DOI: https://doi.org/10.15688/NBIT.jvolsu.2019.4.1

УДК 004.056
ББК 32.971.35

РАЗРАБОТКА МОДЕЛИ ОБНАРУЖЕНИЯ НЕСАНКЦИОНИРОВАННОГО ТРАФИКА

Алексей Александрович Бабенко

Кандидат педагогических наук, доцент кафедры информационной безопасности,
Волгоградский государственный университет
ba_benko@mail.ru, volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Юлия Михайловна Гущина

Студент кафедры информационной безопасности,
Волгоградский государственный университет
yulia.mig@mail.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Рассмотрена проблема обеспечения информационной безопасности в компьютерной сети предприятия. Проведен анализ несанкционированного трафика с целью выявления его признаков. Проанализированы методы обнаружения несанкционированного трафика для выбора наилучшего. Разработана формализованная модель обнаружения несанкционированного трафика.

Ключевые слова: информационная безопасность, компьютерная сеть, атака, несанкционированный трафик, методы обнаружения несанкционированно трафика.

Введение

Информационные системы и технологии являются основными средствами повышения производительности и эффективности работы людей. И на сегодняшний день наряду с задачами эффективной обработки и передачи информации стоит важнейшая задача обеспе-

чения информационной безопасности (ИБ) предприятий.

В [6] согласно глобальному исследованию компании InfoWatch, количество утечек информации с каждым годом растет. Наибольшее количество утечек данных было зафиксировано в компаниях высокотехнологичного сектора, образовательных учреждениях, государственных органах и банках. Чаще всего угрозу представляет собой сетевой трафик [5]. Эта угроза заключается в перехвате данных по сети, целью которого является получение конфиденциальных данных, паролей, корпоративных тайн, адресов компьютерных машин сети и т. д. Возникает необходимость в создании аппаратных и программных средств защиты сетевых ресурсов. Следовательно, создание средства обнаружения несанкционированного трафика является актуальным.

Анализ несанкционированного трафика с целью выявления признаков для его обнаружения

Компьютерная сеть – это цифровая телекоммуникационная сеть, которая позволяет узлам совместно использовать ресурсы. В компьютерных сетях вычислительные устройства обмениваются данными друг с другом, используя соединения (каналы передачи данных) между узлами. Сети включают в себя аппаратное и программное обеспечение. К аппаратным компонентам относятся серверы, клиенты, среда передачи и подключаемые устройства. К программным компонентам – операционные системы и протоколы.

Сеть характеризуется пропускной способностью – это объем трафика, который сеть может поддерживать в любое время. Сетевые данные в основном инкапсулированы в сетевые пакеты, которые обеспечивают нагрузку в сети. Пропускная способность определяется количественно по теоретически максимальному количеству бит в секунду, которое может проходить через сетевое устройство.

Выделяют следующие виды сетевого трафика:

1) входящий, поступающий в сеть, сервер, компьютер;

2) исходящий, идущий от сети, сервера, компьютера в противоположном направлении;

3) внутренний, передающийся внутри какой-то определенной сети – локальной, либо отдельного сегмента глобальной, ограниченной по какому-то признаку (например, провайдером);

4) внешний – циркулирующий за пределами условной сети – локальной, либо определенного сегмента глобальной, ограниченной по определенному признаку.

Также сетевой трафик можно разделить на:

1) санкционированный (осуществляется с разной целью, начиная от защиты корпоративной информации до обеспечения безопасности государства; определяется законодательством, специальными службами, сотрудниками правоохранительных органов, специалистами административных организаций, службами безопасности компаний);

2) несанкционированный (осуществляется злоумышленниками, желающими завладеть конфиденциальными данными, паролями, корпоративными тайнами, адресами компьютеров в сети и т. д.) [4].

Основной особенностью для удаленных атак на инфраструктуру и сетевые протоколы является то, что компоненты любой сетевой информационной системы распределены в пространстве, и связь между ними осуществляется физически, с использованием сетевых соединений, и программно (с использованием механизма сообщений).

