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

ПРИМЕР ПРИМЕНЕНИЯ СЕТЕЙ ПЕТРИ ДЛЯ АНАЛИЗА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ

EXAMPLE OF PETRI NETWORK APPLICATION FOR INFORMATION PROCESS SECURITY ANALYSIS

В статье приводится пример применения сетей Петри для анализа защищенности информационных процессов в телекоммуникационных сетях в условиях воздействия угроз информационной безопасности. Подробно рассматривается применение сетей Петри на примере работы специальной сетевой службы DNS.

The article provides an example of the use of Petri networks to analyze the security of information processes in telecommunications networks in the face of information security threats. The use of Petri networks is discussed in detail on the example of the work of a special DNS network service.

Введение. Информационные технологии активно внедряются как в повседневную жизнь рядовых пользователей, так и в деятельность предприятий и организаций. Использование почтовой и справочной служб, файлового сервиса, веб-службы, IP-телефонии, службы облачных вычислений стало неотъемлемой частью деятельности как физических, так и юридических лиц.

Огромное количество компьютеров, связанных через интернет, используют (и хранят) информацию, представленную в виде веб-страниц.

Защита информации, хранящейся как на персональном компьютере пользователя, так и сервере, обеспечение надежного соединения между браузером и веб-сервером, своевременное предотвращение информационных атак со стороны злоумышленников являются актуальными задачами.

Для моделирования информационных процессов в системах в условиях воздействия угроз информационной безопасности можно применять цепи Маркова [1].

Хорошим инструментом для анализа изменений состояний информационных систем, в том числе и связанных с нарушением безопасности информации, являются сети Петри [2, 3].

При этом при использовании сетей Петри любое воздействие злоумышленника на информационный процесс, протекающий в системе, должно приводить к видимым изменениям его состояния, что позволит обнаружить информационную атаку и принять необходимые меры по защите информации в системе.

Основная часть. Рассмотрим применение сетей Петри на примере работы специальной сетевой службы DNS.

Служба предназначена для формирования IP-адресов пользовательским компьютерам (хостам).

Данный протокол работает по принципу «клиент—сервер».

Персональный компьютер (ПК) пользователя посылает запрос DNS-серверу на получение IP-адреса.

DNS-сервер формирует ответ, который содержит IP-адрес и другие данные.

На рисунке 1 представлена обобщенная структурная схема взаимодействия пользователя и DNS-сервера [4].

На данном рисунке ИТКС — информационно-телекоммуникационная сеть общего пользования, предоставляющая каналы связи для передачи информации между компьютером пользователя и DNS-сервером.

Взаимодействие осуществляется по принципу «запрос—ответ» по протоколу DNS.

Запросы и ответы представляют собой сообщения, имеющие общую структуру.

Данная информация представляет интерес для злоумышленника. Располагая ею, злоумышленник может сформировать информационную атаку и нанести ущерб как пользователю (хосту), так и компьютеру, на котором располагается DNS-сервер.

Одной из возможных атак является перенаправление трафика атакуемого хоста на узел нарушителя [5].

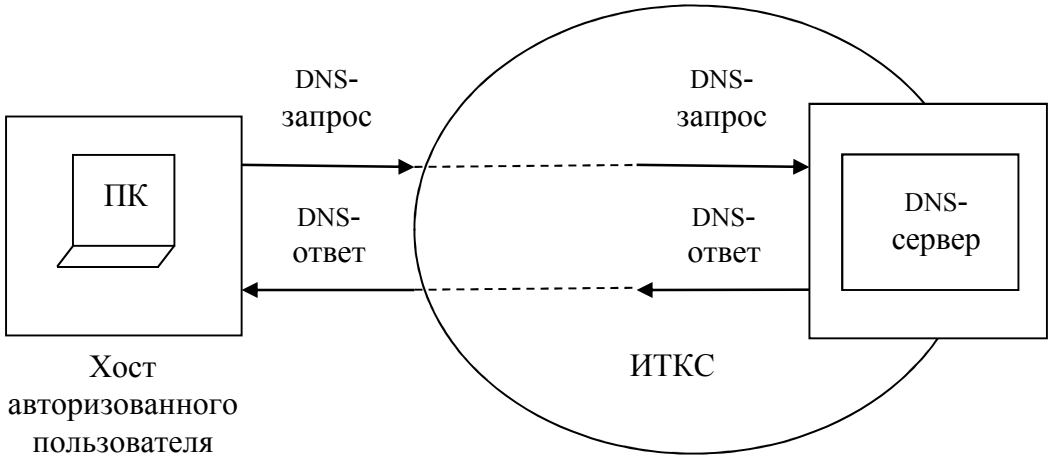

Рис. 1. Обобщенная структурная схема взаимодействия пользователя и DNS -сервера

На рисунке 2 представлена схема реализации подобной информационной атаки.

