ально разнесенные средства обработки (например, программно-аппаратный комплекс другого УЦ). Такая схема называется (*t, n*)-пороговой схемой разделения секрета, где *n* – количество участников, среди которых распределяются части ключа; *t* – количество участников, которые смогут восстановить секретный ключ, «объединив» свои части по определенному алгоритму. Таким образом, противник, даже получив (скомпрометировав) несколько частей, составляющих секретный ключ (но в количестве, меньшем порогового числа), не сможет корректно восстановить ключ УЦ, причем здесь обеспечивается совершенная секретность в смысле теоретико-информационной стойкости. Еще более усложнить задачу противника по восстановлению секретного ключа из составляющих его частей можно путем периодической смены уравнения (в случае схемы разделения секрета Шамира), по которому вычисляются части ключа и восстанавливается секретный ключ. При этом сам секретный ключ не изменяется, а части ключа, полученные по различным уравнениям, никак не связаны между собой. Вследствие этого противнику для корректного восстановления секретного ключа необходимо скомпрометировать не менее *t* частей, полученных по одному уравнению. Таким образом, оцениваемый период смены упомянутого уравнения должен быть менее оцениваемого времени, необходимого противнику для компрометации *t* частей ключа. Еще одним плюсом данного метода (помимо упоминавшейся совершенной секретности) является повышенная стойкость к злоумышленным действиям со стороны законных участников схемы, так как для восстановления секретного ключа необходимо объединиться не менее чем *t* участникам. Из недостатков метода можно выделить необходимость в некоторых схемах наличия секретного аутентичного канала для распределения частей общего секрета.

Э.Ф. Зорин, А.В. Федченко
Россия, г. Юбилейный, Московской обл., 4 ЦНИИ МО РФ

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ КОНТРОЛЯ НАКОПЛЕНИЯ ИНФОРМАЦИИ В БАЗЕ ДАННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Одним из основных элементов информационно–телекоммуникационных систем являются их базы данных. При этом процесс накопления информации в базе данных может быть представлен следующим образом. В каждый момент времени в базу данных коммуникационной системы поступают данные, интенсивность поступления которых равна $\lambda(t)$. В то же время в каждый последующий момент времени данные из базы данных могут изыматься с интенсивностью $\mu(t)$. Будем полагать также, что как входной поток информационных данных, так и поток изъятия данных из базы данных в канале являются пуассоновскими. Таким образом, процесс, протекающий в информационно–телекоммуникационной системе, является марковским с непрерывным временем и дискретными состояниями. Множество этих состояний $(x_0, x_1, x_2, \ldots, x_n)$ ставится в однозначное соответствие с рядом целых неотрицательных чисел $(0, 1, 2, \ldots, n)$, характеризующих количество данных, накопленных в базе. Введенные допущения на практике приводят к относительно небольшим погрешностям (~ 15%), что соизмеримо с точностью данных, закладываемых в модель.

Для любого состояния этого процесса (за исключением граничных точек x_0 и x_n), соседними могут быть только те, индексы которых отличаются от индекса рассматриваемого состояния на величину ± 1.

Граф состояний процесса накопления информации в базе данных показан на рис. 1. С учетом изложенного, процесс накопления информации в базе данных представляет собой скачкообразную случайную функцию ***X(t)***, скачки которой могут принимать значения ***± 1***, в случае, если функция ***X(t)*** отлична от ***0*** и ***n***. Если функция ***X(t) = 0*** (в базе данных нет информации), то скачок будет иметь значение ***(+ 1)***. Если функция ***X(t) = n*** (база данных полностью заполнена информацией), то скачок принимает значение ***(– 1)***.

Рис. 1. Граф состояний процесса накопления информации в базе данных.

Одна из возможных реализаций процесса накопления информации ***X(t)*** в базе данных представлена на рис. 2.

