УДК 004.056.53

А. А. Привалов, Ал. А. Привалов, Е. В. Скуднева, И. В. Чалов

ПОДХОД К ОЦЕНКЕ ВЕРОЯТНОСТИ ВСКРЫТИЯ ПРОСТРАНСТВЕННО-ВРЕМЕННОЙ И ИНФОРМАЦИОННОЙ СТРУКТУРЫ СПД-ОТН

Дата поступления: 06.07.2015
Решение о публикации: 06.07.2015

Цель: Разработать подход и определить вероятность вскрытия пространственно-временной и информационной структуры СПД-ОТН ОАО «РЖД» в ходе реализации APT нарушителем. **Методы:** Для решения задачи использованы методы теории графов, метод топологического преобразования стохастических сетей и метод математического моделирования систем и процессов связи. **Результаты:** Разработана вербальная модель целевой атаки нарушителя, методика оценки структурной скрытности сети передачи данных, включающая алгоритм расчета накопленной вероятности вскрытия автоматизированного рабочего места, распознавания структуры сети передачи данных для графов-эталонов и графов-реализаций, а также обобщенный алгоритм оценки структурной скрытности. **Практическая значимость:** Данный алгоритм ориентирован на включение в состав специального математического программного обеспечения системы управления информационной безопасности для оценки возможности нарушителя при реализации таргетированных атак. Этот подход соответствует этапу сбора информации, наблюдению и выбору нарушителем более успешного момента для осуществления целевой атаки. Разработанные алгоритмы позволяют определить место и время реализации нарушителем типовых угроз, с помощью которых он выявляет вид технологического процесса и определяет наиболее подходящий момент для деструктивного воздействия. Проведенная работа показывает необходимость включения алгоритмов в перечень информационно-расчетных задач системы поддержки принятия решения, что позволит проводить более глубокий анализ возможностей нарушителя и осуществления целевых атак. Алгоритм соответствует логике действий нарушителя при вскрытии сети и системы в целом и может быть использован не только для оценки защищенности, но и для прогнозирования действий нарушителя по вскрытию сети.

Сеть передачи данных, структурная скрытность, нарушитель, таргетированная атака, телекоммуникационная сеть.

Andrey A. Privalov, D. Sci. (Military), professor, aprivalov@inbox.ru (Petersburg State Transport University), **Aleksandr A. Privalov,** Cand. Sci. (Physics and Mathematics), associate professor (Moscow State Pedagogical University), ***Yekaterina V. Skudneva,** postgraduate student, evskudneva@yandex.ru, **Igor V. Chalov**, student, igorchalov4@mail.ru (Petersburg State Transport University)
APPROACH TO THE ASSESSMENT PROBABILITIES OF BREAKING INTO SPACE-TIME AND INFORMATION STRUCTURE OF DATA TRANSMISSION'S NETWORK OF OPERATIONAL AND TECHNOLOGICAL USE

Objective: To develop an approach and to assess the probability of breaking into space-time and information structure of Russian Railways JSC's data transmission network of operational and technological use by a violator carrying out advanced persistent threats. **Methods:** Graph theory methods, method of topological transformation of stochastic networks, and method of mathematical simulation of systems of communication processes were used to solve the problem. **Results:** A verbal model of a targeted attack by a violator was developed, as were a method for assessing structural reserve of a data transmission network that includes an algorithm for calculation of cumulative probability of breaking into a computer work station, pattern recognition for data transmission network for master graphs and realisation graphs, and a generalised algorithm for assessment of structural reserve. **Practical importance:** The algorithm is

orientated for inclusion in specialised mathematical software for information security management system to assess a violator's opportunities during targeted attacks. This approach corresponds to the stage of data collection, observation and choice of a suitable moment for carrying out a targeted attack by a violator. Algorithms developed allow to identify the location and time of a violator carrying out typical threats during which the type of technological process is being determined and the most suitable moment for destructive influence is chosen. The paper shows the need for inclusion of algorithms in the list of information-computing tasks of the decision support system to allow for deeper analysis of a violator's possibilities and of targeted attacks. The algorithm corresponds to the logic of the violator's actions when breaking into a network and into a system as a whole, and can be used not only in assessing protection degree but also for forecasting a violator's actions in breaking into a network.

Data transmission network, structural reserve, violator, advanced persistent threats, telecommunication network.