Суть её заключается в следующем.

Хост авторизованного пользователя посылает на DNS-сервер запрос на получение IP-адреса. Запрос перехватывается злоумышленником (хостом нарушителя) и транслируется на DNS-сервер.

Хост нарушителя формирует ответ с указанием IP-адреса ложного узла, который с IP-адресом настоящего DNS-сервера передается на хост авторизованного пользователя.

Получив ответ, хост авторизованного пользователя будет передавать информацию по ложному IP-адресу (на хост нарушителя).

На рисунке 2 все сигналы, формируемые хостом-нарушителем, обозначены штрихпунктирной линией.

В данном примере представлена угроза информационной безопасности на сетевом уровне.

Угроза направлена на перехват трафика и реализуется за счет внедрения в сеть ложного DNS-сервера, используя уязвимости DNS и IP-протоколов.

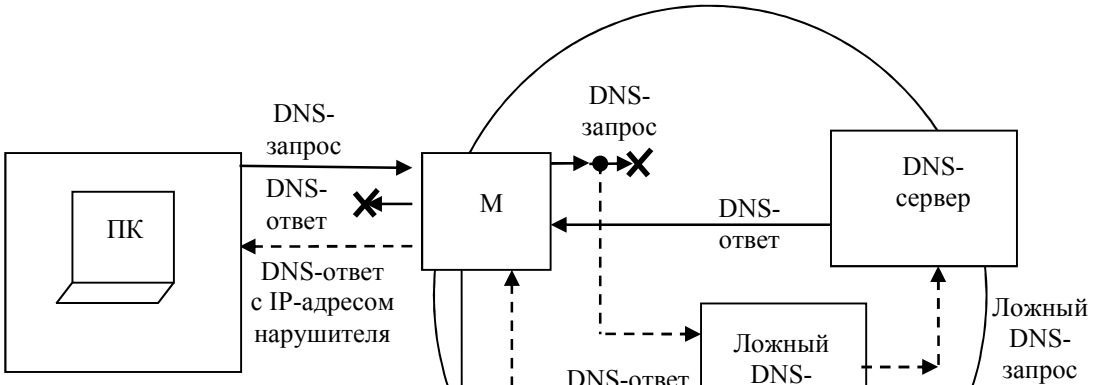

Рис. 2. Схема реализации информационной атаки

Для обнаружения информационных атак применяются различные методы [5].

Одним из таких методов является метод анализа переходов системы из одного состояния в другое. Данный метод основан на применении сетей Петри для моделирования процесса обнаружения сетевой атаки.

Информационная атака рассматривается как вторжение в информационный процесс, приводящее к изменению состояния системы. Таких изменений может быть несколько, и они детерминированы.

Переходы из состояния в состояние связаны с возникновением событий в системе, влияющих на информационный процесс.

Таким образом, сеть Петри представляет собой ориентированный граф, состоящий из состояний и переходов, соединенных между собой дугами.

Анализируемую информационную систему на основе моделирования сетями Петри можно представить как множество состояний С:

$$C = \{S, T, F_{вх}, F_{вых}\},$$

где $S = \{S_i\}$ — множество состояний системы; $T = \{T_j\}$ — множество переходов системы; $F_{вх}$ — входная функция, соответствующая начальному состоянию системы; $F_{вых}$ — выходная функция, соответствующая конечному состоянию системы.

На рисунке 3 представлен пример сети Петри в системе, где отсутствует нарушитель (соответствует информационному процессу, представленному на рис. 1).

