А. Н. Бабкин, *кандидат технических наук, доцент*
Л. В. Акчурина, *кандидат технических наук*
С. П. Алексеенко, *кандидат физико-математических наук, доцент*

МОДЕЛИРОВАНИЕ УГРОЗ ИНФОРМАЦИОННЫХ АТАК В СЕТИ INTERNET НА ОСНОВЕ СЕТЕЙ ПЕТРИ

MODELING INFORMATION ATTACK THREATS ON THE INTERNET BASED ON PETRI NETWORKS

В статье рассматривается возможность моделирования угроз информационных атак в сети Internet на основе сетей Петри. Моделирование основано на формировании маркировки информационно-телекоммуникационной сети последовательно при срабатывании переходов информационного пакета между хостом пользователя, хостом нарушителя и сервером.

The article discusses the possibility of modeling threats of information attacks on the Internet based on Petri networks. Simulation is based on generation of marking of information and telecommunication network sequentially at actuation of transitions of information packet between user host, intruder host and server.

Введение. Одними из основных угроз безопасности информации на сетевом уровне являются угрозы информационных атак, направленных на перехват пользовательского трафика.

Существуют различные способы перехвата трафика [1], к основным из которых относят способы, основанные на создании «ложных узлов», внедрении «снифферов», подмене доверенного объекта и др.

Целью информационных атак является выявление нарушителями характеристик информационно-телекоммуникационных сетей (ИТКС), связанных с анализом сетевых адресов, открытых портов, номеров пакетов и др., и, как следствие, перехват пакетов, передаваемых пользователем по сети.

Для противодействия информационным атакам необходимо предусмотреть в ИТКС механизмы предупреждения и выявления сетевых атак.

Одним из таких механизмов является создание системы обнаружения информационной атаки на основе применения сетей Петри, моделирующих обнаружение вторжений.

Основная часть. Для реализации информационных атак нарушитель использует различные уязвимости протоколов межсетевого взаимодействия [1, 2], например, уязвимость протокола DNS связана с отсутствием аутентификации DNS-ответов.

Уязвимость протокола разрешения адресов ARP связана с возможностью модификации нарушителем ARP-таблицы атакуемого хоста (или маршрутизатора) при отсутствии авторизации при обновлении ARP-таблицы.

Перехват пользовательского трафика при использовании протокола HTTP основан на создании ложного узла сети, при этом используется уязвимость, связанная с отсутствием аутентификации при получении ответа от web-сервера.

Нарушитель для перехвата пользовательского трафика может также использовать уязвимости протоколов RIP и OSPF, BGP и EGP [1, 2].

Уязвимости данных протоколов связаны с возможностями обновления таблиц маршрутизации, приводящих к перенаправлению трафика на хост нарушителя.

В [3] был подробно рассмотрен пример реализации сетевой атаки при работе специальной сетевой службы DNS (рис.1), представлена блок-схема функционирования

информационной системы и представлена сеть Петри, моделирующая процесс обнаружения информационной атаки (рис. 2).