Атака представляет собой угрозу ИБ, которая включает в себя попытку получить, изменить, уничтожить, удалить, внедрить или раскрыть информацию без санкционированного доступа или разрешения [7]. Ниже приведены примеры некоторых наиболее распространенных атак:

1) SQL-инъекция – это уязвимость веббезопасности, которая позволяет злоумышленнику вмешиваться в запросы, которые приложение выполняет в своей базе данных. Злоумышленник может просматривать данные, которые он обычно не может получить. Это могут быть данные, принадлежащие другим пользователям, или любые другие данные, к которым само приложение имеет доступ. Атакующий имеет возможность изменить или удалить эти данные, что приведет к постоянным изменениям поведения приложения и его содержимого.

2) Отказ в обслуживании (DoS, DDoS-атаки). Так можно назвать любую атаку, при которой злоумышленники пытаются предотвратить доступ к службам законным пользователям. При DoS-атаке злоумышленник обычно отправляет избыточные сообщения с просьбой подтвердить серверу подлинность запросов, имеющих недопустимые обратные адреса. Атаки данного типа обычно не приводят к краже или потере важной информации или других активов, они могут привести к нарушению доступности информационных ресурсов.

3) ICMP-flood (ICPM-smurfing) - тип атаки «отказ в обслуживании», принцип работы такой DDoS-атаки заключается в том, что злоумышленник, изменяя адрес источника, пытается перегрузить компьютер с помощью ICMP пакета (больше известный как ping) к конкретным хостам. Обычно сообщения – эхо-запросы (Echo Request) и эхо-ответы (Echo Reply) используются для проверки связи с сетевыми устройствами для проверки работоспособности и соединения между отправителем и получателем. Перегружая цель атаки запросами, сеть вынуждена отвечать равным количеством ответных пакетов, что приводит к недоступности цели для обычного трафика.

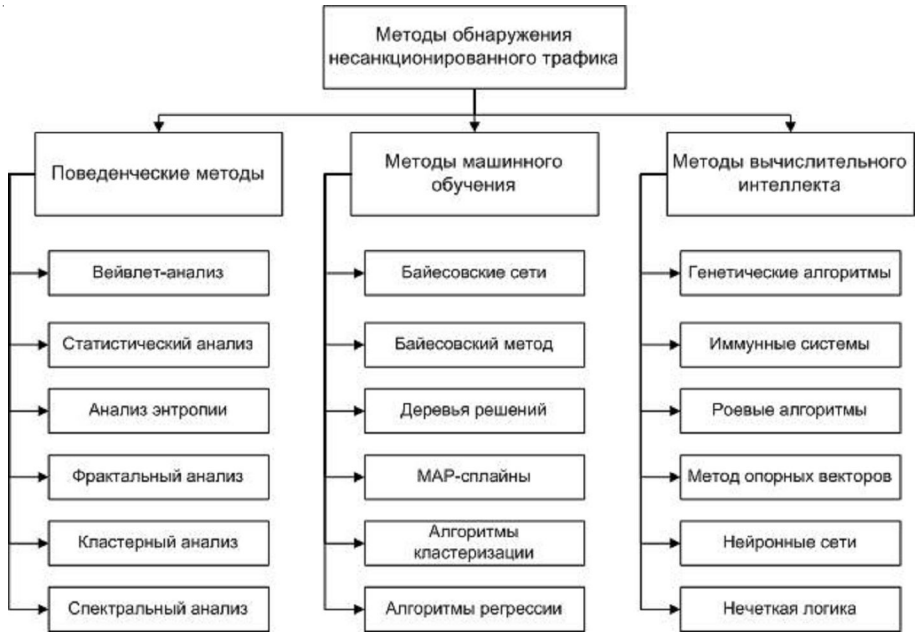
Таким образом, можно сделать вывод о том, что важными признаками несанкционированного трафика являются непосредственно входящие извне в сеть и выходящие из сети информационные пакеты данных и несоответствующие параметры сетевого трафика, то есть нарушение стандартных технических характеристик сетевого трафика.

Анализ методов обнаружения несанкционированного трафика

Методов обнаружения несанкционированного трафика существует огромное количество, а также их модификаций и разновидностей. Предлагается использовать следующую схему классификации методов обнаружения несанкционированного трафика, представленную на рисунке.

