Дровникова Ирина Григорьевна,
доктор технических наук, доцент;
Овчинникова Елена Сергеевна

ДИНАМИЧЕСКИЕ МОДЕЛИ РЕАЛИЗАЦИИ СЕТЕВЫХ АТАК В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

DYNAMIC MODELS OF NETWORK ATTACKS IMPLEMENTATION IN AUTOMATED SYSTEMS OF INTERNAL AFFAIRS BODIES

В статье представлены формальные модели динамики реализации типовых сетевых атак на информационный ресурс современных автоматизированных систем органов внутренних дел, построенные с использованием математического аппарата сетей Петри-Маркова.

The article presents formal models of the dynamics of implementation of typical network attacks on the information resource of modern automated systems of internal Affairs bodies, built using the mathematical apparatus of Petri-Markov networks.

Процесс реализации сетевых атак на информационный ресурс современных автоматизированных систем (АС), эксплуатируемых в защищенном исполнении на объектах информатизации органов внутренних дел (ОВД), является сложным и динамичным, состоящим из множества взаимосвязанных параллельных процессов. Необходимость анализа динамики реализации указанных процессов с определением их временных и статистических характеристик [1] делает целесообразным использование математических моделей, построенных на сетях Петри-Маркова, для исследования процесса реализации сетевых атак на защищенные АС ОВД. В основе таких моделей лежат теории сетей Петри и марковские (полумарковские) процессы [2, 3]. Модели, построенные с использованием аппарата сетей Петри-Маркова, относятся к числу наиболее важных и распространенных математических моделей, традиционно находя свое применение для решения задач синтеза и оптимизации, в том числе при исследовании протекания параллельных процессов [4].

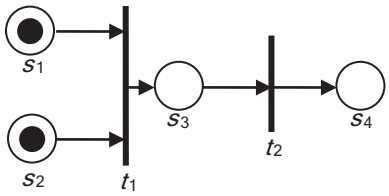
Проведенный анализ 217 угроз, представленных в настоящее время на официальном сайте банка данных угроз информационной безопасности, разработанного Федеральной службой по техническому и экспертному контролю (ФСТЭК) России (bdu.fstec.ru) [5], особенностей эксплуатации современных защищенных АС на объектах информатизации ОВД, результатов опроса экспертов в области безопасности информации позволил выделить восемь типов наиболее опасных и часто реализуемых в настоящее время сетевых атак на информационный ресурс АС ОВД с учетом их источников,

объектов воздействия и возможных последствий реализации (причиненного ущерба) [6]. Сформированный перечень включает в себя следующие основные типы атак: 1) анализ сетевого трафика, 2) сканирование сети, 3) «парольная» атака, 4) подмена доверенного объекта сети, 5) навязывание ложного маршрута, 6) внедрение ложного объекта сети, 7) отказ в обслуживании, 8) удаленный запуск приложений [7].

Построение сетей Петри-Маркова для атак из приведенного перечня позволит в дальнейшем смоделировать процесс их реализации, используя программную среду имитационного моделирования CPN Tools, и получить количественные значения вероятностно-временных характеристик каждой сетевой атаки на информационный ресурс АС ОВД.

При построении сетей использованы следующие обозначения: S_i – позиции, t_j – переходы.

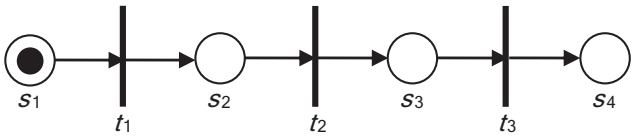
Вид сети Петри-Маркова для атаки «Анализ сетевого трафика» (сниффинг пакетов) представлен на рисунке 1 [1].



S_1 – атакуемые хосты готовы;
S_2 – хост злоумышленника физически готов к перехвату трафика;
t_1 – передача пакета между атакуемыми хостами, перехват пакета;
S_3 – пакет перехвачен;
t_2 – анализ пакета, извлечение необходимых данных (пароля, имени пользователя);
S_4 – полезные данные извлечены из пакета

Рис. 1. Вид сети Петри-Маркова для атаки «Анализ сетевого трафика»

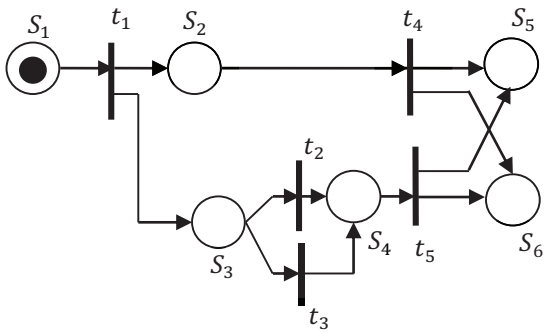
Вид сети Петри-Маркова, моделирующей атаку «Сканирование сети», приведен на рисунке 2 [1].



