РАДИОТЕХНИКА И СВЯЗЬ

УДК 621.39:519.2

Н. Д. ВЕШКУРЦЕВ

Омский государственный
технический университет

ЭНТРОПИЯ ЦЕНТРАЛЬНЫХ МОМЕНТОВ РАСПРЕДЕЛЕНИЯ

Решена задача по определению энтропии центральных моментов распределения стационарных случайных процессов. Ответы задачи подтверждают положения теории информации и корреляционного анализа. Применение результатов решения задачи показано на примере с экспериментальными данными, полученными ранее.

Ключевые слова: энтропия, центральные моменты, вероятность, закон распределения, плотность вероятности, ортогональные полиномы, шкала значений.

Среди вероятностных характеристик стационарных случайных процессов имеются центральные моменты распределения, описывающие энергетические свойства процесса, причем центральный момент первого порядка тождественно равен нулю. Следовательно, нами рассматриваются центральные моменты M_k, где $k = 2, 3, 4$. При $k \geq 5$ центральные моменты в литературе встречаются очень редко, они не используются в разработке рекомендаций для прикладной науки. Может быть, это частично связано с тем, что в фундаментальной науке известно утверждение «Моменты более низкого порядка несут больше сведений о случайном процессе, чем моменты высокого порядка» [1, с. 69]. В связи с этим представляет интерес количественно выразить объем сведений о случайном процессе, который несет центральный момент k-го порядка. Другими словами, необходимо определить количество информации о случайном процессе, которое содержится в численном значении центрального момента.

Решение такой задачи позволило бы, например, разрабатывать шкалу по значениям оценок вероятностных характеристик, по которой можно было бы определять свойства случайного процесса или вещества, формирующего случайный сигнал. При исследовании вещества радиостатистическим методом значения оценок центральных моментов распределения получаются разные, для примера они приведены в табл. 1 [2], где $\tilde{M}_k$ — оценка момента.

Значения оценок моментов — это случайные величины с некоторой вероятностью их появления. Эти значения получены в результате статистической обработки данных, представленных мгновенными значениями случайного сигнала. Если случайный сигнал — напряжение, то размерность оценок моментов будет такой, как это указано в табл. 1.

Таблица 1

Центральные моменты распределения

№ п/п	Вещество	$\hat{M}_2$, В^2	$\hat{M}_3$, В^3	$\hat{M}_4$, В^4
1	Вино Каберне	1,09	−0,06	5,26
2	Вино Каберне с примесью 10 % воды	2,63	0,25	15,15
3	Кукурузное масло	3,24	0,04	20,05
4	Кукурузное масло с примесью 10 % льняного масла	2,29	0,15	12,75

При обработке данных их количество взято настолько большим, насколько позволил эксперимент (в нашем примере использовано 4096 мгновенных значений в каждом эксперименте). Всего выполнено пять независимых измерений при изучении каждого момента распределения. В итоге, статистическая погрешность обработки данных не превышает 10 %.

Помимо разных значений оценок моментов в табл. 1 показано, что нечётные центральные моменты имеют как положительные значения, так и отрицательные. Четные центральные моменты распределения всегда имеют только положительные значения. Объясняется это физическим смыслом центральных моментов распределения. При разработке шкалы планируется использовать значения оценок центральных моментов распределения, однако их размерность разная. Следовательно, необходимо привести значения оценок центральных моментов распределения к одинаковой размерности.

Решение задачи о приведении размерности центральных моментов распределения к единой единице измерения можно получить при помощи энтропии. Известно, что энтропия является некоторой мерой априорной неопределенности, например, случайного процесса. Она имеет размерность единицы информации бит. При определении или измерении значения оценки любого центрального момента затрачивается ровно столько бит информации, сколько будет достаточно, чтобы представить значение оценки момента числом и тем самым понизить неопределенность о свойствах случайного процесса. Как будет показано ниже, энтропия значения оценки центрального момента $M_2 = 1{,}09$ из табл. 1 равна 0,36 бит. Таким образом, неопределенность о свойствах случайного процесса понизилась на 0,36 бита, поскольку нам стала известна его дисперсия.

В теории информации энтропию дискретной случайной величины рассчитывают по формуле [3]

$$H(X) = -P(X)\log P(X), \qquad \textbf{(1)}$$

где X — случайная величина, которой в нашей задаче служит оценка любого центрального момента распределения, т. е. $\hat{M}_2$, $\hat{M}_3$, $\hat{M}_4$; $P(X)$ — вероятность появления значения случайной величины; log — логарифм с основанием два. Для вычисления вероятности $P(X)$ необходим статистический закон отдельно каждого центрального момента распределения.