Поведенческие методы – это методы, основанные на моделях нормального функционирования системы. На основе поведения системы или пользователя данные методы позволяют построить нормальную модель их функционирования для дальнейшего сравнения показателей активности с построенной моделью, и в случае значительных отклонений обнаруживать наличие атаки, возможно еще неизвестной [2].

Методы машинного обучения, которые позволяют создавать и поддерживать систему обнаружения вторжений с минимальным вмешательством человека, являются хоро-



Классификация методов обнаружения несанкционированного трафика

шим практическим подходом для защиты информационных систем. Программа, созданная на основе машинного обучения для обнаружения несанкционированного трафика, может автоматически построить модель на основе набора обучающих данных, содержащую экземпляры данных, которые могут быть описаны с использованием набора различных типов атрибутов и связанных меток.

Методы вычислительного интеллекта имеют схожесть с методами машинного обучения, основаны на генетических алгоритмах и нейронных сетях. Суть данных методов заключается в способности к обучению по образцу, в процессе которого происходит корректировка коэффициентов, связанных с синаптическими весами [3].

Для того чтобы понять, какой метод будет более эффективным для разработки программного средства в данной работе, был проведен анализ, в результате которого было установлено, что наиболее рациональными являются поведенческие методы, а именно - фрактальный анализ. Он обладает средней сложностью реализации, высокой адаптивностью к неизвестным атакам и более точно описывает поведение нагруженного сетевого потока.

Формализованная модель обнаружения несанкционированного трафика

Фрактальный анализ основан на предположении, что сетевой трафик удовлетворяет свойству самоподобия, ключевым понятием в котором являются параметр Херста H [1], который определяется по формуле 1:

$$H = \log_{\frac{N}{2}} \frac{R}{S}, \qquad (1)$$

где N – длина временного ряда $X = \{x_1, \ldots x_n\}$ со средним значением:

$$\bar{x} = \frac{1}{N} \times \sum_{i=1}^{N} x_i, \qquad (2)$$

размах отклонения (изменчивость) ряда R:

$$R = \max_{1 \le i \le N} x_i - \min_{1 \le j \le N} x_j, \qquad (3)$$

и выборочное среднеквадратическое отклонение:

$$S = \sqrt{\frac{1}{N-1} \times \sum_{i=1}^{N} (x_i - \bar{x})^2}. \qquad (4)$$

Текущее вычисленное значение показателя Херста сравнивается со значением:

$$Z = \begin{cases} 0.5 < H < 1, \\ \text{удовлетворяет свойству самоподобия;} \\ H < 0.5 \text{ или } H > 1, \\ \text{трафик несанкционированный.} \end{cases} \qquad (5)$$

Заключение

В настоящее время вопросы построения систем обнаружения несанкционированного трафика представляют собой актуальное направление в области информационных технологий. Существует множество методов обнаружения несанкционированного трафика. Один из них, поведенческий метод, а именно фрактальный анализ, был рассмотрен в данной статье.

СПИСОК ЛИТЕРАТУРЫ

1. Анализ современных методов обнаружения вторжений в компьютерные системы / Т. Н. Шипова [и др.] // Системи обробки інформації. – 2016. – Вып. 1 (138). – С. 133–137.

2. Бабенко, А. А. Разработка системы управления аномальными событиями информационной безопасности / А. А. Бабенко, С. Ю. Микова, В. С. Оладько // Информационные системы и технологии. – 2017. – № 5 (103). – С. 108–116.

3. Браницкий, А. А. Анализ и классификация методов обнаружения сетевых атак / А. А. Браницкий, И. В. Котенко // Труды СПИИРАН. – 2016. – Вып. 45. – С. 207–244.

4. Гальцев, А. А. Системный анализ трафика для выявления аномальных состояний сети / А. А. Гальцев // Электронная библиотека диссертаций. – Электрон. текстовые дан. – Режим доступа: http://www.dissercat.com/content/sistemnyi-analiz-trafika-dlya-vyyavleniya-anomalnykh-sostoyanii-seti. – Загл. с экрана.

5. Глобальное исследование утечек конфиденциальной информации в I полугодии 2018 года. – Электрон. текстовые дан. – Режим доступа: https://www.infowatch.ru/report2018_half (дата обращения 29.10.2019). – Загл. с экрана.

