9. **Гидрофобизация.** Теория и практика / В. Сураев // Технологии строительства. – 2002. – № 1. – С. 120–121.

10. **Гидрофобизация** / А. А. Пащенко. – Киев : Наук. думка, 1973. – 174 с.

11. **Кремнийорганические** гидрофобизаторы в строительстве / А. А. Пащенко. – Алма-Ата : Казахстан, 1968. – 178 с.

12. **Гидрофобизация** зданий / О. А. Лукинский // Жилищное строительство. – 2008. – № 11. – С. 21–23.

13. **Способы** оценки влияния поверхностной гидрофобизации бетона и модифицирующих его структуру добавок / Л. П. Орентлихер, И. П. Новикова, И. И. Лифанов, Э. Н. Юрченко // Бетон и железобетон. – 1991. – № 2 (431). – С. 28–30.

14. **Ультразвуковой** контроль глубины пропитки пористого материала гидрофобизирующим раствором : дис. … канд. техн. наук / С. В. Николаев. – Санкт-Петербург : СЗТУ, 2006. – 199 с.

15. **Обеспечение** эффективной гидрофобной защиты неорганических строительных материалов : дис. … канд. техн. наук / С. Г. Ершова. – Новосибирск : Сибстрин, 2006. – 174 с.

УДК 004.056.53

А. А. Привалов, Н. В. Евглевская
Петербургский государственный университет путей сообщения Императора Александра I

К. Н. Зубков
ООО «Телесофт»

МОДЕЛЬ ПРОЦЕССА ВСКРЫТИЯ ПАРАМЕТРОВ СЕТИ ПЕРЕДАЧИ ДАННЫХ ОПЕРАТОРА IP–ТЕЛЕФОННОЙ СЕТИ КОМПЬЮТЕРНОЙ РАЗВЕДКОЙ ОРГАНИЗОВАННОГО НАРУШИТЕЛЯ

Проведенный анализ показал, что информационные воздействия на технологические процессы организуются на основе данных, извлеченных организованным нарушителем из информации, циркулирующей в инфокоммуникационных сетях и обрабатываемой на объектах информатизации. Рассмотрена модель процесса вскрытия параметров сети передачи данных оператора IP-телефонной сети компьютерной разведкой организованного нарушителя. Данная модель позволяет учитывать особенности конфигурации IP-телефонных сетей и количественно оценивать длительность цикла управления, необходимого организованному нарушителю для получения всех требующихся разведданных, а также определить требования к периодичности контроля безопасности информации с целью обеспечения заданного уровня защищенности.

стохастическая сеть, эквивалентная функция, организованный нарушитель, метод топологического преобразования стохастических сетей.

Введение

Несанкционированные воздействия на компьютерные сети как коммерческих организаций и федеральных структур, так и крупных промышленных объектов осуществляются на основе данных, добываемых организованным нарушителем с использо-

ванием средств компьютерной и агентурно-технической разведки. В литературе встречаются статьи, в которых приведены модели компьютерной разведки, однако эти модели ориентированы на анализ защищенности объектовых локальных вычислительных сетей, а получаемые в ходе моделирования результаты не могут быть использованы для оценки информационной безопасности IP-телефонных сетей, получивших широкое распространение.

Для операторов IP-телефонной сети, обеспечивающих передачу голосового трафика, последствия компьютерных атак, успешно проведенных организованным нарушителем, могут привести не только к финансовым потерям, но и повлиять на репутацию компании путем нарушения доступности и качества предоставляемых услуг телефонной связи абонентам.

На объекте информатизации сталкиваются интересы двух противоборствующих сторон: организованного нарушителя и системы управления безопасностью. С одной стороны, организованный нарушитель воздействует на телекоммуникационную сеть в течение времени t_1 с целью осуществления основных этапов компьютерной разведки с последующей реализацией атаки. С другой стороны, система управления безопасностью обнаруживает несанкционированные действия нарушителя и осуществляет необходимые меры по противодействию за некоторое время t_2. Как показывает практика, воздействия со стороны системы управления безопасностью оказываются с задержкой, а чаще всего – постфактум, когда организованный нарушитель уже достиг поставленной цели.

