. – 2-е изд. – М. : Вильям, 2001. – 672 с.
5. Глоссарий [электронный ресурс]. – Электрон. дан. – Режим доступа: http://www.glossary.ru. – Загл. с экрана.
6. *Кузнецов О. О.* Захист інформації та економічна безпека підприємства : монография / О. О. Кузнецов, С. П. Євсеєв, С. В. Кавун. – Х. : ХНЕУ, 2008. – 360 с.

Надійшла 08.09.2009

Євсеєв С. П., Король О. Г., Гончарова А. І.

ПОБУДОВА МОДЕЛЕЙ АТАК НА ВНУТРІШНЬОПЛАТІЖНІ БАНКІВСЬКІ СИСТЕМИ

Аналізуються погрози інформаційних даних у внутрішньоплатіжних банківських системах (ВПБС). Розробляються модель реалізації погроз інформаційних даних у ВПБС, математичні моделі пасивної і активної атак, досліджуються основні напрями захисту у ВПБС.

Ключові слова: погрози, внутрішньоплатіжна банківська система, математична модель, модель реалізації погроз, пасивна атака, активна атака, захист, шифрування, автентичність, цілісність.

Evseev S. P., Korol O. G, Goncharova A. I.

MODEL-BUILDING OF ATTACKS ON INTERNAL-PAYMENT BANKING SYSTEM

Threats to information data in an internal-payment banking system (IPBS) are being analyzed. The realization model of information data threats in IPBS as well as the mathematical models of passive and active attacks are being developed. The general protection areas in IPBS are being studied.

Key words: threats, internal-payment banking system, mathematical model, realization model of threats, passive attack, active attack, protection, encoding, authenticity, integrity.

УДК 621.391

Калекина Т. Г.[1], Коваленко Т. Н.[2]

[1]Канд. техн. наук, доцент Харьковского национального университета радиоэлектроники

[2]Канд. техн. наук, доцент Харьковского национального университета радиоэлектроники

ОБОСНОВАНИЕ КРИТЕРИЯ СТРУКТУРНО-ИНФОРМАЦИОННОЙ СВЯЗНОСТИ ПРИ АНАЛИЗЕ НАДЕЖНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ

В работе предложены комплексные показатели надежности телекоммуникационных систем и сетей, учитывающие одновременно как структурные, так и функциональные характеристики сети. Предложенные показатели позволяют оценить не только потенциальную надежность телекоммуникационной сети – верхнюю границу структурной надежности, но и надежность сети с учетом ограниченной пропускной способности каналов.

Ключевые слова: надежность, структурная связность, информационная связность, интегральный показатель, граф, телекоммуникационная сеть.

Вопросы анализа надежности сложных разветвленных телекоммуникационных систем и сетей (ТКС) всегда были в центре внимания проектировщиков перспективных систем связи. Под структурной надежностью сети связи понимается объективное свойство сети обеспечивать связность пользователей сети с качеством не хуже заданного. Без средств анализа надежности ТКС отдел информационных технологий предприятия не сможет ни проконтролировать, ни тем более обеспечить необхо-

димый уровень обслуживания для конечных пользователей сети. Результаты анализа производительности и надежности позволяют контролировать соглашение об уровне обслуживания (Service Level Agreement, SLA), заключаемое между пользователем сети и ее администраторами. Обычно в SLA оговариваются такие параметры надежности, как коэффициент готовности службы в течение года и месяца, максимальное время устранения отказа, а также параметры производительности, средняя и максимальная пропускная способность при соединении двух точек подключения пользовательского оборудования, время реакции сети, максимальная задержка пакетов при передаче через сеть [1, 2]. При этом одной из актуальных задач является выбор и обоснование комплексных показателей, позволяющих наиболее полно оценить надежность телекоммуникационной системы. В качестве критерия оценки надежности ТКС целесообразно взять такой показатель, который, с одной стороны, больше всего отвечает целевому предназначению сети, а с другой – дает возможность переходить к оценке качества функционирования высших звеньев иерархии некоторой сложной системы, в область управления которой телекоммуникационная сеть входит как составляющая.