Закон распределения центрального момента будем искать с помощью ряда [1]

$$W_1(x) = \sum_{k=-\infty}^{\infty} C_k\, \varphi(x)\, Q_k(x), \qquad \textbf{(2)}$$

где $W_1(x)$ — плотность вероятности случайной величины X; $\varphi(x)$ — некоторая воспроизводящая функция;

$$C_n = \int_{-\infty}^{\infty} W_1(x) Q_n(x)\, dx \quad - \qquad \textbf{(3)}$$

коэффициенты ряда распределения; $Q_n(x)$ — совокупность ортогональных полиномов. От рационального выбора полиномов зависит число членов ряда (2) и быстрая его сходимость. Кроме того, в нашей задаче случайные оценки $\hat{M}_2$, $\hat{M}_4$ имеют только положительные значения, а случайная оценка $\hat{M}_3$ — положительные и отрицательные значения. Следовательно, закон распределения оценок моментов $\hat{M}_2$, $\hat{M}_4$ должен располагаться только в положительной области значений числовой оси, а закон распределения оценки момента $\hat{M}_3$ — в обеих областях значений числовой оси.

Анализ литературы и известных решений [4] показал, что в нашей задаче целесообразнее всего использовать ортогональные полиномы Лагерра, для которых воспроизводящая функция равна

$$\varphi(x) = \frac{x^{\alpha} e^{-x}}{\Gamma(\alpha + 1)}, \qquad \textbf{(4)}$$

где $\Gamma(\alpha + 1)$ − гамма-функция, а также $x \geq 0$, $\alpha > 0$.

Функция (4) есть гамма-распределение, с использованием которого идет построение ряда (2). Дальнейшее исследование ряда (2) с полиномами Лагерра для дисперсии случайного процесса выполнено в работе [4]. При этом получен следующий результат:

$$W_1(x) = \frac{\left(\frac{n}{2}\right)^{n/2} x^{\frac{n}{2}-1}}{\Gamma\left(\frac{n}{2}\right)} e^{-\frac{nx}{2}}, \qquad \textbf{(5)}$$

где $W_1(x)$ — одномерная плотность вероятности значений оценки дисперсии, n — число степеней свободы закона распределения (5). Применение выражения (5) ограничено, поскольку оно получено при равенстве нулю корреляции между измеренными значениями оценок моментов распределения. Если $n = 1$, то закон распределения (5) совпадает с законом Пирсона или χ^2 (хи-квадрат) по другой терминологии. При $n \geq 2$ закон распределения (5) отличается от закона Пирсона, коэффициенты асимметрии и эксцесса при этом равны $\gamma_1 = 2\sqrt{2/n}$, $\gamma_2 = 12/n$.

Анализ выражения (5) показал, что при $n = 1$ плотность вероятности положительная как при $x \geq 0$, так и при $x < 0$. Следовательно, закон Пирсона с одной степенью свободы можно применить для описания распределения центрального момента третьего порядка. Когда $n = 2$, то плотность вероятности (5) положительная только при $x \geq 0$, а при других x она равна нулю. Поэтому этот вариант можно использовать для описания закона распределения центральных