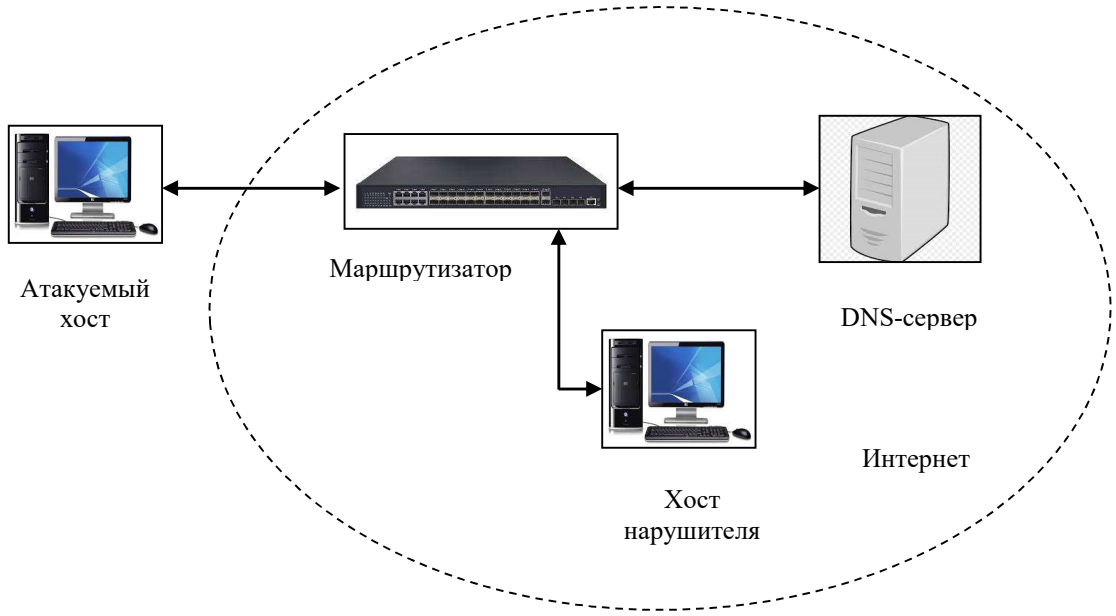

Рис. 1. Обобщенная структурная схема ИТКС,
в которой реализуется информационная атака при работе специальной сетевой службы DNS

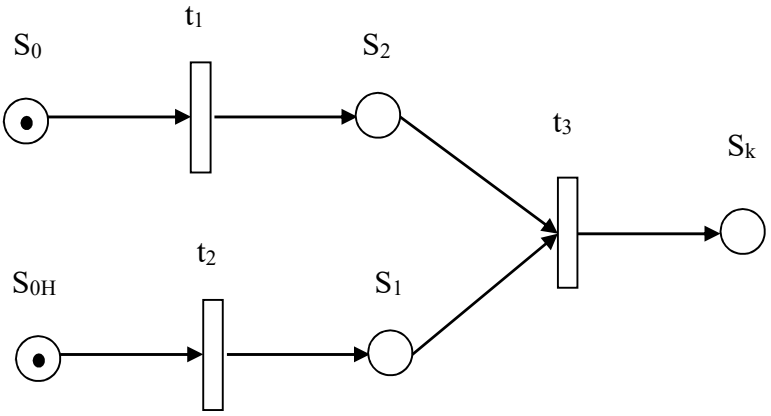

Рис. 2. Сеть Петри, моделирующая процесс обнаружения
информационной атаки

На рис. 2 представлены:

S_0 — начальное состояние атакуемого хоста;

t_1 — переход, связанный с реализацией взаимодействия атакуемого хоста и сервера;

S_{0H} — начальное состояние хоста нарушителя;

t_2 — переход, связанный с перехватом запроса атакуемого хоста нарушителем;

S_1 — состояние хоста нарушителя, связанное с формированием ложного ответа;

S_2 — состояние атакуемого хоста, связанное с ожиданием получения ответа;

t_3 — переход, связанный с получением ложного ответа;

S_k — состояние ИТКС, связанное с направлением трафика на хост нарушителя.

Рассмотрим более подробно реализацию сети Петри, представленную на рис. 2, с формированием маркировки сети ИТКС последовательно при срабатывании переходов информационного пакета между хостом пользователя, хостом нарушителя и сервером.