Для получения данных об IP-сети организованный нарушитель реализует следующие этапы компьютерной разведки:

1. Обнаружение сети и осуществление первичного доступа к ней путем анализа сетевого трафика для определения паролей доступа, передаваемых по сети.

2. Сбор информации о сети, включающий в себя:

– идентификацию узлов сети;

– сканирование портов и идентификацию сетевых сервисов;

– установление типа и версии операционной системы;

– определение технической роли узла.

3. Получение привилегированных прав доступа к целевым узлам сети.

4. Скрытие следов проникновения в сеть посредством удаления соответствующих записей в журналах регистрации, а также организация постоянного доступа («черного хода») к объекту воздействия.

Авторами статьи разработана модель первых двух этапов компьютерной разведки, поскольку разведданные, полученные в результате ее успешной реализации, являются достаточными для осуществления выбора деструктивных воздействий на телекоммуникационную сеть организованным нарушителем.

С целью определения и последующей оценки времени, необходимого организованному нарушителю для получения всех разведданных об IP-сети, необходимо поставить и решить следующую задачу.

1 Постановка задачи

Пусть на объекте оператора IP-телефонной сети развернута имеющая в своем составе m узлов беспроводная сеть, к которой организованный нарушитель осуществляет первичный доступ посредством перехвата и анализа сетевого трафика за случайное время t_e с функцией распределения $E(t)$.

После успешной реализации перехвата сетевого трафика нарушитель с вероятностями P_d, P_n и P_v приступает к получению IP-адресов сетевых узлов, данных о портах и сетевых сервисах, а также типе и версии операционной системы за случайное время t_d, t_n, t_v с функциями распределения $D(t)$, $N(t)$ и $V(t)$ соответственно. Функции распределения $D(t)$, $N(t)$ и $V(t)$ определяются с использованием ранее разработанных моделей [1]. В противном случае указанные процессы возобновляются с вероятностями $(1 - P_d)$, $(1 - P_n)$ и $(1 - P_v)$ через некоторое случайное время паузы t_1, t_2, t_3 с функциями распреде-

ления $B_1(t)$, $B_2(t)$ и $B_3(t)$ соответственно. При успешном исходе нарушитель анализирует все полученные данные за некоторое случайное время t_a с функцией распределения $A(t)$ и принимает решение о технической роли сетевых узлов.

Требуется определить среднее время T и функцию распределения $F(t)$ времени вскрытия параметров сети передачи данных оператора IP-телефонной сети организованным нарушителем в условиях ведения компьютерной разведки.

2 Разработка модели процесса вскрытия параметров сети передачи данных оператора IP-телефонной сети

Представим описанный выше процесс в виде стохастической сети (рис. 1).

Эквивалентная функция стохастической сети (рис. 1), определяемая с использованием уравнения Мэйсона [2], имеет вид:

$$Q(s) = \frac{e(s)\cdot d(s)\cdot P_1\cdot n(s)\times}{1-x(s)-y(s)-z(s)+x(s)y(s)+} \quad (1)$$
$$\frac{\times P_2\cdot v(s)\cdot P_3\cdot a(s)}{+x(s)z(s)+y(s)z(s)-x(s)y(s)z(s)},$$

где $x(s) = d(s)\cdot(1-P_1)\cdot b_1(s)$;

$y(s) = n(s)\cdot(1-P_2)\cdot b_2(s)$;

$z(s) = v(s)\cdot(1-P_3)\cdot b_3(s)$;

$f(s) = \int_0^\infty F(t)\exp(-st)dt$ – преобразование Лапласа функций распределения времени реализации частных процессов.