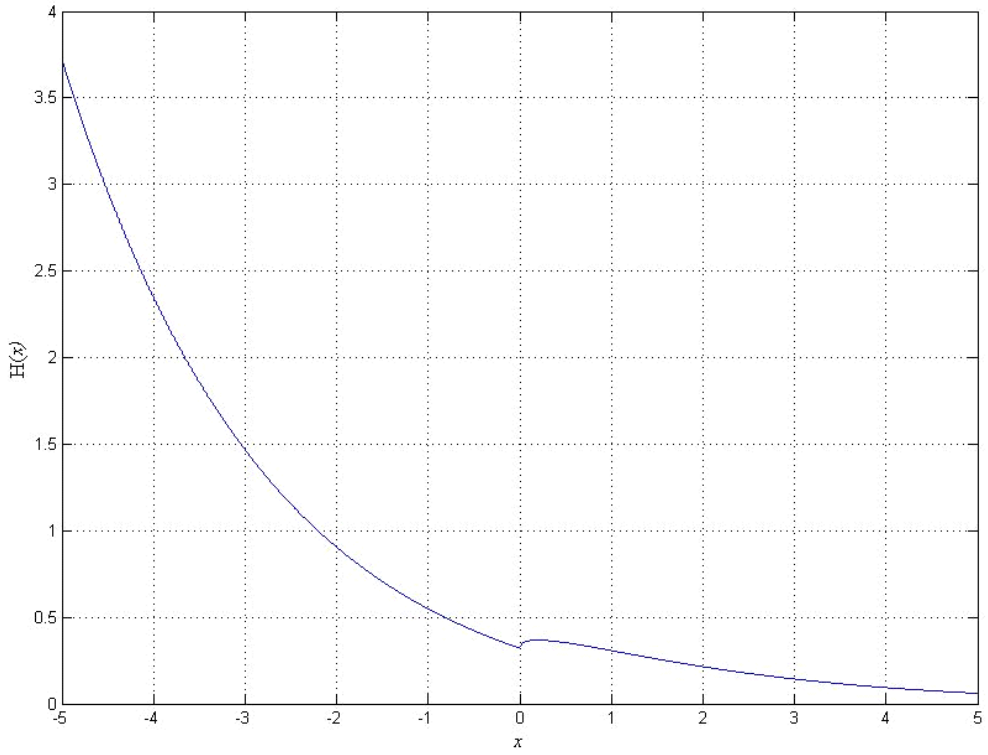

Рис. 1. Энтропия центрального момента распределения 3-го порядка

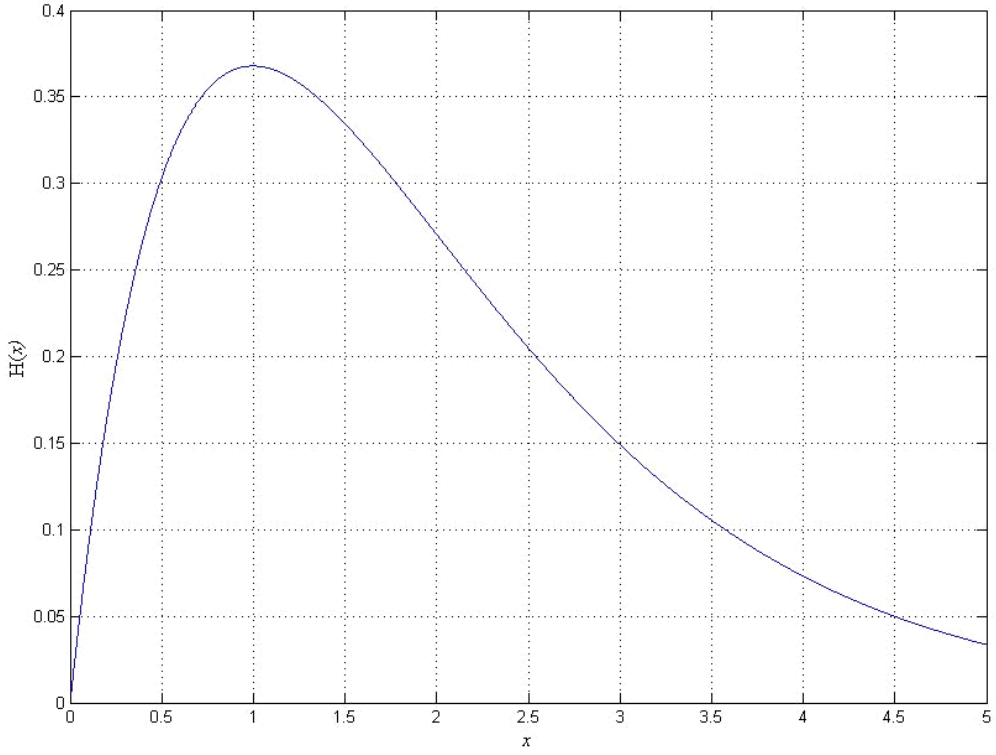

Рис. 2. Энтропия центральных моментов распределения 2-го и 4-го порядков

моментов распределения второго и четвертого порядков. При $n=3$ плотность вероятности (5) получается и положительной, и отрицательной. Такой вид закона распределения не имеет физического смысла и не может использоваться при решении любой прикладной задачи.

Переход от плотности вероятности (5) к функции распределения вероятности выполним известными приемами, в результате чего получим функцию распределения вероятности в следующем виде:

$$F_1(x)=\frac{\Gamma\left(\frac{n}{2},\frac{n}{2}x\right)}{\Gamma\left(\frac{n}{2}\right)}, \qquad \textbf{(6)}$$

где $\Gamma\left(\frac{n}{2},\frac{n}{2}x\right)$ — неполная гамма-функция. При $n=1$ функция (6) совпадает с функцией распределения вероятности, известной для закона Пирсона. Функ-

Таблица 2
Энтропия центральных моментов распределения

Центральные моменты	Порядковый номер в табл. 1			
	1	2	3	4
$\hat{M}_2$, бит	0,36	0,17	0,13	0,23
$\hat{M}_3$, бит	0,33	0,36	0,35	0,36
$\hat{M}_4$, бит	0,05	0,0005	0,0005	0,002

ция (6) требуется для вычисления вероятности, включенной в формулу (1). В итоге искомая вероятность равна

$$P(X < x) = F_1(X < x) = \frac{\Gamma\left(\frac{n}{2}, \frac{n}{2}x\right)}{\Gamma\left(\frac{n}{2}\right)}, \qquad (7)$$

где x — значение оценки центрального момента распределения. Расчеты выполнены с помощью формул (1, 7), результаты которых представлены на рис. 1 для $n=1$ и на рис. 2 для $n=2$.