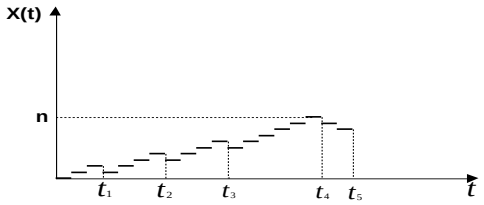

Рис. 2. Реализация процесса накопления информации в базе данных.

Предположим также, что интенсивности потоков входной и выходной информации являются постоянными величинами. В этом случае, каждая принятая в базу данных информация будет находиться в ней случайное время ***t***, распределенное по показательному закону с математическим ожиданием

$$M[t]=\frac{1}{\mu}$$

Граф состояний процесса накопления информации в базе данных будет иметь вид, представленный на рис. 3.

Рис. 3. Граф состояний процесса накопления информации в базе данных при $\lambda_k = \lambda$, $\mu_k = k\mu$.

Тогда в соответствии с приведенным графом состояний базы данных система дифференциальных уравнений для вероятностей состояний базы данных будет иметь вид [1]:

$$\frac{dP_0(t)}{dt}=-\lambda P_0(t)+\mu P_1(t);$$

……..

$$\frac{dP_k(t)}{dt}=-(\lambda+k\mu)P_k(t)+\lambda P_{k-1}(t)+(k+1)\mu P_{k+1}(t), \qquad (1)$$

где $P_k(t)=P(X(t)=k)$, k=0, 1, 2, …, n.

Найдем математическое ожидание случайной функции ***X(t)***, для чего правую и левую части уравнения (1) умножим на ***k*** и, проведя суммирование по ***k***, получим

$$\sum_{k=0}^{\infty}\frac{kdP_k(t)}{dt}=\sum_{k=0}^{\infty}k\left[-\left(\lambda+k\mu\right)P_k(t)+\lambda P_{k-1}(t)+(k+1)d_{k+1}(t)\right] \quad (2)$$

Введем обозначения:

$$m_x(t)=\sum_{k=0}^{\infty}kP_k(t) \qquad \sum_{k=0}^{\infty}P_k(t)=1$$

Тогда, при принятых допущениях постоянства величин λ и μ получим

$$m_x(t)=\frac{\lambda}{\mu}\left(1-e^{-\mu t}\right)+m_{x_0}e^{-\mu t} \quad (3)$$

Учитывая, что $m_{x_0}=0$, получим следующее выражение для определения математического ожидания случайной функции ***X(t)***, характеризующей процесс накопления информации в базе данных

$$m_x(t)=\frac{\lambda}{\mu}\left(1-e^{\mu t}\right) \quad (4)$$

Для определения дисперсии случайной функции ***X(t)*** воспользуемся соотношением

$$D_x(t)=\alpha_{2x}(t)-[m_x(t)]^2 \quad (5)$$

где $\alpha_{2x}(t)$ – второй начальный момент случайной функции ***X(t)***;

$m_x(t)$ – математическое ожидание случайной функции ***X(t)***.

Дифференцируя выражение (5) и учитывая, что

$$\frac{dm_x(t)}{dt}=\lambda-\mu m_x(t)$$

получим следующее дифференциальное уравнение для определения дисперсии случайной функции ***X(t)***

$$\frac{dD_x(t)}{dt}=-2\mu D_x(t)+\mu m_x(t)+\lambda \quad (6)$$

Решая дифференциальное уравнение (6) при начальных условиях $m_x(0)=0$ и $D_x(0)=0$, получим следующее соотношение для определения дисперсии случайной функции ***X(t)***, являющейся второй важной характеристикой процесса накопления информации в базе данных коммуникационной системы

$$D_x(t)=\frac{\lambda}{\mu}\left(1-e^{-\mu t}\right) \quad (7)$$

Из полученного соотношения следует, что дисперсия случайной функции ***X(t)***, имеющей распределение Пуассона, численно равна ее математическому ожиданию, т.е.