Количественно надежность сложных технических систем, к которым относятся и телекоммуникационные системы, можно охарактеризовать рядом показателей: наличием в заданных двухполюсных сетях направлений связи, математическим ожиданием количества этих путей, отношением количества исправных ребер к их общему количеству, мощностью простого минимального сечения множества – минимальной совокупности элементов, отказ которых нарушает связность [3, 4]. В основе всех перечисленных выше показателей положен один факт: наступление события связности или несвязности. Поэтому в качестве интегрального критерия надежности связи обычно используется критерий структурной связности, который определяется следующим образом: надежностью связи между узлами X_k и X_l называется вероятность $P_{k,l}$ того, что работоспособным является хотя бы один путь из множества путей на графе сети между данными узлами. Реальные телекоммуникационные сети могут представлять собой довольно сложную структуру, поэтому используются приближенные методы, позволяющие определить верхние и нижние границы структурной надежности [4].

Под отказом канала связи понимается такое состояние, при котором оборудование канала полностью вышло из строя, либо его параметры настолько ухудшились, что дальнейшее использование канала невозможно. Под отказом узла коммутации понимается невозможность передачи через него информации от входящих каналов на исходящие. Такой отказ эквивалентен одновременному отказу всех ребер, инцидентных этому узлу. Отказ узла приводит к нарушению значительно большего числа путей, чем отказ ребра, однако вероятность такого события значительно меньше вероятности отказа ребра. Поэтому при оценке структурной надежности связей будем рассматривать только влияние ребер, считая, что надежность узлов $p_i = 1$. Под надежностью $p(l_{ij})$ ребра l_{ij} будем понимать вероятность нахождения ребра в состоянии работоспособности.

Простейшими формулами вычисления надежности структур последовательного и параллельного соединения ненадежных элементов являются следующие:

$$P_{k,l} = \prod_{i=1}^{m} p_i, \qquad (1)$$

$$P_{k,l} = 1 - \prod_{i=1}^{n} q_i, \qquad (2)$$

где m, n – число элементов, соединенных последовательно и параллельно, соответственно; p_i – надежность i-го элемента; q_i – вероятность отказа i-го элемента.

Суть практически всех методов вычисления $P_{k,l}$ так или иначе заключается в реализации некоторых преобразований исходного графа двухполюсной сети, приводящих либо к простейшему последовательному, либо параллельному соединению элементов [3, 4]. Самым простым методом вычисления вероятности связности является метод, основанный на разложении структуры сети относительного какого-нибудь его элемента (метод разложения Шеннона – Мура).

Критерий структурной связности не может в полной мере характеризовать надежность связи, т. к. он не учитывает алгоритмы функционирования сети, в частности, алгоритм выбора исходящих направлений на узлах в процессе установления соединений. Поэтому для оценки надежностных характеристик сети в целом рассмотрим критерий структурно-информационной связности и критерий информационной надежности, характеризующие качество обслуживания запросов (вызовов) в условиях ненадежности элементов сетей.

Под вероятностью структурно-информационной связности между двумя фиксированными узлами сети, при наличии между ними потока информации, понимается вероятность того, что в заданном интервале времени при поступлении очередного запроса

на передачу информации в процессе поиска установления соединения найден хотя бы один исправный путь между данными узлами.

В качестве критерия структурно-информационной связности от узла X_k к узлу X_l вводится показатель

$$H_{k,\,l} = \frac{Y_{kl}^{\text{вх}} - Y_{kl}^{\text{пот}}}{Y_{kl}^{\text{вх}}}, \qquad (3)$$

где $Y_{kl}^{\text{вх}}$ – поток, поступивший на обслуживание от узла X_k к узлу X_l; $Y_{kl}^{\text{пот}}$ – необслуженный (потерянный) поток при организации связи от узла X_k к узлу X_l.

При определении $H_{k,\,l}$ учитывается алгоритм обслуживания поступающих запросов на узлах сети. Для случая, когда используется алгоритм установления соединения с возвратом на уже пройденные узлы и повторным поиском пути, т. е., если для организации связи между узлами сети допускается перебор всех возможных путей между ними, показатель $H_{k,\,l}$ определяется соотношением

$$H_{k,\,l} = \frac{Y_{kl}^{\text{вх}} - Y_{kl}^{\text{пот}}}{Y_{kl}^{\text{вх}}} = \frac{Y_{kl}^{\text{вх}} - Y_{kl}^{\text{пот}}(1 - p_{kl})}{Y_{kl}^{\text{вх}}} = P_{k,\,l}, \quad (4)$$

т. е. структурно-информационная связность равна структурной связности.

Оценка структурно-информационной связности сети в целом проводится по матрице $H = \|H_{k,\,l}\|$, элементами которой являются значения $H_{k,\,l}$, если $Y_{kl}^{\text{вх}} > 0$. Если $Y_{kl}^{\text{вх}} = 0$ или $k = 1$, то значение элемента $H_{k,\,l}$ не определено. Будем считать, что сеть находится в работоспособном состоянии, если $H_{k,\,l} \neq 0$ для всех значений k, l.