S_1 – хост злоумышленника готов, программа настроена и запущена;
t_1 – определение активных хостов сети при помощи ICMP-запроса;
S_2 – активные хосты определены;
T_2 – определение типов ОС активных хостов сети;
S_3 – типы ОС определены;
t_3 – сканирование сервисов на активных хостах сети;
S_4 – активные сервисы определены

Рис. 2. Вид сети Петри-Маркова для атаки «Сканирование сети»

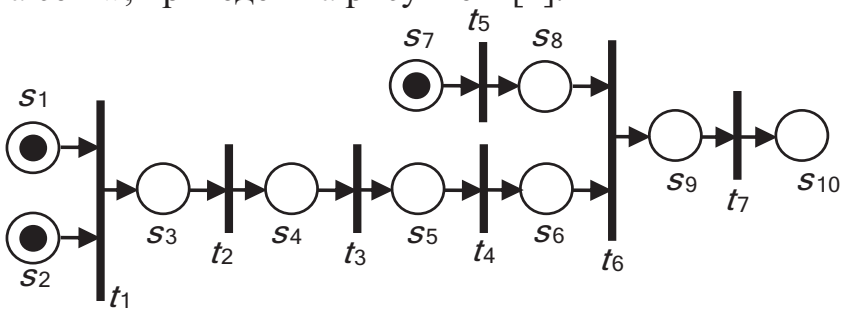
Вид сети Петри-Маркова для «Парольной» атаки представлен на рисунке 3 [8].



S_1 – хост злоумышленника готов, включился в сеть общего пользования;
t_1 – атакуемый хост запрашивает пароль;
S_2 – атакуемым хостом запрос пароля проведен;
S_3 – хост злоумышленника, не зная пароля, решил подобрать его по специальному словарю или путем прямого перебора;
t_2 – подбор пароля по словарю;
t_3 – подбор пароля прямым перебором;
S_4 – результат подбора пароля;
t_4, t_5 – промежуточные псевдо переходы;
S_5 – пароль подобран правильно, НСД к атакуемому хосту осуществлен;
S_6 – пароль подобран неправильно, атака сорвана

Рис. 3. Вид сети Петри-Маркова для «Парольной» атаки

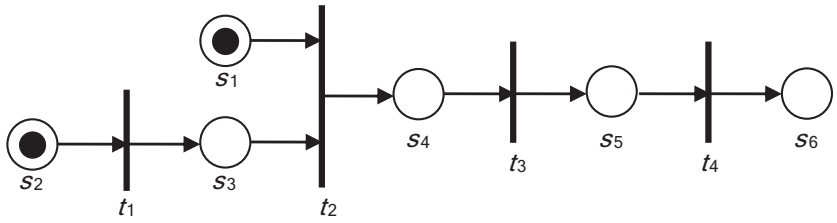
Вид сети Петри-Маркова, моделирующей атаку «Подмена доверенного объекта сети», приведен на рисунке 4 [1].



S_1 – атакуемый хост готов;
S_2 – хост злоумышленника готов к проведению атаки SYN-flood и ожидает перезагрузки атакуемого хоста;
t_1 – перезагрузка атакуемого хоста (в результате атаки SYN-flood или самопроизвольная);
S_3 – атакуемый хост недоступен;
t_2 – отправка C-SYN;
S_4 – C-SYN обработан сервером;
t_3 – прием S-SYN;
S_5 – S-SYN принят хостом злоумышленника;
t_4 – отправка C-SYN2 от имени атакуемого хоста;
S_6 – C-SYN2 обработан сервером;
S_7 – хост злоумышленника готов к подбору S-ACK2;
t_5 – подбор S-ACK2;
S_8 – S-ACK2 подобран;
t_6 – отправка подходящего S-ACK2;
S_9 – S-ACK2 принят, соединение с правами атакуемого хоста установлено;
t_7 – отправка данных;
S_{10} – результат – выполнение сервером команды злоумышленника

Рис. 4. Вид сети Петри-Маркова для атаки «Подмена доверенного объекта сети»

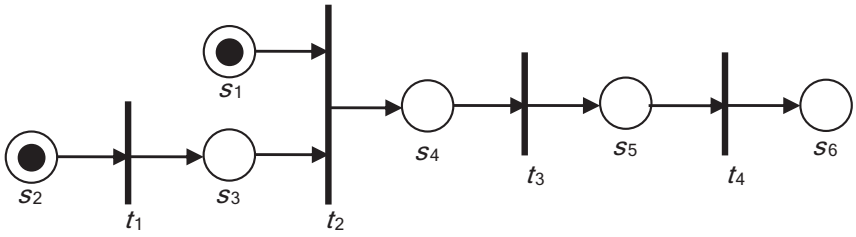
Вид сети Петри-Маркова, моделирующей атаку «Навязывание ложного маршрута», представлен на рисунке 5 [1].