$$D_x=m_x \quad (8)$$

В случае, если объем информации в базе данных коммуникационной подсистемы ограничен и равен ***n***, дифференциальные уравнения для математического ожидания и дисперсии накопленной информации в базе данных будут иметь вид:

$$\frac{dm_x(t)}{dt}=\lambda-m_x(t)-\lambda P_n(t) \quad (9)$$

$$\frac{dD_x(t)}{dt}=-2\mu D_x(t)+\mu m_x(t)+\lambda-\lambda P_n(t)\left(1+2n-2m_x(t)\right) \quad (10)$$

Полученные соотношения в дальнейшем могут быть использованы для приближенного определения объема информации в базе данных и времени ее заполнения до требуемого уровня.

Реализация математической модели предоставляет возможность контроля накопления информации в базе данных, что способствует обнаружению несанкционированных воздействий на информационно–телекоммуникационные системы в процессе их функционирования и предопределяет необходимость принятия соответствующих мер по защите информации от несанкционированного доступа.

Библиографический список

1. *Овчаров Л.А., Селетков С.Н.* Автоматизированные банки данных. Москва, «Финансы и статистика», 1982.

А.В. Власенко, В.Г. Смирнов
Россия, г. Краснодар, Кубанский ГТУ

ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО ОТКРЫТЫМ КАНАЛАМ СВЯЗИ

С развитием правовой базы в России конкурентная борьба принимает все более и более цивилизованный вид. Намного безопаснее задавить и разорить конкурента, владея оперативной информацией о нем, его деятельности, партнерах, перспективах развития. Такая информация позволяет занять лидирующее положение на рынке. Предприятия добывают информацию о конкурентах из открытых источников (печатные издания, судебные тяжбы, найм на работу бывших сотрудников интересующей фирмы); путем промышленного шпионажа (прослушивания линий связи, регистрация наводок цепей питания); агентурным способом (внедрение своего сотрудника в конкурирующую фирму). Каждый из этих способов добывания информации по-своему опасен, но необходимо закрывать информацию от утечки, каким бы вариантом добывания информации не воспользовался злоумышленник.

Необходимо учитывать то, что практически вся информация на предприятиях и организациях хранится на носителях, причем этими носителями могут быть как традиционная бумага, так и дискеты, жесткие диски и т.п. Также эта информация хранится и обрабатывается на компьютерах, циркулирует в локально-вычислительных сетях, передается по открытым линиям связи партнерам. Все эти факты требуют от владельцев и руководства предприятий жить и работать по следующему принципу: Сохранность и конфиденциальность секретной информации есть благополучие собственника этой информации. Проведем анализ некоторых продуктов защиты информации, циркулирующей по открытым каналам связи. Защищенная электронная почта X.400 на базе электронного почтамта Messenger 400 (M400) фирмы Infonet Software Solutions (ISS) предназначена для предоставления абонентам почтовых услуг по обмену защищенными (зашифрованными и подписанными) сообщениями с использованием механизма двусторонней аутентификации абонента на почтамте и почтамта на абонентском пункте, реализованного с помощью ЭЦП. Защищенная электронная почта X.400 способна устойчиво функционировать в различных сетях, в том числе на недорогих низкоскоростных линиях, и использовать различные протоколы связи, включая X.25, X.28, TCP/IP, IPX/SPX и другие. Система хранения и передачи сообщений поддерживает развитые средства маршрутизации, обеспечивающие возможность оптимальной производительности и настройки с целью уменьшения стоимости коммуникационных услуг. Использование сервисов, предусмотренных стандартом X.400, а именно квитанций о доставке и прочтении, гарантированной доставке и маршрутизации, является большим преимуществом данной почтовой системы по сравнению с другими системами. Другой продукт, представленный на российском рынке, – защищенная электронная Интернет-почта Курьер-А(В), разработана российской компа-