Анализ графиков на рис. 1, 2 показывает, что энтропия центральных моментов распределения разная, но незначительно различается в зависимости от порядка момента. В области положительных значений оценок центральных моментов энтропия немного превосходит 0,35 бита. Однако в области отрицательных значений оценки центрального момента 3-го порядка энтропия стремится к бесконечности. На наш взгляд, этому имеется объяснение, связанное с физическим смыслом центрального момента 3-го порядка. Момент M_3 характеризует асимметрию закона распределения, т. е. смещение математического ожидания энергии сигнала относительно нуля. Смещение энергии сигнала в отрицательную область значений настолько маловероятно, что потребуется бесконечно много информации для выявления такого эффекта, поскольку энергия сигнала всегда положительная физическая величина. Также отметим, что энтропия нормального закона распределения случайного процесса с математическим ожиданием $m_1=0$ и $M_2=1$ равна 2 битам. По всем данным энтропия моментов распределения не может превышать энтропию статистического закона. Таким образом, значения энтропии на рис. 1, 2 соответствуют известным положениям теории информации.

С помощью рис. 1, 2 определим энтропию оценок моментов распределения, указанных в табл. 1. Результаты вычислений сведены в табл. 2.

В отличие от табл. 1, размерность центральных моментов в табл. 2 одинаковая, она равна биту. Теперь моменты распределения можно умножать, складывать, вычитать и т. д.; из них можно строить шкалу значений, причем центральный момент 4-го порядка имеет совсем малый вес, т. к. его значения колеблются в районе 0,002 – 0,05 бита. Получается, что центральный момент 4-го порядка меньше других несет сведений о случайном процессе. Таким образом, можно утверждать, что нам удалось экспериментальными данными подтвердить приведенное в начале статьи высказывание из книги [1, с. 69] о моментах высоких порядков.

Заключение. Получена энтропия центральных моментов распределения стационарных случайных процессов, которая на много меньше энтропии статистического закона. Кроме того, центральные моменты высшего порядка имеют энтропию меньше, чем моменты низшего порядка, а следовательно, они несут о случайном процессе меньше сведений нежели моменты низшего порядка.

С помощью энтропии размерность центральных моментов распределения приведена к единой единице измерения, которой является бит. Таким образом, стали возможны арифметические действия с центральными моментами разных порядков при разработке шкалы значений с размерностью бит, бит/см^2 или иной другой.

Библиографический список

1. Тихонов, В. И. Статистическая радиотехника / В. И. Тихонов. – М. : Сов. радио, 1966. – 678 с.

2. Вешкурцев, Ю. М. Радиостатистический метод исследования веществ. Ч. 2. / Ю. М. Вешкурцев, Н. Д. Вешкурцев, Е. А. Фадина // Омский научный вестник. Сер. Приборы, машины и технологии. – 2013. – № 1 (117). – С. 238–242.

3. Стратанович, Р. Л. Теория информации / Р. Л. Стратанович. – М. : Сов. радио, 1975. – 424 с.

4. Виленкин, С. Я. Статистическая обработка результатов исследования случайных функций / С. Я. Виленкин. – М. : Энергия, 1979. – 320 с.

ВЕШКУРЦЕВ Никита Дмитриевич, аспирант кафедры «Автоматизированные системы обработки информации и управления».
Адрес для переписки: zedati90@gmail.com

Статья поступила в редакцию 02.04.2014 г.

Книжная полка

Куэй, Р. Электроника на основе нитрида галлия / Р. Куэй ; под ред. А. Г. Васильева ; пер. с англ. Ю. А. Концевого, Е. А. Митрофанова. – М. : Техносфера, 2011. – 587 с.

В издании представлен широкий круг вопросов, связанных с выбором подложек для гетероэпитаксии, с методами изготовления гетероэпитаксиальных структур, с технологией транзисторов на этих структурах. Рассмотрены материалы, приборы, много типов транзисторов, способных работать в различных диапазонах сверхвысоких частот. Рассматриваются схемы, создаваемые на этих транзисторах. Особое внимание уделяется вопросам надежности СВЧ-транзисторов на основе нитрида галлия.

УДК 621.396.946:004.056.53

А. В. МОРОЗОВ

Омский государственный университет путей сообщения

ИССЛЕДОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ НА КОМБИНИРОВАННЫХ МОДЕЛЯХ

В статье приведены сведения о количественном оценивании информационной безопасности беспроводных сетей. Показано, что наиболее эффективным направлением анализа, позволяющим объективно оценивать информационную безопасность объектов информатизации, является комбинированное использование нескольких методов. Даны конкретные рекомендации по применению имеющегося математического и программного аппарата для обеспечения безопасности.

Ключевые слова: беспроводные сети, информационная безопасность, количественная оценка, критический маршрут, метод критических вершин, методика комбинированной оценки.

В практическом анализе информационной безопасности (ИБ) желательно иметь их количественные оценки. Существует несколько способов количественного описания ИБ, приведенных, например, в [1]. Они включают, в частности, вероятностные, графические, имитационные, игровые методы и модели описания. Методика, основанная на нечетких множествах [2], может использоваться, но далека от совершенства и дает весьма расплывчатые результаты.

Наиболее плодотворной, количественной оценкой ИБ для разных информационных объектов и ее практической реализации является методика комбинированной оценки.