Для этого представим сеть Петри в следующем виде (рис. 3):

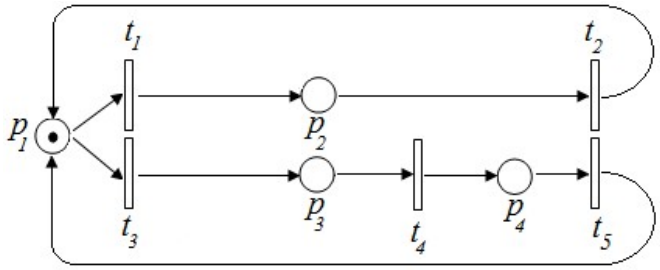

Рис. 3. Сеть Петри, моделирующая информационную атаку на хост пользователя

На рис. 3 позиции и переходы имеют следующую смысловую нагрузку:

P_1 — начальное состояние атакуемого хоста (запрос сформулирован при появлении маркера);

t_1 — переход, связанный с реализацией взаимодействия атакуемого хоста и сервера, роль данного перехода может выполнять маршрутизатор;

P_2 — состояние, связанное с формированием ответа на запрос пользователя на DNS-сервере;

t_2 — переход, связанный с реализацией передачи информации с сервера пользователю;

t_3 — переход, связанный с реализацией взаимодействия атакуемого хоста и злоумышленника, роль данного перехода может выполнять маршрутизатор, на котором информация была перехвачена злоумышленником;

P_3 — состояние хоста нарушителя, связанное с формированием запроса злоумышленника на ложный DNS-сервер;

t_4 — переход, связанный с реализацией передачи информации от злоумышленника на ложный DNS-сервер;

P_4 — состояние, связанное с формированием ответа на ложный запрос пользователя на ложном DNS-сервере;

t_5 — переход, связанный с реализацией передачи информации от ложного DNS-сервера на атакуемый хост.

Следует отметить, что сети Петри, моделирующие процесс обнаружения информационной атаки в сети ИТКС и представленные соответственно на рис. 2 и рис. 3 , отличаются друг от друга.

Сеть Петри, представленная на рис. 2, построена на основе анализа переходов ИТКС из одного состояния в другое.

Информационная атака рассматривается как вторжение в информационный процесс, приводящее к изменению состояния ИТКС.

Таких изменений может быть несколько, и они детерминированы.

Сеть Петри, представленная на рис. 3, построена на основе формирования маркера состояния сети ИТКС, связанного с возможными переходами ИТКС из одного состояния в другое.

Рассмотрим более подробно процесс моделирования информационной атаки на основании сети Петри, представленной на рис. 3.

Маркировку сети можно рассматривать как многомерный вектор, число координат которого равно количеству состояний в сети.

В нашем случае $\mu = (P_1, P_2, P_3, P_4)$, что включает четыре состояния.

Наличие маркера в позиции отмечается единичкой, тогда начальная маркировка сети, указанной на рисунке 3 имеет вид

$$\mu_0=\{1, 0, 0, 0\},$$

где μ_0 — начальное состояние ИТКС (фаза формирования запроса атакуемого хоста генерируется запросом пользователя, и, как только он сформирован, включается маркер в позиции P_1).

Возможны 2 способа развития ситуации:

1. Запрос хостом сформирован, он сразу через маршрутизатор t_1 направляется на DNS-сервер (P_2).

Запрос пошел по назначению.

В этом случае такая маркировка сети ИТКС:

$$\mu_1=\{0, 1, 0, 0\}.$$

DNS-сервер отвечает на запрос и маркировка сети следующая:

$$\mu_2=\{1, 0, 0, 0\}.$$

2. Сформированный запрос перехватывается хостом нарушителя (P_3), запрос ушел не по назначению, тогда маркировка сети имеет вид

$$\mu_1=\{0, 0, 1, 0\}.$$

Формируется запрос на ложный DNS-сервер (P_4):

$$\mu_2=\{0, 0, 0, 1\}.$$

С ложного DNS-сервера запрос возвращается на хост пользователя:

$$\mu_3=\{1, 0, 0, 0\}.$$

Далее ситуация с новым запросом повторяется.

Диаграмма дерева маркировки сети Петри, представленной на рис. 3, указана на рис. 4.