6. Глобальное исследование утечек конфиденциальной информации в 2018 году. – Электрон.

текстовые дан. – Режим доступа: https://www.infowatch.ru/report2018 (дата обращения: 29.10.2019). – Загл. с экрана.

7. Моделирование сетевых атак злоумышленников в корпоративной информационной системе / В. А. Гнеушев [и др.] // Промышленные АСУ и контроллеры. – 2017. – № 6. – С. 51–60.

REFERENCES

1. Shipova T.N., Bosko V.V., Berezyuk I.A., Parhomenko Yu.M. Analiz sovremennykh metodov obnaruzheniya vtorzheniy v kompyuternye sistemy [Analysis of Modern Methods of Detecting Intrusions into Computer Systems]. *Systemy obrobky informatsyiy*, 2016, iss. 1 (138), pp. 133-137.

2. Babenko A.A., Mikova S.Yu., Oladko V.S. Razrabotka sistemy upravleniya anomalnymi sobytiyami informatsionnoy bezopasnosti [Development of Information Security's Abnormal Events Control System. Information Systems and Technologies]. *Informatsionnye sistemy i tekhnologii* [Scientific and Technical Journal], 2017, no. 5, pp. 108-116.

3. Branickij A.A., Kotenko I.V. Analiz i klassifikatsiya metodov obnaruzheniya setevykh atak [Analysis and Classification of Network Attack Detection Methods]. *Trudy SPIIRAN*, 2016, no. 45, pp. 207-244.

4. Galcev A.A. Sistemnyy analiz trafika dlya vyyavleniya anomalnykh sostoyaniy seti [System Traffic Analysis to Identify Abnormal Network Conditions]. *Elektronnaya biblioteka dissertatsiy* [Electronic Library of Dissertations]. URL: http://www.dissercat.com/content/sistemnyi-analiz-trafika-dlya-vyyavleniya-anomalnykh-sostoyanii-seti.

5. *Globalnoe issledovanie utechek konfidentsialnoy informatsii v I polugodii 2018 goda* [Global Study of Confidential Information Leaks in the First Half of 2018]. URL: https://www.infowatch.ru/report2018_half (accessed 29 October 2019).

6. *Globalnoe issledovanie utechek konfidentsialnoy informatsii v 2018 godu* [Global Study of Confidential Information Leaks in 2018]. URL: https://www.infowatch.ru/report2018 (accessed 29 October 2019).

7. Gneushev V.A., Kravets A.G., Kozunova S.S., Babenko A.A. Modelirovanie setevykh atak zloumyshlennikov v korporativnoy informatsionnoy sisteme [Modeling Network Attack of Attacker in the Corporate Information System]. *Promyshlennye ASU i kontrollery*, 2017, no. 6, pp. 51-60.

DEVELOPMENT OF A MODEL FOR DETECTING UNAUTHORIZED TRAFFIC

Alexey A. Babenko

Candidate of Sciences (Pedagogy), Associate Professor, Information Security Department,
Volgograd State University
ba_benko@mail.ru, volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Yuliya M. Gushchina

Student, Department of Information Security,
Volgograd State University
yulia.mig@mail.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. Information systems and technologies are the main means of increasing people's productivity and efficiency. And today, along with the tasks of effective processing and transmission of information, the most important task is to ensure the information security of enterprises. According to the global study by InfoWatch, the number of information leaks is growing every year. The largest number of data leaks were recorded in high-tech companies, educational institutions, government agencies and banks. Most often, network traffic is a threat. This threat consists in the interception of data over the network, the purpose of which is to obtain confidential data, passwords, corporate secrets, addresses of network

computers, etc. There is a need to create hardware and software tools to protect network resources. Therefore, creating a tool for detecting unauthorized traffic is relevant. The authors consider the problem of information security in the enterprise computer network and carry out the analysis of unauthorized traffic in order to identify its signs. The researchers analyze methods for detecting unauthorized traffic to select the best one and present a developed formalized model for detecting unauthorized traffic.

Key words: information security, computer network, attack, unauthorized traffic, methods for detecting unauthorized traffic.