Внутреннюю структуру информационной системы (ИС) целесообразно представлять в виде графа, в котором вершины являются элементами сети, а ребра (дуги) — средствами взаимодействия (передача информации или каналы связи). Каждый из этих элементов может быть описан количественно в функции времени, причем оценки зависят от поставленной задачи. Например, для оптимизации загрузки сети наиболее эффективными могут быть потоки информации по каждой из дуг как средние по времени за заданный временной интервал, пиковые нагрузки, размеры информационных сообщений (максимальные, минимальные, средние за интервал оценивания), размеры буферной памяти в узлах сети, время задержки (ожидание связи), потери информации, связанные с природой беспроводной связи, и т.д. Нас в данном случае интересуют угрозы безопасности. Оценки в данном случае могут быть следующих типов:

— вероятность несанкционированного доступа к информационным ресурсам от произвольного размещения нарушителя (одиночный или множественный вариант) в функции времени;

— стоимость однократного нарушения по простейшему варианту «одиночное нарушение — одиночный пункт нападения», также в функции времени;

— затраты на восстановление ущерба от нарушения по предыдущему варианту.

Введем следующие обозначения:

— P (X_{IJ},t) — вероятность успешной атаки 1-го нарушителя на J-й элемент информационной системы;

— C (X_{IJ}, t) — стоимость ущерба от однократного нападения в тех же координатах;

— З (X_{IJ} ,t) — стоимость восстановления информационной системы после нарушения ИБ.

Как видно из обозначений, все приведенные оценки являются функциями времени. Описываемые ими процессы являются случайными, причем нестационарными. Можно отметить их некоторые особенности. В частности, внутренние и внешние взаимодействия в информационных системах можно рассматривать простейшие стационарные случайные процессы с равномерной загрузкой и равномерной плотностью распределения, не зависящей от времени [3]. Это примитивная модель, не учитывающая реальной суточной загрузки сети, особенно в нештатных (пиковых) режимах, но она может быть использована в качестве первичной оценки, особенно по максимуму одного из анализируемых параметров.

Все количественные оценки имеют жесткую привязку к информационным объектам и зависят от множества внешних и внутренних факторов. Внутренние — топология сети, режимы работы легальных пользователей (включая операционные системы, дополнительное программное обеспечение, режимы суточной работы, взаимодействие с другими пользователями и с внешней средой, включая Интернет). Внешние — количество внешних связей, режимы работы с ними. Большие проблемы создают беспроводные технологии Wi-Fi и Wi-MAX, у которых серьезно снижен уровень безопасности сети и её пользователей. Поскольку, ко всем прочим проблемам обеспечения безопасности у беспроводных сетей добавляются уязвимости, связанные с уровнем доступа к среде, в силу нефиксированной природы связи [4].

Кроме того, в качестве количественной оценки могут быть использованы показатели трафика (потоки информации, задержки, потери — всё также в функции времени).

Для более корректного описания представим информационную систему в виде графа, в котором вершины представляют собой автономные объекты, имеющие некоторые информационные ресурсы и которые могут взаимодействовать с другими такими же объектами. Под объектами в зависимости от глубины детализации могут быть персональные компьютеры или приравниваемые к ним аппаратные средства, локальные сети (LAN), беспроводные локальные сети (WLAN), корпоративные сети (MAN) с включаемым коммутационным оборудованием и стандартным оборудованием связи, а также смешанные LAN/WLAN сети.

Представим такую систему в виде, приведенном на рис. 1. Здесь обозначено: 1, ..., 6 — объекты ИС, ВВ — внешние взаимодействия, Н — нарушения.

Каждый из выделенных объектов может иметь свои взаимодействия в зависимости от структуры системы. Не обязательно граф внутренних взаимодействий должен быть полносвязным, это обстоятельство учитывается в системе взаимодействий, в матрице задержек или потерь информации.

Сделаем дополнительные определения. Для этого изобразим структуру элементарного подмножества ИС, приведенную на рис. 2. Здесь I и J — узлы элементарной сети из двух абонентов, α_{IJ} — количественная оценка взаимодействия. Понятно, что это функция времени, поэтому в дальнейшем она фигурирует в виде $\alpha_{IJ}(t)$. Для количественной оценки применим любой из трех вышеописанных критериев.

Для оценки внешних взаимодействий можно использовать ту же схему с добавлением функций внешних воздействий $\beta_I(t)$ и $\beta_J(t)$.

Для последующего аналитического описания введем гипотезы независимости и равномерности внешних воздействий.

Независимость внешних воздействий означает, что внешние атаки на ИС не зависят друг от друга. В таких случаях функции просто суммируются:

$$\beta_S(t) = \Sigma_I \beta_I(t) + \Sigma_J \beta_J(t). \quad \textbf{(1)}$$

Равномерность внешних воздействий показывает, что их вероятности не зависят от времени. Фактически это не так, но упрощает дальнейший анализ. Для приближения к этой гипотезе можно использовать понятие интервал стационарности, на котором эта гипотеза применима [5].

