УДК 621.39

МОДЕЛИРОВАНИЕ АТАКИ СПУФИНГА В КОМПЛЕКСНОЙ СИСТЕМЕ СИНХРОНИЗАЦИИ И ДОСТАВКИ ШКАЛЫ ВРЕМЕНИ

Е. В. ОПАРИН, Е. В. ОПАРИНА
Петербургский государственный университет путей сообщения
Императора Александра I
Санкт-Петербург, Россия

Комплексная система синхронизации и доставки шкалы времени является важным элементом современных и перспективных телекоммуникационных сетей, вследствие чего системы синхронизации и доставки шкалы времени постоянно подвержены атакам различной природы со стороны организованных злоумышленников, в том числе и атакам спуфинга [1–3].

На рис. 1 представлена разработанная модель атаки спуфинга в комплексной системе синхронизации и доставки шкалы времени, которая содержит все основные этапы воздействия организованного злоумышленника, независимо от применяемых технологических решений построения сетей связи и состава инструментария атакующего.

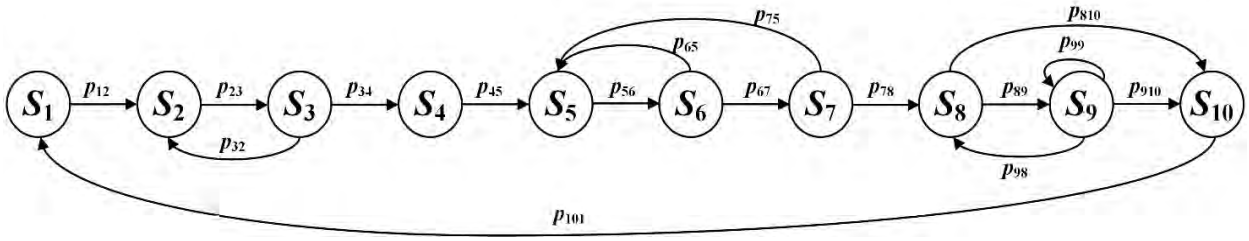

Рис. 1. Модель действий злоумышленника, реализующего атаку спуфинга в комплексной системе синхронизации и доставки шкалы времени

Указанная модель (см. рис. 1) включает в себя следующие состояния: S_1 – исходное состояние; S_2 – сбор злоумышленником исходных данных об объекте атаки; S_3 – обработка злоумышленником полученных исходных данных; S_4 – разрыв соединения в выбранном сегменте атаки; S_5 – состояние, когда злоумышленник осуществляет идентификацию своего узла в системе; S_6 – состояние, когда злоумышленник осуществляет аутентификацию своего узла в системе; S_7 – состояние, когда злоумышленник осуществляет авторизацию своего узла в системе; S_8 – состояние, когда злоумышленник осуществляет мероприятия, направленные на поддержание своего легитимного присутствия в системе; S_9 – состояние, когда злоумышленник осуществляет генерирование вредоносных сообщений; S_{10} – завершение атаки [4, 5].

Для оценки вероятностно-временных характеристик атаки спуфинга в комплексной системе синхронизации и доставки шкалы времени построена имитационная модель в среде *AnyLogic* (рис. 2).

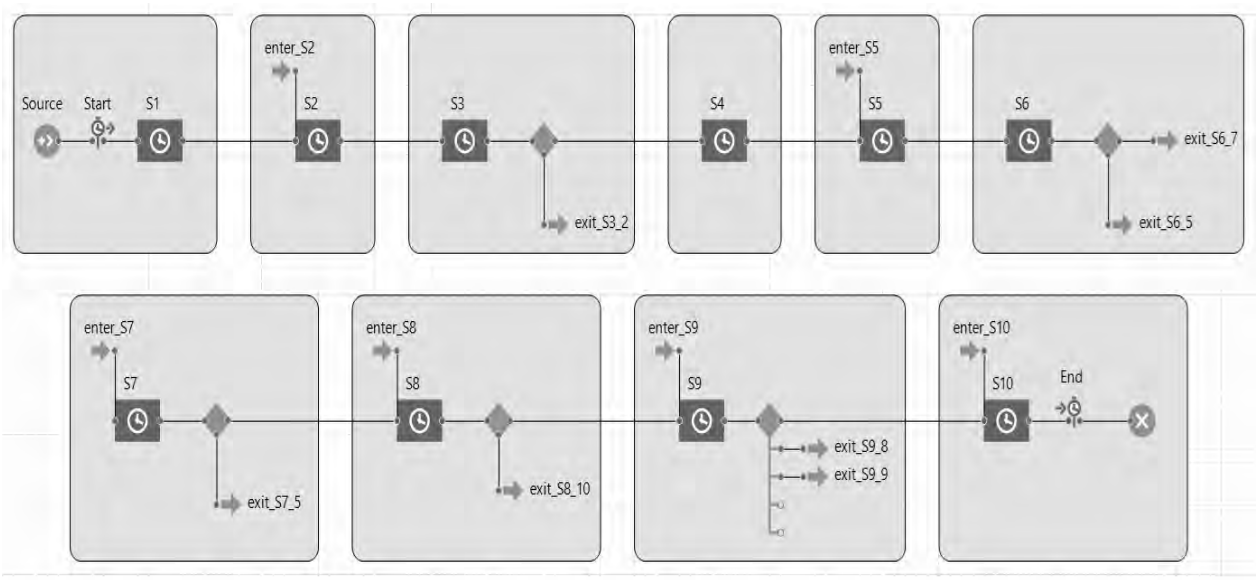

Рис. 2. Имитационная модель процесса проведения атаки спуфинга в комплексной системе синхронизации и доставки шкалы времени

По результатам проведенного имитационного моделирования получено, что среднее время атаки спуфинга составляет 347,49 ч, что примерно равно 14,48 сут.

В итоге разработана имитационная модель действий злоумышленника при реализации атаки спуфинга в комплексной системе синхронизации и доставки шкалы времени, которая независима от состава исходных данных. Модель полностью работоспособна и адекватна. Полученные результаты могут служить основой, анализируя которые специалисты информационной безопасности могут оптимально распределять имеющиеся в своем распоряжении ресурсы, чтобы наиболее эффективно блокировать действия организованного злоумышленника.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. **Канаев, А. К.** Обеспечение информационной безопасности системы тактовой сетевой синхронизации на основе её энтропийного анализа / А. К. Канаев, Е. В. Опарин, Е. В. Опарина // Изв. Петерб. ун-та путей сообщения. – 2022. – Т. 19, № 3. – С. 505–514.

2. Вербальная модель процесса взаимодействия телекоммуникационной сети объекта с системой злоумышленника / Н. В. Евглевская [и др.] // Изв. Тульского гос. ун-та. Технические науки. – 2020. – № 7. – С. 265–269.

3. Модели компьютерных атак на программно-конфигурируемые сети / И. Б. Саенко [и др.] // Наукоемкие технологии в космических исследованиях Земли. – 2023. – Т. 15, № 1. – С. 37–47.

4. **Алексеев, А. И.** Сети, чувствительные ко времени, и их использование на железнодорожном транспорте / А. И. Алексеев, А. К. Канаев // СПБНТОРЭС: тр. ежегодной науч.-техн. конф. – 2023. – № 1 (78). – С. 202–205.

5. **Канаев, А. К.** Использование служебного канала для построения сети синхронизации в OTN / А. К. Канаев, Э. В. Логин, Ф. А. Прошин // СПБНТОРЭС: тр. ежегодной науч.-техн. конф. – 2022. – № 1 (77). – С. 144–147.