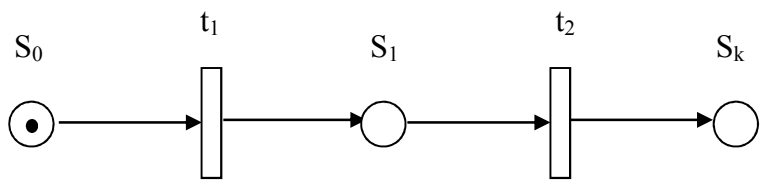

Рис. 3. Пример сети Петри, моделирующей информационный процесс в системе без наличия нарушителя

На рисунке 3: S_0 — начальное состояние системы (состояние ПК пользователя); t_1 — переход, связанный с формированием запроса к серверу пользовательским компьютером (процедуры запроса); S_1 — состояние системы, связанное с ожиданием ответа от сервера; t_2 — переход, связанный с получением ПК ответа от сервера (процедура ответа); S_k — конечное состояние системы (запуск TCP-соединения).

На рисунке 4 представлен пример сети Петри, моделирующей процедуру обнаружения информационной атаки со стороны нарушителя.

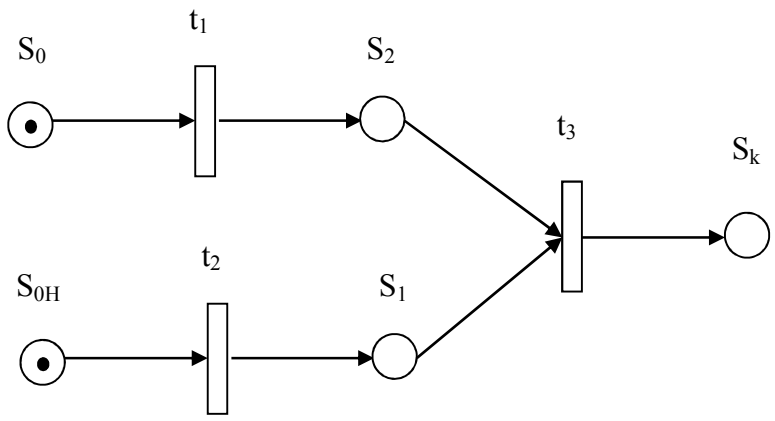

Рис. 4. Сеть Петри, моделирующая процесс обнаружения информационной атаки

На рисунке 4 обозначены: S_0 — начальное состояние системы (состояние ПК пользователя); t_1 — переход, связанный с реализацией взаимодействия пользовательского компьютера и сервера (процедуры формирования запроса); S_{0H} — начальное состояние хоста нарушителя; t_1 — переход, связанный с перехватом запроса от ПК пользователя); S_1 — состояние хоста нарушителя, связанное с формированием ложного ответа); S_2 — состояние ПК пользователя, связанное с ожиданием получения ответа; t_3 — переход, связанный с получением ложного ответа; S_k — состояние системы, связанное с направлением трафика на хост нарушителя.

Удобство использования сетей Петри заключается в том, что имеется возможность преобразования блок-схемы функционирования системы в сеть Петри.

Так, сеть Петри, представленная на рисунке 3, является результатом преобразования блок-схемы, представленной на рисунке 5.