В последнее время в специальной литературе среди компьютерных атак на автоматизированные системы критически важных объектов выделяют целевые, таргетированные или APT-атаки (advanced persistent thread – «сложные протяжённые угрозы») [3]. Отличительные особенности этих атак – целенаправленность и уникальность. Их целью является срыв основного технологического процесса. Исследования показали, что стандартные средства защиты распознавания информационных угроз не могут им противостоять [3]. Целевые атаки характеризуются сложностью, многомерностью и протяженностью во времени. Их объектом является конкретная автоматизированная система, организующая определенный целевой процесс или их совокупность.

Вербальная модель целевой атаки на сеть передачи данных

Таргетированная атака включает в себя следующие этапы: вскрытие структуры сети, тестирование элементов сети передачи данных и уничтожение следов присутствия [3].

В телекоммуникационных сетях, в частности в сети передачи данных оперативно-технологического назначения (СПД-ОТН), отображается процесс управления движением поездов или перевозочным процессом. Он проявляется в числе и времени работы корреспондентов, в объеме передаваемых данных, в местоположении источников информации и команд, что отражается в пространстве используемых IP-адресов.

При наблюдении за технологическим процессом можно установить корреспондирующие пары используемых IP-адресов, что позволяет определить место размещения абонента, с кем и когда он работает, в интересах какого этапа цикла управления перевозочным процессом происходит информационный обмен, какова его интенсивность и как это соотносится с реализуемым процессом перевозки. Для нанесения ущерба необходимо вскрыть сеть и произвести компьютерную атаку.

Центральными блоками модели целевой атаки являются: подсистемы поиска и технического анализа (сетевой сканер), контроля трафика, места определения источника информации. Полученные результаты анализируются в подсистеме обработки и управления (рис. 1).

Исследование показывает, что APT-атаки реализуют в телекоммуникационном пространстве принципы, заложенные в автоматизированной системе обработки и анализа разведывательных данных ASAS [1].

Методика распознавания структуры сети передачи данных

В ходе APT вскрытие структур обеспечивается представлением элементов телекоммуникационной сети в виде вершин графа, а