S_1 – атакуемый хост готов;
S_2 – злоумышленник активен;
t_1 – настройка программы;
S_3 – программа настроена;
t_2 – передача ложных ICMP-redirect-сообщений на атакуемый хост;
S_4 – ложное ICMP-redirect-сообщение принято атакуемым хостом;
t_3 – изменение таблицы маршрутизации атакуемого хоста;
S_5 – таблица маршрутизации атакуемого хоста изменена;
t_4 – перехват и анализ трафика атакуемого хоста (для внутрисегментной атаки);
t_4 – нарушение маршрутизации атакуемого хоста (для межсегментной атаки);
S_6 – трафик перехвачен и проанализирован (для внутрисегментной атаки);
S_6 – связь между атакуемым хостом и сервером нарушена (для межсегментной атаки)

Рис. 5. Вид сети Петри-Маркова для атаки «Навязывание ложного маршрута»

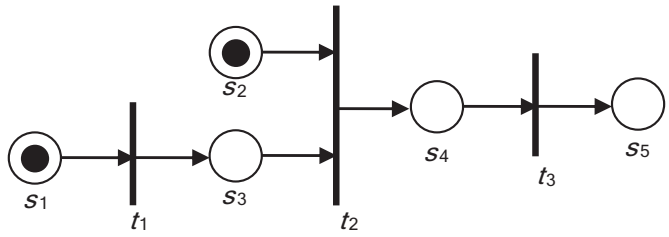
Вид сети Петри-Маркова, моделирующей атаку «Внедрение ложного объекта сети» (ARP-spoofing), приведен на рисунке 6 [1].



S_1 – атакуемый хост формирует широковещательный ARP-запрос;
S_2 – хост злоумышленника находится внутри сегмента сети атакуемого хоста;
t_1 – подготовка к проведению атаки (сканирование MAC-адресов хостов сети и настройка программы);
S_3 – хост злоумышленника готов к проведению атаки;
t_2 – отправка ложного ARP-ответа;
S_4 – ложный ARP-ответ принят атакуемым хостом;
t_3 – изменение ARP-таблицы атакуемого хоста;
S_5 – ARP-таблица атакуемого хоста изменена;
t_4 – перехват и анализ трафика атакуемого хоста;
S_6 – результат – трафик перехвачен и проанализирован

Рис. 6. Вид сети Петри-Маркова для атаки «Внедрение ложного объекта сети»

Вид сети Петри-Маркова для атаки «Отказ в обслуживании» (SYN-flood) представлен на рисунке 7 [1].



S_1 – хост злоумышленника готов;

t_1 – запуск и настройка программы для SYN-flood;

S_2 – атакуемый хост готов принять SYN-пакеты с несуществующим обратным адресом в очередь неоткрытых соединений;

S_3 – программа запущена и настроена;

t_2 – отправка SYN-пакетов и постановка их в очередь атакуемому хосту;

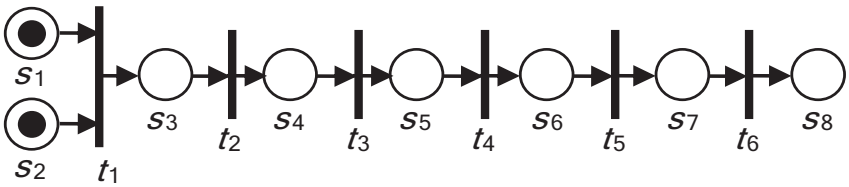
S_4 – запросы поставлены в очередь ожидаемых соединений атакуемому хосту;

t_3 – переполнение очереди атакуемого хоста;

S_5 – атакуемый хост не в состоянии обрабатывать другие запросы

Рис. 7. Вид сети Петри-Маркова для атаки «Отказ в обслуживании»

Вид сети Петри-Маркова, моделирующей атаку «Удаленный запуск приложений» (IP-hijacking), приведен на рисунке 8 [1].