При принятых допущениях можно составить матрицу взаимодействий $R_{IJ}(t)$ размером N*N, состоящую из элементов $\alpha_{IJ}(t)$, где N — количество узлов анализируемой ИС, $\alpha_{IJ}(t)$ — весовой коэффициент, определяемый в зависимости от типа решаемой задачи. Матрица имеет вид, приведенный на рис. 3. По матрице можно решать множество прикладных задач, связанных с определением $\alpha_{IJ}(t)$.

Предположим, в качестве количественной оценки взят показатель удельного трафика $C_{IJ}(t) = I(t)/T$, где T — время анализа. Тогда можно поставить следующие задачи (их список может быть дополнен).

1. Оптимизация трафика по выделенной сети по одному из возможных критериев: максимум суммарного количества переданной информации при существующих ограничениях по каждому из направлений.

2. Минимум потерь при заданных ограничениях на удельный трафик по каждому из направлений.

3. Минимизация времени задержки по всему графу или его фрагментам.

Поставленные задачи могут решаться в рамках существующих математических методов и алгоритмов. В частности, они могут различаться в зависимости от способа описания объекта. Для непрерывных объектов способ их описания — дифференциальные уравнения в частных производных [6]. Ограничениями в таких случаях являются начальные и граничные условия, а также способ описания решения. Вероятно, в таких нечетких рамках можно получить любое решение, угодное автору.

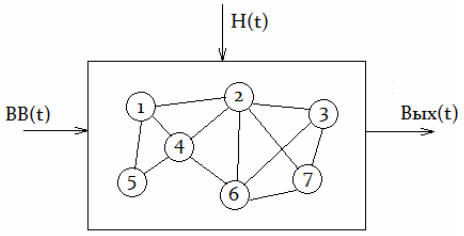

Рис. 1. Структура информационной системы

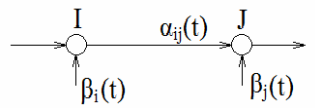

Рис. 2. Элементарное взаимодействие

$$\begin{vmatrix} \alpha_{11}(t) & \alpha_{12}(t) \ldots\ldots\ldots\ldots & \alpha_{1n}(t) \\ \alpha_{21}(t) & \alpha_{22}(t) \ldots\ldots\ldots\ldots & \alpha_{2n}(t) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & \\ \alpha_{n1}(t) & \alpha_{n2}(t) \ldots\ldots\ldots\ldots & \alpha_{nn}(t) \end{vmatrix}$$

Рис. 3. Матица взаимодействий в информационной системе

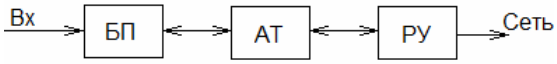

Рис. 4. Схема реагирования на трафик

В подобных условиях более приемлемы дискретные задачи и решения, но с одним отличием: они являются функциями непрерывного аргумента — времени. С учетом этого фактора они превращаются в динамические и предполагают, по крайней мере, два подхода:

— классическая динамическая задача с использованием вариабельности во времени количества клиентов сети (N) и динамики их работы;

— учет воздействия на сеть клиентов сети и операторов.

Первая задача может решаться с помощью фиксации количества клиентов для трех случаев: максимальная (пиковая) загрузка, минимум клиентов и их стабильный режим работы (область гарантированного обслуживания). Любая из этих подзадач решается с использованием известного в теоретической кибернетике симплекс-метода [7]. Применительно к поставленной проблеме он усложняется необходимостью учета зависимости от времени. При этом возникает задача выбора интервала времени T и соответствующие ей технические решения. Для иллюстрации технологии динамического анализа трафика возможна структура наблюдения за объектами в реальном времени, приведенная на рис. 4. Здесь обозначено: АТ — анализатор трафика; БП — блок памяти; РУ — решающее устройство. В реальном времени АТ оценивает текущий трафик в БП, причем от размеров памяти зависит и режим работы

системы анализа: чем короче буфер, тем оперативнее анализ и время реагирования.

Функции АТ может выполнять или сервер локальной сети, или коммутационное оборудование (коммутаторы, маршрутизаторы).

Для корректного описания политики безопасности возможны различные критерии. Один из них — стоимость дополнительного оборудования (программного обеспечения). Обозначим стоимость дополнительных мероприятий по защите информации через $Ц_{\Sigma}$, суммарную оценку потерь при нарушениях ИБ через $П_{\Sigma}$. Тогда очевидно следующее неравенство:

$$Ц_{\Sigma} < П_{\Sigma}. \quad (2)$$

Матрицу взаимодействий можно структурировать, по крайней мере, двумя способами.