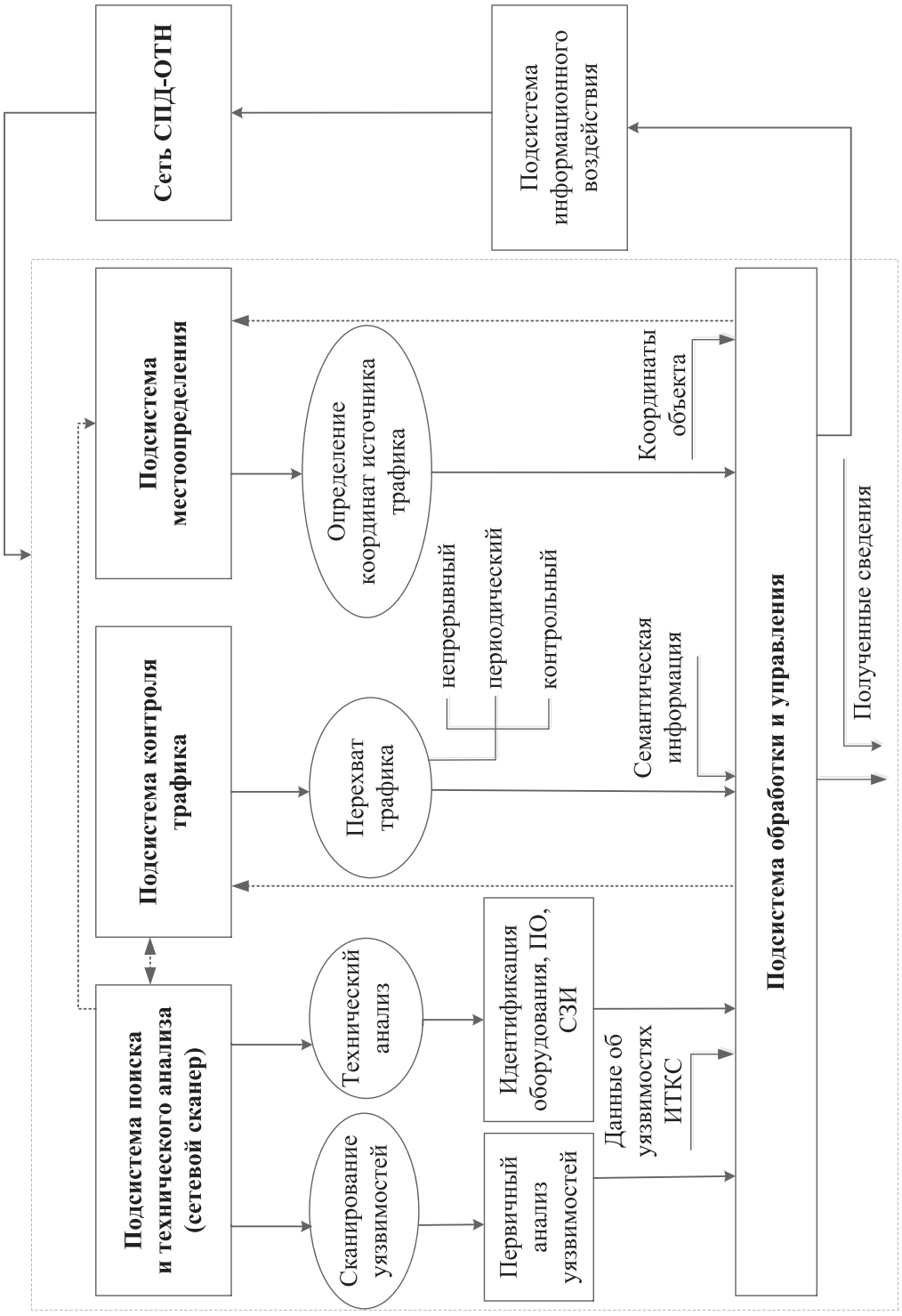

Рис. 1. Вербальная модель целевой атаки

информационные связи между ними – в виде ветвей. Таким образом формируется пространственно-временная структура, соответствующая тому или иному этапу технологического процесса, реализуемого в том числе в сети передачи данных. Зная типовые структуры, соответствующие основным технологическим процессам, нарушитель формирует базу графов-эталонов. В дальнейшем он сравнивает наблюдаемые структуры СПД-ОТН с типовой и определяет вид и этап реализуемого технологического процесса.

Так вскрывается вид деятельности органов управления ОАО «РЖД», взаимодействующих через СПД-ОТН.

Для распознавания деятельности группировок вооруженных сил со средствами радиосвязи были разработаны алгоритмы [2], однако область их применения ограничена только аналоговыми сетями радиосвязи специального назначения, поэтому авторы существенно модифицировали данные алгоритмы для распознавания структуры IP-сетей СПД-ОТН.

Исходными данными для алгоритма (рис. 2) являются типовые структуры, соответствующие основным технологическим процессам. При этом графом реализации называется исследуемая сеть, а графом-эталоном – набор типовых схем организации технологического процесса в сети СПД-ОТН.

Алгоритм распознавания структуры СПД-ОТН предусматривает представление графа в виде матрицы смежности. Алгоритм разделен на ряд этапов. На первом этапе для нахождения путей и циклов реализуется подпрограмма, использующая метод поиска в глубину. На втором этапе проверяется равенство числа вершин, числа путей (циклов) в графе и равенство степеней, генерируется матрица подстановки из проверяемых циклов. На третьем этапе находятся вершины, не входящие в исследуемые циклы, проверяется сохранение отношения смежности и равенства в них. На последнем этапе выполняются дополнения к подстановке и выводится результат распознавания.

При этом, как следует из модели, в целом успех APT-атак в основном зависит от успешного вскрытия пространственно-временной и информационной структур СПД-ОТН и АСУ перевозочным процессом.

Алгоритм оценки структурной скрытности сети передачи данных

Алгоритм оценки структурной скрытности СПД-ОТН можно использовать как для отдельных элементов ТКС, так и для сети передачи данных в целом.

Вероятность обнаружения автоматизированного рабочего места (терминала) IP-сети рассчитывается по алгоритму (рис. 3, блоки 4–9). Исходными данными являются результаты сканирования сети, которые были изложены в статье [4].