Для заданного минимально допустимого значения связности $h^{\min}$ сеть считается в работоспособном состоянии, если $H_{k,\,l} > H^{\min}$ на множестве $H_{k,\,l}$, для которых значения определены. Исходными данными алгоритма определения $H_{k,\,l}$ являются: структура сети, значения надежности всех ветвей сети, $Y_{kl}^{\text{вх}}$, план распределения потоков (маршрутные таблицы).

Критерий структурно-информационной связности оценивает потенциальную надежность сети. Значение этого критерия является верхним пределом вероятности связи между узлами сети. Однако, связь между узлами может быть не установлена не только по причине нарушения работоспособности каналов, но и по причине отсутствия в данный момент времени свободных канальных ресурсов. Для определения вероятности связи между узлами сети в условиях, когда пропускная способность линий ограничена, введено понятие информационной связности $Q_{k,\,l}$ от узла X_k к узлу X_l. Определяется информационная связность по формуле

$$Q_{k,\,l} = \frac{Y_{kl}^{\text{вх}} - Y_{kl}^{\text{пот}}}{Y_{kl}^{\text{вх}}}. \qquad (5)$$

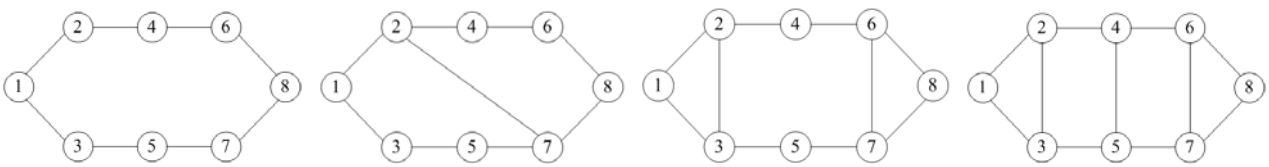
Формула (5), как и входящие в нее величины, аналогична (3). Различие заключается в методике определения потерянного потока $Y_{kl}^{\text{пот}}$. При определении $H_{k,\,l}$ учитывается потерянный поток только по причине отказа ветви, а при определении $Q_{k,\,l}$ – и по причине занятости всех канальных ресурсов. С ростом пропускной способности линий связи $Q_{k,\,l} \to H_{k,\,l}$.

Проведем анализ структурно-информационной связности сетей, структуры которых изображены на рис. 1. Предположим, что для организации связи между узлами X_1 и X_8 допускается перебор всех возможных путей между ними. В этом случае показатель структурно-информационной связности $H_{1,\,8}$ определяется соотношением (4) и структурно-информационная связность равна структурной связности $P_{1,\,8}$. При расчетах примем, что вероятность исправного состояния ребер одинакова и равна p.

Для структуры, приведенной на рис. 1, *а* вероятность связности вершин X_1 и X_8 рассчитывается согласно выражениям (1) и (2) и составляет:

$$P_{1,\,8}^{(1)} = 1 - (1 - p^4)^2 = 2p^4 - p^8 = H_{1,\,8}^{(1)}. \qquad (6)$$

Для расчета структурной надежности сети, граф которой приведен на рис. 1, *б*, будем использовать метод с применением теоремы разложения. В качестве элемента разложения выберем ребро-перемычку l_{27}. Вероятность связности вершин X_1 и X_8 при



а) *б*) *в*) *г*)

Рис. 1. Структуры исследуемых сетей

исправном и неисправном состоянии ребра-перемычки l_{27} рассчитывается в соответствии с соотношениями (1) и (2). Вероятность $P_{1,8}$ связности вершин X_1 и X_8 есть сумма вероятностей $p(G^0_{1,8}\big|l_{27})$ и $p(G^0_{1,8}\big|\overline{l_{27}})$ существования структуры двойственной схемы подграфа $G^0_{1,8}$:

$$P^{(2)}_{1,8} = p(F_{1,8}=1) = p(l_{27})\cdot p(G^0_{1,8}\big|l_{27}) + q(l_{27})\cdot p(G^0_{1,8}\big|\overline{l_{27}}).$$

Таким образом, вероятность связности вершин X_1 и X_8 равна

$$P^{(2)}_{1,8} = p\cdot(1-(1-p)(1-p^3))^2 + (1-p)\cdot(1-(1-p^4)^2);$$

$$P^{(2)}_{1,8} = 2p^9 - 3p^8 + p^7 - 2p^6 + 2p^4 + p^3 = H^{(2)}_{1,8}. \quad (7)$$