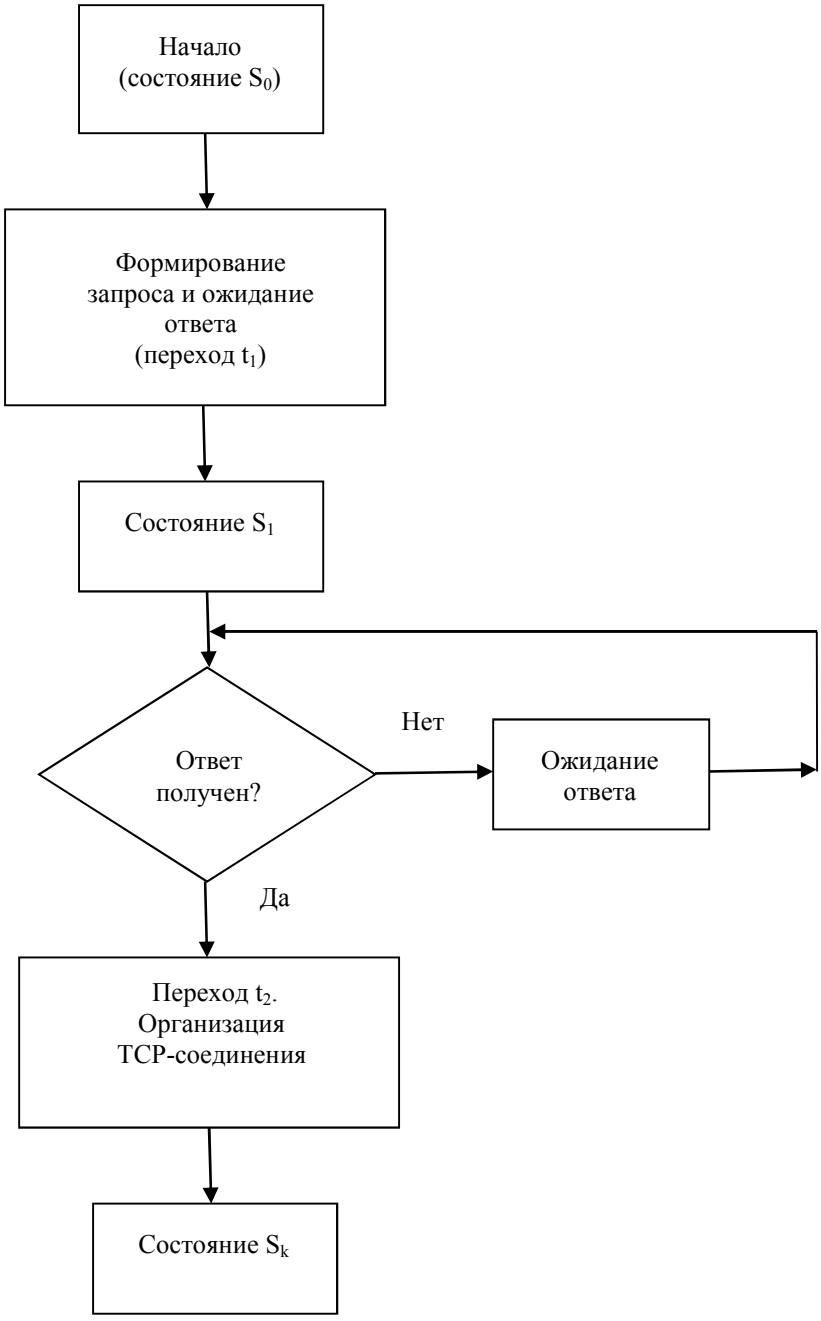

Рис. 5. Блок-схема функционирования информационной системы

Как отмечалось выше, переходы из состояния в состояние связаны с возникновением событий в системе, влияющих на организацию информационных процессов (например, запуск приложений, организацию TCP-соединения) и, как следствие, возникновение возможных информационных атак со стороны нарушителя (злоумышленника).

Ключевым фактором применения сетей Петри является видимое изменение в системе с точки зрения нарушения информационной безопасности (новое состояние системы).

Таким фактором, исходя из блок-схемы, представленной на рисунке 5, может быть время ожидания ответа ПК со стороны DNS-сервера.

Заключение. Для надежного функционирования информационной системы необходимо обеспечение её информационной безопасности.

На этапе построения ИС, а также в условиях эксплуатации хорошим инструментом моделирования возможных информационных атак является применение метода анализа переходов ИС из одного состояния в другое.

В основе данного метода лежат сети Петри.

Как отмечалось выше, удобство использования сетей Петри заключается в том, что имеется возможность преобразования блок-схемы функционирования системы в сеть Петри, и моделирования возможных информационных атак на её основе.

Использование сетей Петри позволяет обнаружить широкий спектр информационных атак в ИС в реальных условиях эксплуатации.

ЛИТЕРАТУРА

1. Бабкин А. Н., Акчурина Л. В. Моделирование процессов передачи данных в телекоммуникационной сети в условиях воздействия угроз информационной безопасности // Вестник ВИ ФСИН России. — 2021. — № 3. — С.50—57.

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

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

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

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

REFERENCES

1. Babkin A. N., Akchurina L. V. Modelirovanie processov peredachi dannyh v telekommunikacionnoj seti v usloviyah vozdejstviya ugroz informacionnoj bezopasnosti // Vestnik VI FSIN Rossii. — 2021. — № 3. — S.50—57.

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

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

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

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