Каждый терминал передает IP-пакеты с интенсивностью λ_{ij}. Тогда вероятность реализации процесса по этому объекту к заданному моменту времени хотя бы один раз можно определить выражением [2]

$$P_i^*(t) = 1 - e^{-\sum_{j=1}^{d_i} \int_0^t \lambda_{ij} \cdot p_{ij}^*(x) dx},$$

где λ_{ij} – интенсивность передачи IP-пакетов, находится с помощью формулы

$$\lambda_{ij} = \frac{N_{ij}}{t_{\text{сеанса}}},$$

где N_{ij} – количество IP-пакетов между корреспондирующими парами; $t_{\text{сеанса}}$ – время TCP(UDP)-соединения между терминалами; $p_{ij}^*(x)$ – вероятность обнаружения IP-пакетов корреспондирующих пар; d_i – число терминалов, работающих в режиме передачи и приема IP-пакетов.

Алгоритм включает подпрограмму определения принадлежности графа реализации соответствующего СПД-ОТН к графам-эталонам.

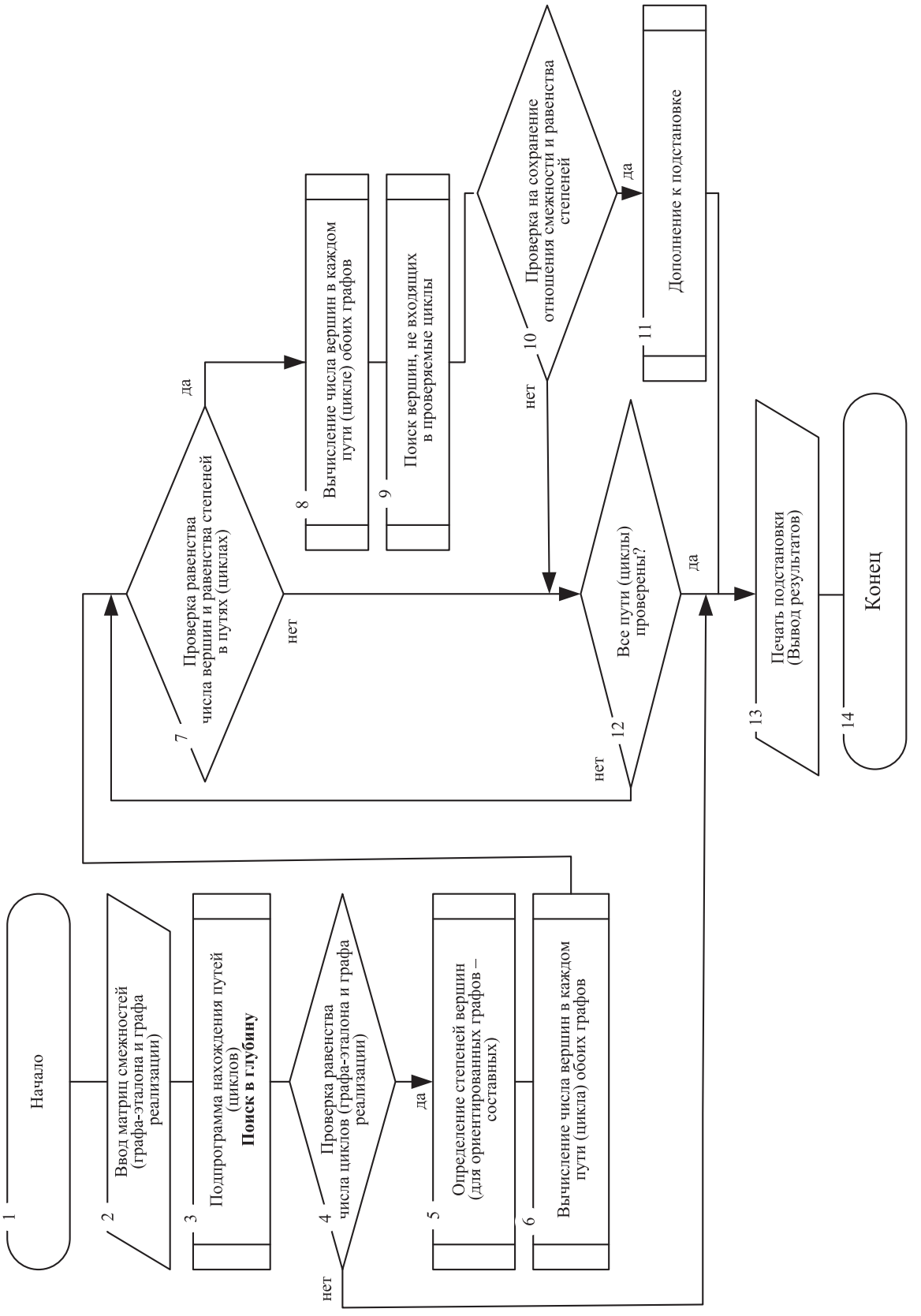

Рис. 2. Алгоритм распознавания структуры СПД-ОТН

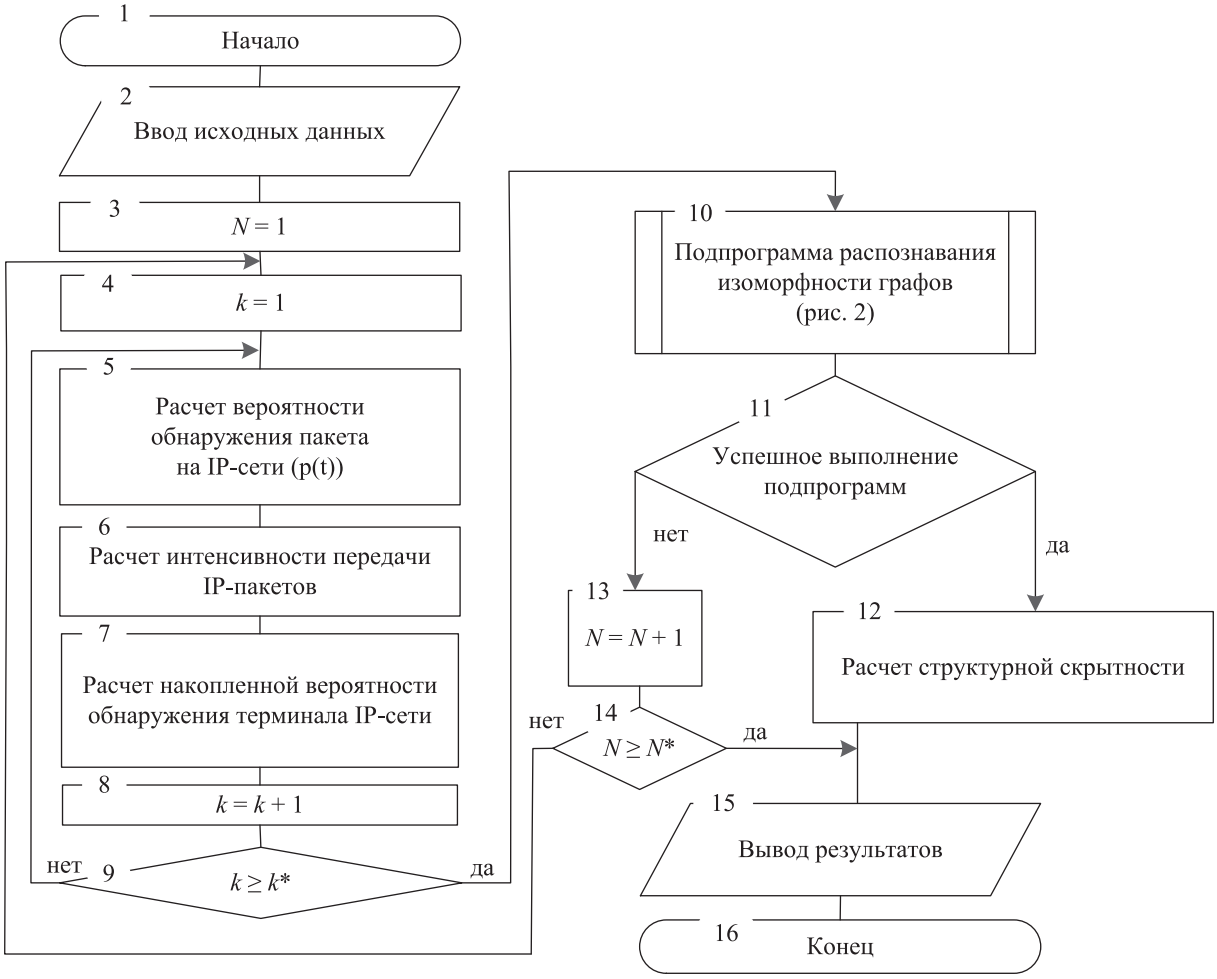

Рис. 3. Алгоритм оценки структурной скрытности сети передачи данных

В основе работы этого блока лежит процедура распознавания изоморфности вхождения (вложения) взвешенных графов: одного – получаемого в результате статистического розыгрыша СПД-ОТН, второго – графа-эталона.