S_1 – атакуемые хосты готовы;

S_2 – хост злоумышленника готов к перехвату трафика;

t_1 – обмен пакетами между атакуемыми хостами для установления соединения, перехват;

S-SYN и C-ACK;

S_3 – пакет S-SYN, C-ACK перехвачен;

t_2 – отправка RST от имени второго атакуемого хоста;

S_4 – соединение между атакуемыми хостами закрыто для первого из них;

t_3 – отправка первым атакуемым хостом S-SYN2 для второго хоста, перехват S-SYN2;

S_5 – C-SYN2 обработан первым атакуемым хостом;

t_4 – отправка C-SYN2 от имени второго атакуемого хоста;

S_6 – S-SYN2 перехвачен, возникновение ACK-бури между атакуемыми хостами;

t_5 – отправка S-ACK2 от имени второго атакуемого хоста;

S_7 – S-ACK2 прият, соединение с правами второго атакуемого хоста установлено;

t_6 – обмен модифицированными данными со вторым атакуемым хостом по ACK, с первым – по ACK-2;

S_8 – результат

Рис. 8. Вид сети Петри-Маркова для атаки «Удаленный запуск приложений»

Перспективы использования представленных моделей динамики реализации типовых сетевых атак на информационный ресурс современных АС ОВД связаны с оцениванием опасности реализации сетевых атак и разработкой модели актуальных атак для формирования количественных требований к системам защиты информации от несанкционированного доступа в АС, эксплуатируемых в защищенном исполнении на объектах информатизации ОВД, что поможет повысить реальную защищенность существующих и разрабатываемых систем.

ЛИТЕРАТУРА

1. Радько Н.М. Проникновения в операционную среду компьютера: модели злоумышленного удаленного доступа / Н.М. Радько, Ю.К. Язов, Н.Н. Корнеева. – Воронеж: Воронеж. госуд. технич. ун-т, 2013. – 265 с.
2. Синегубов С.В. Моделирование систем и сетей телекоммуникаций / С.В. Синегубов. – Воронеж: Воронеж. ин-т МВД России, 2016. – 336 с.
3. Применение математического аппарата сетей Петри-Маркова для определения временных и вероятностных характеристик системы управления высоконагруженными веб-порталами с повышенной отказоустойчивостью / Р.Н. Акиншин [и др.] // Научный вестник МГТУ ГА. – 2014. – № 210. – С. 87-90.
4. Котов В.Е. Сети Петри / В.Е. Котов. – Москва: Наука, 1984. – 158 с.
5. Банк данных угроз ФСТЭК России. [Электронный ресурс]. – Режим доступа: http://bdu.fstec.ru/threat. – (Дата обращения: 30.09.2020).
6. Анализ и классификация основных угроз информационной безопасности автоматизированных систем на объектах информатизации органов внутренних дел / А.В. Бацких [и др.] // Безопасность информационных технологий = IT Security. – Т. 27. – № 1. – 2020. – С. 40-50.
7. Овчинникова Е.С. Анализ типовых сетевых атак на автоматизированные системы органов внутренних дел / И.Г. Дровникова, Е.С. Овчинникова, В.В. Конобеевских // Вестник Дагестанского госуд. технич. ун-та. Технич. науки. – Т. 47. – № 1. – 2020. – С. 72-85.
8. Язов Ю.К. Организация защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. – Воронеж: Кварта, 2018. – 588 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Дровникова Ирина Григорьевна. Профессор кафедры автоматизированных информационных систем ОВД. Доктор технических наук, доцент.

Воронежский институт МВД России.

E-mail: idrovnikova@mail.ru

Россия, 394065, г. Воронеж, просп. Патриотов, 53. Тел. (473) 200-51-82.

Овчинникова Елена Сергеевна. Адъюнкт кафедры автоматизированных информационных систем ОВД.
Воронежский институт МВД России.
E-mail: yelena_ovchinnikova1@mail.ru
Россия, 394065, г. Воронеж, проспект Патриотов, 53.
Тел. (473) 200-51-90.

Drovnikova Irina Grigoryevna. Professor of the chair of Automatic Information Systems. Doctor of technical sciences.
Voronesh Institute of the Ministry of the Interior of Russia.
Work address: Russia, 394065, Voronezh, Patriotov Prospect, 53.
Tel. (473) 200-51-82.

Ovchinnikova Elena Sergeevna. Post-graduate student of the chair of information systems in interior affairs department.
Voronezh Institute of the Ministry of the Interior of Russia.
E-mail: yelena_ovchinnikova1@mail.ru
Work address: Russia, 394065, Voronezh, Prospect Patriotov, 53.
Tel. (473) 200-51-90.

Ключевые слова: автоматизированная система; сетевая атака; сеть Петри-Маркова; динамическая модель; вероятностно-временные характеристики.
Key words: automated system; network attack; Petri-Markov network; dynamic model; probabilistic-time characteristics.

УДК 004.051