Предполагая, что функции распределения времени реализации частных процессов относятся к классу экспоненциальных и проведя соответствующие преобразования, получим:

$$Q(s) = \frac{e\cdot d\cdot P_1\cdot n\cdot P_2\cdot v\cdot P_3\cdot a\times}{(a+s)\cdot(e+s)\cdot(s^6+A\cdot s^5+} \quad (2)$$
$$\frac{\times(b_1+s)\cdot(b_2+s)\cdot(b_3+s)}{+B\cdot s^4+C\cdot s^3+D\cdot s^2+E\cdot s+H)},$$

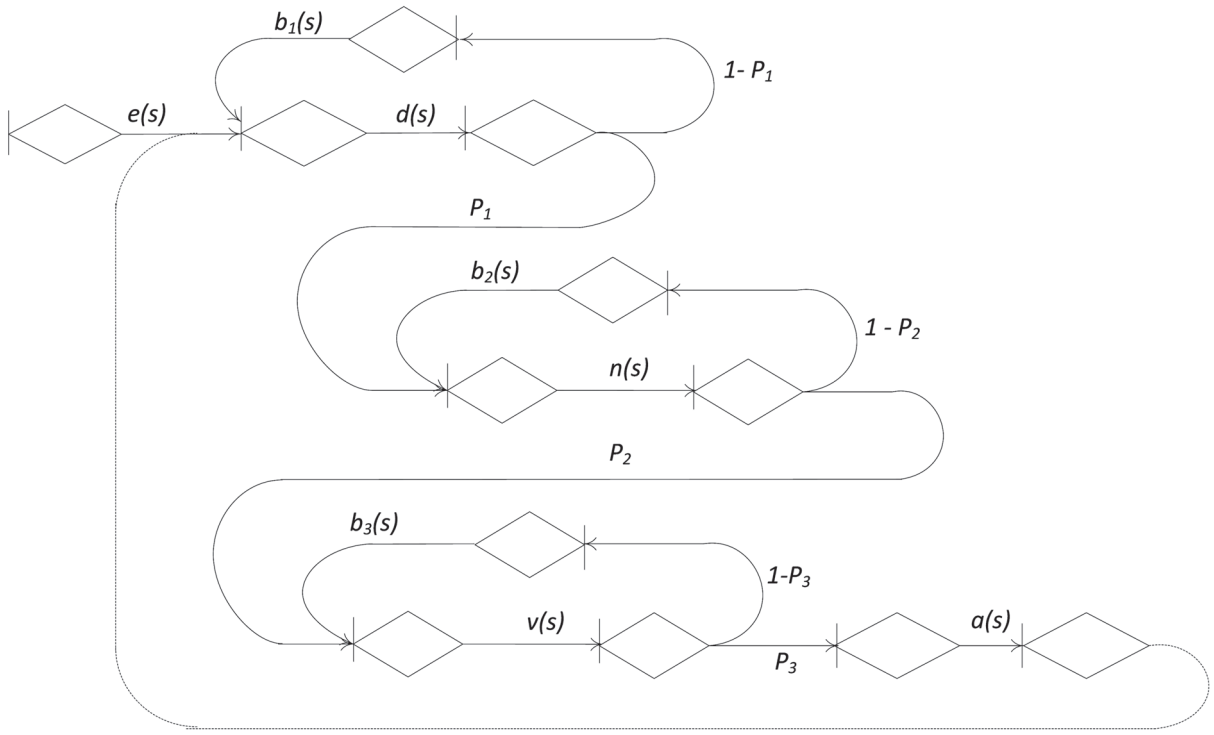

Рис. 1. Стохастическая сеть процесса вскрытия сети передачи данных оператора IP-телефонной сети нарушителем