При успешном выполнении подпрограмм рассчитывается показатель структурной скрытности:

$$P_{i/k} = \frac{w_i(k)}{N^*},$$

где $w_i(k)$ – число случаев, когда граф реализации относится к i-му эталону при фактическом розыгрыше k-го элемента.

Таким образом, представленные алгоритмы позволяют распознавать структуру СПД-ОТН, обнаружить терминал IP-сети, оценить структурную скрытность сети передачи данных.

Пример расчета структурной скрытности фрагмента СПД-ОТН

Рассмотрим использование представленных алгоритмов для оценки структурной скрытности на примере фрагмента сети передачи данных (рис. 4).

Рассчитаем вероятность обнаружения терминала IP-сети по алгоритму рис. 3 (блоки 4–9).

Результат работы подпрограммы представлен на рис. 5. Показана вероятность вскрытия каждого из шести участников информационного обмена IP-сети участка СПД-ОТН на определенном временно́м отрезке.

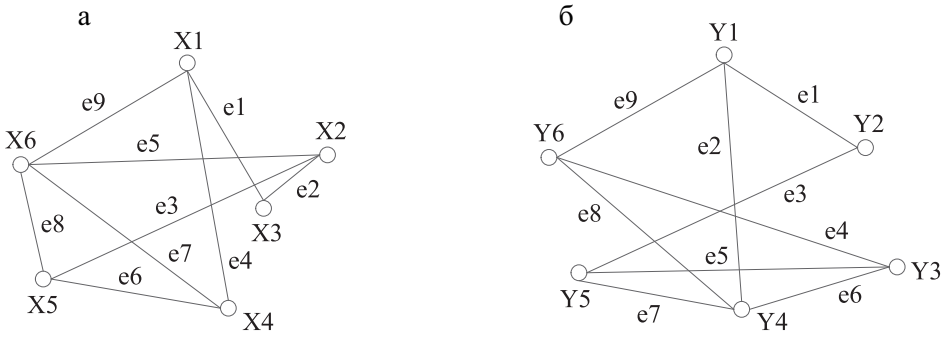

Рис. 4. Структура информационного обмена:
а) граф фрагмента сети передачи данных (1); б) граф реализации (2)

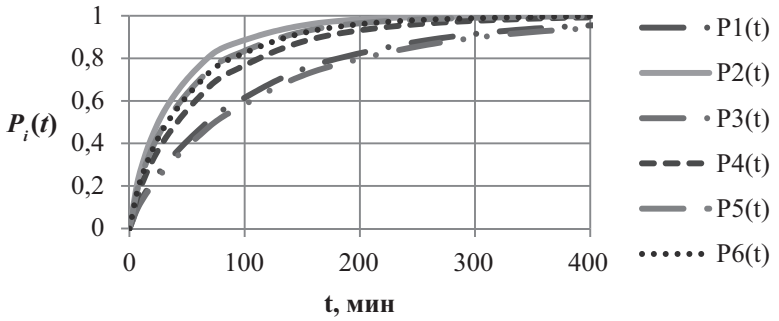

Рис. 5. Вероятость вскрытия корреспондентов IP-сети

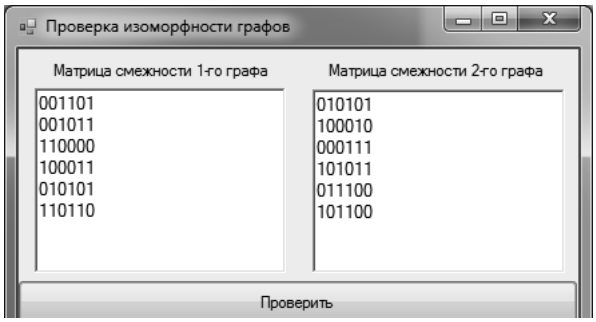

Рис. 6. Проверка изоморфности

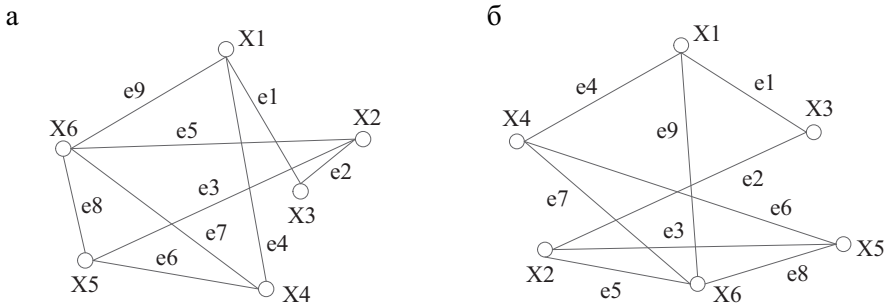

Рис. 7. Соответствие портрета и информационного обмена реализуемого процесса:
а) граф 1; б) граф 2