1. Ранжирование элементов $\alpha_{IJ}(t)$ в порядке убывания:

$$\alpha_{IJ}(t) \geq \alpha_{I+1,J}(t) \geq \alpha_{I,J+1}(t). \quad (3)$$

Введем *коэффициент качества* — константу M (M>1), на которую делятся все коэффициенты $\alpha_{IJ}(t)$:

$$\gamma_{IJ}(t) = \alpha_{IJ}(t)/M. \quad (4)$$

В соответствии с критерием качества выбирается пороговое значение Δ, по которому производится сравнение:

$$\gamma_{IJ}(t) \leq \Delta. \quad (5)$$

Если условие (5) выполняется, значение $\gamma_{IJ}(t)$ обнуляется. Это может существенно снизить затраты на защиту информационных ресурсов. Отметим, что $\gamma_{IJ}(t)$ — функция времени, что предполагает решение динамической задачи, в том числе в реальном времени.

2. Декомпозиция матрицы взаимодействий — представление ее в виде произведения более простых (меньшей размерности) или особых (ленточные и им подобные).

Применительно вероятностной оценке справедливы общие аксиомы. Введем некоторые определения.

1. *Элементарное звено доступа* (рис. 5) — отдельное ребро графа; начальная вершина A — является исходным состоянием пользователя (нарушителя), получение доступа — конечная вершина B, трудоемкость доступа — r. Трудоемкость может оцениваться количеством операций, необходимых для доступа, или пропорциональным ему временем. Понятно, что для штатного пользователя и нарушителя значения r разные: в идеальном случае для пользователя $r_{П} \to 0$, для нарушителя $r_{Н} \to \infty$.

Если принять рассмотренную выше модель пуассоновского потока, для безопасности необходимо, чтобы у нарушителя $\lambda_{Н} \to \infty$, для пользователя $\lambda_{П} \to 0$. Соображения по оценке значений λ рассмотрим ниже.

2. *Последовательная цепочка доступа* (рис. 6) соответствует последовательному преодолению двух (и более) элементов защиты с трудоемкостями r_1 и r_2 соответственно.

Если элементы защиты не зависят друг от друга, а вероятности выражаются функциями $P_{П1}(t)$ и $P_{П2}(t)$, результирующая вероятность

$$P_{П}(t) = P_{П1}(t) * P_{П2}(t) \quad (6)$$

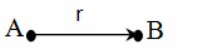

Рис. 5. Элементарное звено доступа

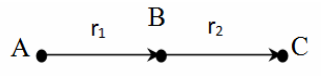

Рис. 6. Последовательный доступ

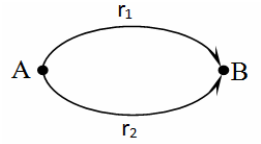

Рис. 7. Параллельный доступ

или при наличии k последовательных звеньев

$$P_{П}(t) = \prod_{i=1}^{K} P_{Пi}(t). \quad (7)$$

Соответственно, безопасность

$$P_{Б} = 1 - P_{Н} = 1 - \prod_{i=1}^{K} P_{Нi}(t). \quad (8)$$

Этот результат хорошо интерпретируется практически: чем больше элементов последовательной защиты, тем труднее их преодолеть нарушителю, т.е. тем выше безопасность.

3. *Параллельный доступ* (рис. 7) соответствует группе пользователей одного и того же ресурса; в общем случае трудоемкости доступа r_1 и r_2 разные (например, разные длины паролей).

Очевидно, для нарушителя цель будет достигнута, если он получит доступ по одному из возможных. Это соответствует произведению вероятностей безопасности:

$$p_{Б}(t) = \prod_{i=1}^{K} p_{Бi}(t) = \prod_{i=1}^{K} [1 - p_{Нi}(t)]. \quad (9)$$

Из выражения (9) следует, что общая безопасность параллельного звена хуже наихудшей из составляющих цепочек.

Выражение (9) имеет место в случае, когда нарушитель имеет возможность одновременного доступа ко всем параллельным звеньям; в более сложном варианте нужно учитывать вероятности такого доступа $p_{Дi}$:

$$p_{Б}(t) = \prod_{i=1}^{K} [1 - p_{Дi} p_{Нi}(t)]. \quad (10)$$

Очевидно, при анализе систем защиты можно представить цепочку действий нарушителя в виде диаграммы доступа, проводя анализ информационной системы [8]. После построения такой диаграммы можно определять такую ее характеристику, как *критический маршрут*: последовательность действий нарушителя, имеющая наименьшую трудоемкость или наибольшую вероятность нарушения. Эта величина может характеризовать общую безопасность системы. С другой стороны, улучшая параметры элементов защиты, находящихся на критическом пути, можно наиболее эффективно повысить общую безопасность.

Такая задача хорошо формализуется. Предположим, на графе задаются начальная и конечная вершины и заданы веса дуг. Ищутся все возможные маршруты между этими вершинами, с помощью формул (6),...,(10) вычисляются веса маршрутов. Маршрут с наиболее высокой вероятностью нарушения и является критическим. В частности, на критическом маршруте отыскивается дуга с наибольшим весом (если речь идет о вероятности нарушения, это наибольшая вероятность, если о времени проникновения, это наименьшее время). После отыскания такой дуги делаются попытки ее усиления, после чего расчет повторяется до вычисления другого критического маршрута и, соответственно, другой дуги с наибольшим весом. Таким итеративным методом с вычислением общей безопасности всей сети можно находить приемлемую безопасность всей сети.