где $e=1/t_e$; $d=1/t_d$; $n=1/t_n$; $v=1/t_n$; $a=1/t_a$; $b_1=t_1$; $b_2=1/t_2$; $b_3=1/t_3$ – среднее время перехвата и анализа сетевого трафика; установление IP-адреса узла сети; сканирования портов и идентификации сетевых сервисов; определения типа и версии операционной системы узла сети; анализа полученных данных и принятия решения о технической роли разведуемого узла сети, паузы перед повторной попыткой перехвата сетевого трафика, сканирования портов, определения типа ОС соответственно.

$$A := d + v + b_2 + b_3 + b_1 + n;$$

$$B := b_1 v + db_2 + vb_3 P_3 + db_1 P_1 + b_2 nP_2 + b_2 b_3 + b_2 v + db_3 + b_1 b_2 + nb_3 + b_1 n + b_1 b_3 + dn + nv + dv;$$

$$C := vb_3 P_3 (d + b_1) + db_1 P_1 b_3 + b_2 nP_2 (d + b_1) + b_2 nP_2 (b_1 + v + b_3) + db_2 (v + b_3) + b_1 b_2 b_3 + vb_3 P_3 (n + v) + dnv + nb_3 (b_1 + d) + db_1 P_1 (b_2 + v + n) + b_1 v(n + b_2);$$

$$D := b_2 nvP_2 P_3 + db_1 P_1 nv + db_1 P_1 (nb_3 + b_2 v) + vb_3 P_3 (db_2 + n + b_1 b_2 + dn) + db_1 b_2 P_1 P_2 (n + d) + db_1 vb_3 P_1 P_3 + b_2 nP_2 (db_3 + b_1 v + dv + b_1 b_3);$$

$$E := db_1 b_2 P_1 P_2 (nv + nb_3 + vb_3) + b_2 nvb_3 P_2 P_3 (d + b_1) + db_1 vb_3 P_1 P_3 n;$$

$$H := db_1 nb_2 vb_3 P_1 P_2 P_3 \_$$

коэффициенты разложения

Для определения оригинала $Q(s)$ используем разложение Хевисайда, позволяющее при $s_1 \neq s_2$ представить выражение (2) в виде суммы вычетов в полюсах s_k, $k = \overline{1,8}$:

$$Q(s) = \sum_{k=1}^{8} \frac{f(s_k)}{\varphi'(s_k)} \cdot \frac{1}{s - s_k}, \qquad (3)$$

где $s_1 = -a$; $s_2 = -e$;

$$s_{3,4} = -\frac{1}{2}(b_3 + v \pm \sqrt{4vb_3 P_3 - (b_3 + v)^2};$$

$$s_{5,6} = -\frac{1}{2}(b_2 + n \pm \sqrt{4nb_2 P_2 - (b_2 + n)^2};$$

$$s_{7,8} = -\frac{1}{2}(d + b_1 \pm \sqrt{4db_1 P_1 - (d + b_1)^2};$$

$$f(s) = e \cdot d \cdot P_1 \cdot n \cdot P_2 \cdot v \times \times P_3 \cdot a \cdot (b_1 + s) \cdot (b_2 + s) \cdot (b_3 + s);$$

$$\varphi(s) = (a + s) \cdot (e + s) \cdot (s^6 + A \cdot s^5 + B \cdot s^4 + C \cdot s^3 + D \cdot s^2 + E \cdot s + H).$$

Определив оригинал (3), используя таблицы соответствия [3], и проинтегрировав полученный результат с переменным верхним пределом, получим искомую функцию распределения:

$$F(t) = \sum_{k=1}^{8} \frac{f_k(s_k)}{\varphi'_k(s_k)} \cdot \frac{1 - e^{s_k t}}{-s_k}. \qquad (4)$$

В свою очередь, среднее время, затрачиваемое организованным нарушителем на получение всех разведданных об IP-телефонной сети:

$$\mathrm{T} = \int_0^{\infty} td\left[F(t)\right] = \sum_{k=1}^{5} \frac{f_k(s_k)}{\varphi'_{\ddot{e}}(sk) s_k^2}. \qquad (5)$$

3 Результаты моделирования

По формулам (4) и (5) произведены расчеты, результаты которых представлены в виде графиков на рис. 2 и 3.