Проанализировав структуры, изображенные на рис. 1, *в*, *г*, и рассмотрев все возможные состояния элементов разложения, получим выражения для расчета вероятности связности вершин X_1 и X_8 в сетях с соответствующими структурами:

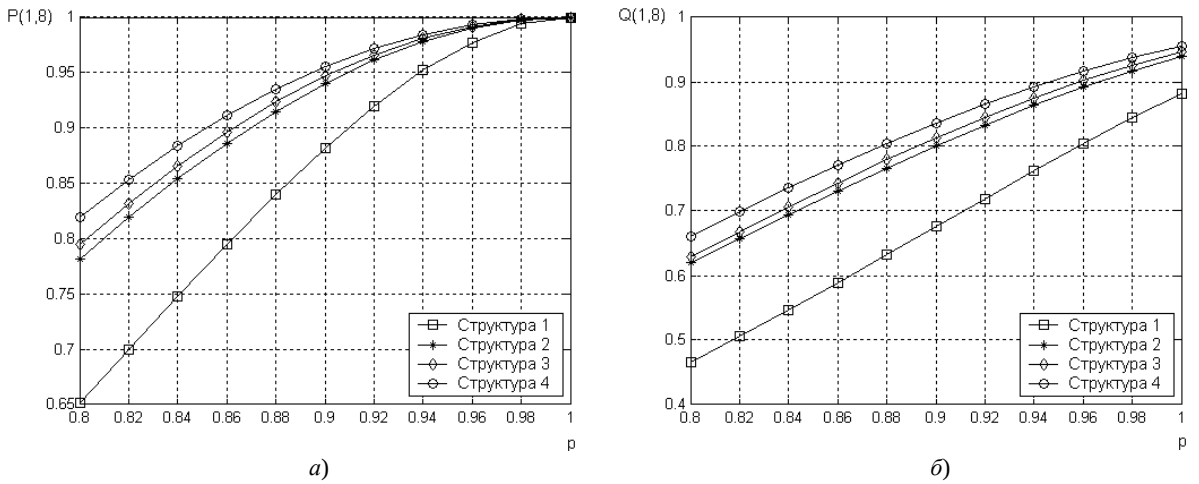
$$P^{(3)}_{1,8} = -3p^{10} + 8p^9 - 4p^8 + 2p^7 - 12p^6 + 8p^5 + 2p^4 = H^{(3)}_{1,8}, \quad (8)$$

$$P^{(4)}_{1,8} = 8p^{11} - 36p^{10} + 52p^9 - 15p^8 - 18p^7 + 2p^6 + 6p^5 + 2p^4 = H^{(4)}_{1,8}. \quad (9)$$

На рис. 2, *а* приведены полученные с использованием выражений (6), (7), (8), (9) графики зависимости вероятности $P_{1,8}$ структурной (структурно-информационной) связности от вероятности p исправного состояния ребер для исследуемых структур сетей. При определении информационной связности $Q_{1,8}$ необходимо учитывать поток, потерянный по причине занятости всех канальных ресурсов. На рис. 2, *б* приведены графики зависимости вероятности $Q_{1,8}$ информационной связности от вероятности p исправного состояния ребер, если пропускная способность линий связи ограничена и вероятность отсутствия свободных канальных ресурсов составляет $p_0 = 0,1$.

Как видно из приведенных на рис. 2, *а* графиков, самой ненадежной является сеть со структурой, представленной на рис. 1, *а*, которая представляет собой кольцо без перемычек. Введение в такую сеть одной перемычки (рис. 1, *б*) значительно увеличивает ее надежность. Увеличение количества перемычек приводит к росту вероятности структурной и информационной связности, хотя и не такому значительному, как при переходе от структуры без перемычек к структуре с одной перемычкой. Так, при надежности всех ветвей сети $p = 0,9$, связности $P_{1,8}$ в сети без перемычек вероятность составляет 0,88, в сети с одной перемычкой – 0,94, а в сетях с двумя и тремя перемычками – 0,95 и 0,96 соответственно. Наилучшей из рассмотренных структур с точки зрения надежности является кольцо с тремя перемычками (рис. 1, *г*).