Если ввести в рассмотрение допустимую вероятность нарушения $P_{НДОП}$, а в ходе анализа вычислять результирующую вероятность нарушения $P_{НР}(t)$, то задача анализа — поиск такого критического времени работы сети $t_{КР}$, для которого справедливо неравенство:

$$P_{НР}(t_{КР})\ d + P_{НДОП}. \qquad \textbf{(11)}$$

Проведение мероприятий по совершенствованию защиты можно проводить по критерию стоимости. Обозначим стоимость дополнительных мероприятий по защите информации через $Ц_{\Sigma}$, суммарную оценку потерь при нарушениях ИБ через $П_{\Sigma}$. Тогда очевидно следующее неравенство:

$$Ц_{\Sigma} < П_{\Sigma}. \qquad \textbf{(12)}$$

В противном случае задача решается другими средствами, например, изменением структуры сети, поиском менее дорогостоящих средств защиты.

Второй тип задач, которые можно решать на графовой модели, — поиск критических вершин. Для этого введем в рассмотрение понятие *веса вершины* W_I, который можно оценить как сумму весов прилегающих к ней дуг:

$$W_I = \sum_{Q=1}^{N} W_q . \qquad \textbf{(13)}$$

Предлагается оригинальный **метод критических вершин**, заключающийся в следующем.

1. По имеющемуся графу (диаграмме доступа) вычисляются по формуле (13) веса вершин W_I. Составляется таблица весов.

2. Полученная таблица ранжируется в порядке убывания.

3. Первый член таблицы анализируется по признаку наибольшей составляющей W_q.

4. Проводится комплекс мер по изменению веса W_q.

5. Полученная после модернизации новая таблица уводит к п. 1.

Критерий оценивания тот же, выражение (12).

Автором статьи проведен анализ способов количественной оценки информационной безопасности. На его основе предложен оригинальный метод критических вершин, предлагаемые оценки которого действенны, хорошо алгоритмизируются и имеют реальный практический выход.

Библиографический список

1. Майстренко, В. А. Безопасность информационных систем и технологий / В. А. Майстренко, В. Г. Шахов. — Омск : Изд-во ОмГТУ, 2006. — 232 с.

2. Петренко, С. А. Управление информационными рисками. Экономически оправданная целесообразность / С. А. Петренко, С. В. Симонов. — М. : ДМК Пресс, 2004. — 384 с.

3. Шахов, В. Г. Введение в информационные системы и телекоммуникации / В. Г. Симонов. — Омск : Изд-во ОмГУПС, 2001. — 87 с.

4. Морозов, А. В. Анализ атак на беспроводные компьютерные интерфейсы / А. В. Морозов, В. Г. Шахов // Омский научный вестник. — 2012. — № 3 (113). — С. 323—327.

5. Бендат, Д. С. Измерение и анализ случайных процессов / Д. С. Бендат, А. Дж. Пирсол. — М. : Мир. 1971. — 390 с.

6. Кендалл, М. Статистические выводы и связи / М. Кендалл, А. Стьюарт. — М. : Наука, 1973. — 900 с.

7. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. — М. : ДМК Пресс, 2010. — 544 с.

8. Заде, Л. Понятие лингвистической переменной и его применение к принятию приближенных решений / Л. Заде. — М. : Мир, 1976. — 446 с.

МОРОЗОВ Антон Валерьевич, аспирант кафедры «Автоматика и системы управления».
Адрес для переписки: morozav89@mail.ru

Статья поступила в редакцию 18.03.2014 г.

Книжная полка

Богачков, И. В. Матричные методы анализа СВЧ-устройств : учеб. электрон. изд. локального распространения : учеб. пособие для студентов по специальности 201200 «Средства связи с подвижными объектами» / И. В. Богачков ; ОмГТУ. — Омск : Изд-во ОмГТУ, 2014. — 1 о=эл. опт. диск (CD-ROM).

В учебном пособии рассмотрены матричные методы анализа линеаризованных СВЧ-устройств, приведены примеры анализа СВЧ-устройств с использованием различных методов, подробно описаны матрицы рассеяния базовых элементов, разработанная под руководством автора программа для анализа линейных СВЧ-устройств «Папирус» и порядок работы с ней. Предназначено для студентов всех форм обучения специальностей 201200 «Средства связи с подвижными объектами», 210402 «Проектирование и эксплуатация средств обеспечения информационной безопасности в системах связи с подвижным объектом» (направление 654 «Телекоммуникации»), а также может быть использовано в учебном процессе других радиотехнических и связных специальностей (200700, 200800) при изучении дисциплин «Устройства СВЧ». Описаны элементы библиотеки базовых элементов, даны контрольные задания, указания и рекомендации по их решению и оформлению.