При расчетах предполагалось, что среднее время добывания данных о сети передачи данных t_e = 120 мин; t_d = 60 мин; t_n = = 40 мин; t_a = 90 мин; $b_1 = b_2 = b_3$ = 30 мин. Указанные временные величины были получены на основе данных промежуточного моделирования [1]. Значения вероятностей установления IP-адреса узла сети, идентификации сетевых сервисов и определения типа

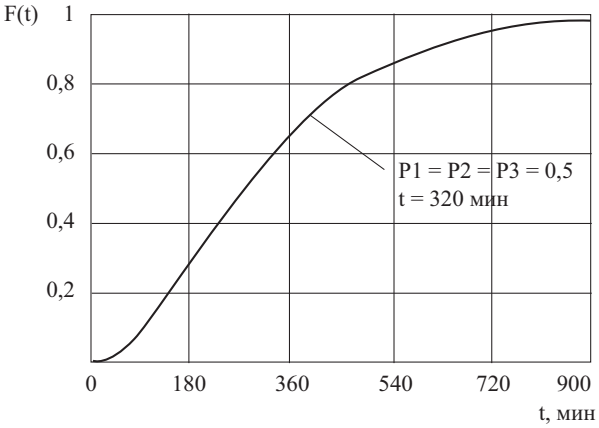

Рис. 2. Функция распределения времени, необходимого организованному нарушителю для получения данных о сети при одинаковых вероятностях осуществления этапов компьютерной разведки

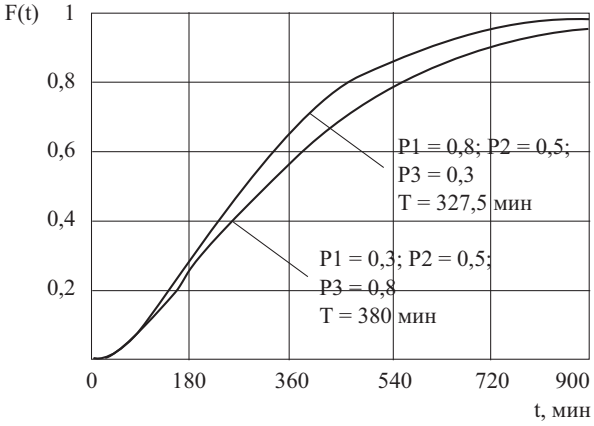

Рис. 3. Функция распределения времени, необходимого организованному нарушителю для получения данных о сети при различных вероятностях осуществления этапов компьютерной разведки

операционной системы сетевого узла с $P1$, $P2$ и $P3$ принимались равными 0,3; 0,5 и 0,8.

Анализ полученных результатов показал, что:

– разработанная модель является работоспособной, чувствительной к изменению исходных данных, адекватно отображает процесс вскрытия параметров сети передачи данных оператора IP-телефонной сети системой компьютерной разведки и позволяет определить вероятностно-временные характеристики процесса компьютерной разведки организованного нарушителя;

– полученные в ходе моделирования значения среднего времени, необходимого организованному нарушителю для осуществления компьютерной разведки, позволяют проводить оценку влияния различных параметров на защищенность сети передачи данных и количественно оценивать уровень ее защищенности после реализации предпринятых мер защиты сети от компьютерной разведки.

Заключение

Таким образом, в статье предложена математическая модель процесса вскрытия параметров сети передачи данных оператора IP-телефонной сети компьютерной разведкой организованного нарушителя, позволяющая учесть особенности проведения компьютерной разведки при вскрытии параметров IP-телефонных сетей с использованием ранее разработанных авторами моделей [5]. В общем случае предлагаемая модель может быть использована для анализа разведзащищенности и других, в том числе и мультимедийных TCP/IP, сетей при условии корректировки исходных данных, характеризующих анализируемую сеть.