Из графиков, приведенных на рис. 2, *б* видно, что при учете ограниченности пропускной способности каналов сети вероятность связности $P_{1,8}$ становится ниже, чем в идеализированных условиях. Так, если вероятность отсутствия свободных канальных ресурсов составляет $p_0 = 0,1$, то при надежности всех ветвей $p = 0,9$ в сети с наиболее надежной структурой вероятность информационной связности $Q_{1,8} \cong 0,84$, в то время как вероятность структурной связности $P_{1,8} \cong 0,96$. В сети с кольцевой структурой без



а) *б*)

Рис. 2. Графики зависимости вероятности структурной и информационной связности от надежности ветвей сети

перемычек, которая является наименее надежной из рассмотренных вариантов, вероятность информационной связности $Q_{1,8} = 0,9$ вообще не может быть достигнута даже при надежности всех ветвей $p = 1$.

Таким образом, в данной работе предложены показатели надежности ТКС, учитывающие одновременно как структурные, так и функциональные характеристики сети. Использование предложенных показателей для оценки надежности телекоммуникационных систем и сетей позволяет оценить не только потенциальную надежность ТКС – верхнюю границу структурной надежности сети, но и ее надежность с учетом алгоритмов обслуживания поступающих запросов на узлах сети, плана распределения потоков, ограниченных пропускных способностей каналов. На примере сетей с различной структурой было показано, что вероятность связи между узлами сети существенно зависит не только от надежности ветвей сети, но и от вероятности наличия в данный момент времени свободных канальных ресурсов.

СПИСОК ЛИТЕРАТУРЫ

1. *Олифер В. Г.* Компьютерные сети. Принципы, технологии, протоколы / Олифер В. Г., Олифер Н. А. – С-Пб. : Питер Принт, 2004. – 668 с.
2. *Стеклов В. К.* Основи управління мережами та послугами телекомунікацій / Стеклов В. К., Кільчицький Є.В. – К. : Техника, 2002. – 438 с.
3. *Филин Б. П.* Методы анализа структурной надежности сетей связи / Филин Б. П. – М. : Радио и связь, 1988. – 208 с.
4. *Дудник Б. Я.* Надежность и живучесть систем связи / Б. Я. Дудник, В. Ф. Овчаренко, В. К. Орлов и др. ; под ред. Б. Я. Дудника. – М. : Радио и связь, 1984. – 216 с.

Надійшла 24.11.2008

Калєкіна Т. Г., Коваленко Т. М.

ОБГРУНТУВАННЯ КРИТЕРІЮ СТРУКТУРНО-ІНФОРМАЦІЙНОЇ ЗВ'ЯЗНОСТІ ПРИ АНАЛІЗІ НАДІЙНОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

В роботі запропоновано комплексні показники надійності телекомунікаційних систем і мереж, які враховують одночасно як структурні, так і функціональні характеристики мережі. Запропоновані показники дозволяють оцінити не лише потенційну надійність телекомунікаційної мережі – верхню межу структурної надійності, але й надійність мережі з урахуванням обмеженої пропускної здатності каналів.

Ключові слова: надійність, структурна зв'язність, інформаційна зв'язність, інтегральний показник, граф, телекомунікаційна мережа.

Kalekina T. G., Kovalenko T. N.

JUSTIFICATION OF STRUCTURAL-INFORNATIONAL CONNECTIVITY INDICATOR WHEN ANALYZING RELIABILITY OF TELECOMMUNICATION SYSTEMS AND NETWORKS

In this work the integrated reliability indicators for telecommunication systems and networks are proposed, that consider both structural and functional network characteristics. The indicators make it possible to evaluate not only potential reliability of a telecommunication network which is the upper bound of structural reliability but also network reliability subject to limited channel throughput.

Key words: reliability, structural connectivity, informational connectivity, integrated indicator, graph, telecommunication network.

УДК 004.9

Киричек Г. Г.

Старший викладач Запорізького національного технічного университета

КЕРУВАННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ НА ВСІХ РІВНЯХ ІЄРАРХІЇ ОТРИМАННЯ ЗНАНЬ

Система навчання представлена у вигляді багаторівневої конструкції взаємодіючих між собою та із зовнішнім середовищем елементів. Розроблено модель розподіленої системи керування інформаційними потоками на всіх рівнях ієрархії отримання знань з її подальшою реалізацією в інформаційній системі.

Ключові слова: керування інформацією, модель одержання знань, пошукова модель, навчальний процес, інформаційна система, інформаційні ресурси, імовірність одержання інформації.

ВСТУП

Вищий навчальний заклад (ВНЗ) за своєю суттю є інноваційною структурою – розробка і використання нових освітніх технологій і підходів є невід'ємною частиною його життєдіяльності. Організаційна структура ВНЗ життєздатна і динамічна. Тому система керування інформаційними потоками на всіх рівнях ієрархії отримання знань повинна забезпечувати