Распознаем структуру СПД-ОТН по алгоритму рис. 2. Результат работы подпрограммы представлен на рис. 6.

Графы, приведенные на рис. 4, записываются в виде матриц смежности. В рассматриваемом примере полученный результат говорит о том, что граф 1 и граф 2 изоморфны. Таким образом, граф соответствующий реализации определенного технологического процесса отображается в графе реализации (рис. 7).

Рассчитаем структурную скрытность по алгоритму рис. 3. Получим показатель 0,07.

Заключение

Таким образом, в СПД-ОТН процесс управления перевозками отображается в виде корреспондирующих пар, число и взаимосвязь которых раскрывается во время функционирования сети или развития целевого процесса. Нарушитель, основываясь на данных, полученных в ходе наблюдения, способен выбрать наиболее успешный момент для проведения таргетированной атаки. Целевая атака на первом этапе распознает структуру сети. Разработанные алгоритмы показывают, что нарушитель может использовать угрозы типа «сканирование сети», «анализ трафика», «анализ пространства IP-адресов», с помощью которых можно установить вид технологического процесса, определить наиболее уязвимое место и момент деструктивного воздействия для нанесения наибольшего ущерба.

Разработанные алгоритмы позволяют оценить возможности нарушителя и включить их в перечень информационно-расчетных задач системы поддержки принятия решения для проведения более глубокого анализа по возможностям нарушителя по целевым атакам.

Библиографический список

1. Греков В. Автоматизированная система обработки и анализа разведывательных данных ASAS / В. Греков // Зарубежное воен. обозрение. – 1990. – № 12. – С. 27–35.

2. Куделя В. Н. Методы математического моделирования систем и процессов связи / В. Н. Куделя, А. А. Привалов, О. В. Петриева, В. П. Чемиренко; под общ. ред. В. П. Чемиренко. – СПб. : Изд-во Политехн. ун-та, 2009.

3. Попович Д. Смерть антивируса / Д. Попович // Безопасность деловой информации. – 2014. – № 6. – С. 10–13.

4. Скуднева Е. В. Модель процесса передачи однопакетного сообщения по IP-сети / Е. В. Скуднева, Ю. С. Карабанов, В. О. Кириленко, Е. О. Болтенкова // Бюл. результатов научных исследований. – 2015. – Вып. 1 (14). – С. 84–95.

References

1. Grekov V. *Zarubezhnoye voyennoye obozreniye – Foreign Military Rev.*, 1990, Is. 12, pp. 27-35.

2. Kudelya V. N., Privalov A. A., Petriyeva O. V. & Chemirenko V. P. Metody matematicheskogo modelirovaniya sistem i protsessov svyazi [Methods of Mathematical Simulation of Communications Systems and Processes], ed. Chemirenko V. P. St. Petersburg, Polytechnical University Press, 2009.

3. Popovich D. *Bezopasnost delovoy informatsii – Bus. Inf. Secur.*, 2014, no. 6, pp. 10-13.

4. Skudneva Ye. V., Karabanov Yu. S., Kirilenko V. O. & Boltenkova Ye. O. *Byulleten rezultatov nauchnykh issledovaniy – Bull. of Res. Results*, 2015, Is. 1 (14), pp. 84-95.

ПРИВАЛОВ Андрей Андреевич – д-р воен. наук, профессор, aprivalov@inbox.ru; *СКУДНЕВА Екатерина Валентиновна – аспирант, evskudneva@yandex.ru; ЧАЛОВ Игорь Владимирович – студент, igorchalov4@mail.ru (Петербургский государственный университет путей сообщения Императора Александра I); ПРИВАЛОВ Александр Андреевич – канд. физ.-мат. наук, доцент (Московский педагогический Государственный университет).