Полученные в ходе моделирования результаты позволяют оценить время, необходимое нарушителю для оказания воздействия на защищаемую сеть, и определить требования к периодичности и глубине контроля информационной безопасности.

Библиографический список

1. **Метод** топологического преобразования стохастических сетей и его использования для анализа систем связи ВМФ / А. А. Привалов. – Санкт-Петербург : ВМА, 2001. – 186 с.

2. **IP-телефония /** В. С. Гольдштейн, А. В. Пинчук, А. Л. Суховицкий. – Москва : Радио и связь, 2001. – 336 с.

3. **Таблицы** интегральных преобразований / Г. Бейтмен, А. Эрдейи. Т. 1. Преобразования Фурье, Лапласа, Мелина ; пер. с англ. Н. Я. Вилей-

кина. Серия «Справочная математическая библиотека». – Москва : Наука, 1969. – 344 с.

4. **Компьютерные** сети. Принципы, технологии, протоколы : учебник для вузов. 4-е изд. / В. Г. Олифер, Н. А. Олифер. – Санкт-Петербург : Питер, 2010. – 944 с.

5. **Моделирование** комплексов радиоразведки и радиоподавления вооруженных сил зарубежных государств / В. Н. Куделя, В. Е. Кузнецов, А. М. Лихачев, В. В. Масановец, А. А. Привалов. – Санкт-Петербург : Военный Университет Связи, 2004. – 156 с.

УДК 621.396.933.2

Е. В. Соболев, Ал-Рубой Мудар, Е. А. Рубцов
Санкт-Петербургский государственный университет гражданской авиации

ВЫБОР РАЦИОНАЛЬНОГО СОСТАВА И РАЗМЕЩЕНИЯ РАДИОМАЯКОВ VOR/DME В РЕСПУБЛИКЕ ИРАК ДЛЯ ОБЕСПЕЧЕНИЯ ЗОНАЛЬНОЙ НАВИГАЦИИ

Оценена степень покрытия воздушных трасс зонами действия сети маяков VOR/DME (при расчете зон действия учитывался сложный характер рельефа, влияющий на дальность действия РТС). По результатам анализа сделан вывод, что инфраструктура РТС навигации недостаточна для выполнения полетов по концепции зональной навигации. Предложено дооснастить аэродромы, на которых уже есть маяки VOR, дальномерным оборудованием DME, а также внедрить дополнительные навигационные маяки VOR/DME. Анализ зон действия для новой конфигурации маяков показал, что при этом обеспечивается стопроцентное покрытие воздушных трасс для высоты полета 10 000 м, а также трехкратное повышение степени покрытия воздушных трасс по сравнению с существующей ситуацией для высоты полета 6000 м.

зона действия, VOR/DME, зональная навигация.

Введение

Государство Ирак обладает большим экономическим потенциалом. На территории страны сосредоточено около 10 % мировых запасов нефти, имеются месторождения природного газа, велика площадь сельскохозяйственных земель, бассейны рек Тигр и Евфрат удовлетворяют потребность в водных ресурсах. Выгодное географическое положение страны способствует развитию внутренних и внешних воздушных сообщений.

Однако данный потенциал был практически полностью нивелирован политическими и социальными конфликтами последних десятилетий: Ирано-Иракской войной (1980–1988 гг.), оккупацией Кувейта (1990–1991 гг.), гражданской нестабильностью: репрессиями против шиитского и курдского населения со стороны правительства и последующей войной, закончившейся вводом в страну сил Коалиции и свержением режима Саддама Хусейна.

Сложная военно-политическая обстановка в Ираке сохраняется по сей день: экстремистские и террористические группировки продолжают совершать теракты и нападения.

Несмотря на это, в настоящее время идет полномасштабное восстановление экономики страны. Вследствие изменения полити-