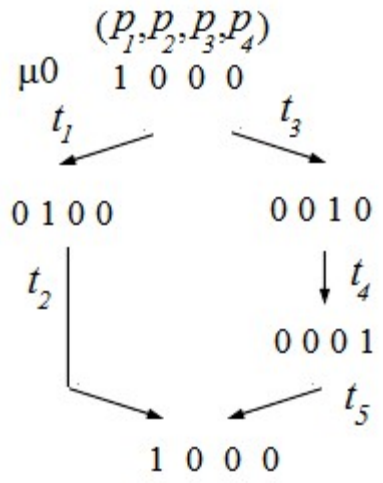

Рис. 4. Диаграмма сети Петри, моделирующая информационную атаку на хост пользователя

Как отмечалось выше, отличительной особенностью представленного алгоритма моделирования угроз информационных атак в сети Internet (сети ИТКС) на основе сетей Петри является формирование маркера состояния сети, связанного с возможными переходами ИТКС из одного состояния в другое.

Под маркером в данном случае понимается признак состояния сети.

Он представляет собой число, значение которого может меняться в зависимости от стадии перехода (t_i) ИТКС из одного состояния в другое.

Анализ маркера после каждого перехода позволит определить начало информационной атаки со стороны хоста нарушителя и своевременно принять меры по противодействию.

Вывод. В статье рассматривается механизм формирования сети Петри при возникновении информационной атаки, связанной с перехватом трафика пользователя в сети Internet путем перехвата DNS-запроса от атакуемого хоста и формирования ложного DNS-сервера.

В статье приведены две разные сети Петри, каждая из которых имеет определенный прикладной смысл.

Сеть на рис. 2 отслеживает количество успешных для злоумышленника атак.

Сеть на рис. 3 описывает передвижение пакета информации по сетям интернета.

Если для последней сети ввести счетчик выполненных запросов, усложнив ее, то появляется возможность отслеживания эффективности защитных характеристик в сети ИТКС.

Представленный алгоритм моделирования угроз информационных атак в сети Internet на основе сетей Петри может быть применен к различным способам перехвата трафика [1, 2].

Отличительной особенностью данного моделирования является формирование маркера состояния информационного процесса, представляющего собой числовое значение и позволяющего своевременно противодействовать возникающим угрозам.

ЛИТЕРАТУРА

1. Язов Ю. К., Соловьев С. В. Организация защиты информации в информационных системах от несанкционированного доступа : монография. — Воронеж : Кварта, 2018. — 588 с.

2. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов. — 5-е изд. — СПб. : Питер, 2016. — 992 с.

3. Бабкин А. Н., Акчурина Л. В., Алексеенко С. П. Пример применения сетей Петри для анализа защищенности информационных процессов // Вестник Воронежского института МВД России. — 2022. — № 4. — С. 65—71.

4. Котов В. Е. Сети Петри. — М. : Наука, 1984.

5. Кудж С. А., Логинова А. С. Моделирование с использованием сетей Петри // Вестник МГТУ МИРЭА. — 2015. — № 1.

REFERENCES

1. YAzov YU. K., Solov'ev S. V. Organizaciya zashchity informacii v informacionnyh sistemah ot nesankcionirovannogo dostupa : monografiya. — Voronezh : Kvarta, 2018. — 588 s.

2. Olifer V., Olifer N. Komp'yuternye seti. Principy, tekhnologii, protokoly : uchebnik dlya vuzov. — 5-e izd. — SPb. : Piter, 2016. — 992 s.

3. Babkin A. N., Akchurina L. V., Alekseenko S. P. Primer primeneniya setej Petri dlya analiza zashchishchennosti informacionnyh processov // Vestnik Voronezhskogo instituta MVD Rossii. — 2022. — № 4. — S. 65—71.

4. Kotov V. E. Seti Petri. — M. : Nauka, 1984.

5. Kudzh S. A., Loginova A. S. Modelirovanie s ispol'zovaniem setej Petri // Vestnik MGTU MIREA. — 2015. — № 1.