РАКЕТНО-КОСМИЧЕСКОЕ ПРИБОРОСТРОЕНИЕ И ИНФОРМАЦИОННЫЕ СИСТЕМЫ
2022, том 9, выпуск 4, с. 9–16

СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ КОСМИЧЕСКИМИ АППАРАТАМИ, ОБРАБОТКА ИНФОРМАЦИИ И СИСТЕМЫ ТЕЛЕМЕТРИИ. ДИСТАНЦИОННОЕ ЗОНДИРОВАНИЕ ЗЕМЛИ

УДК 621.39 DOI 10.30894/issn2409-0239.2022.9.4.9.16

Полумарковская модель деятельности злоумышленника при реализации атаки спуфинга в подсистеме единого времени

А. К. Канаев, *д. т. н., профессор, kanaevak@mail.ru*
Петербургский государственный университет путей сообщения Императора Александра I, Санкт-Петербург, Российская Федерация
Е. В. Опарин, *к. т. н., onapuh@mail.ru*
Гипротранссигналсвязь — филиал АО «Росжелдорпроект», Санкт-Петербург, Российская Федерация
Е. В. Опарина, *к. т. н., доцент, sirayaekaterina@mail.ru*
Петербургский государственный университет путей сообщения Императора Александра I, Санкт-Петербург, Российская Федерация

Аннотация. В статье приведен анализ процесса функционирования систем единого времени в составе телекоммуникационной системы. Выделены основные средства генерирования, распространения и передачи сигналов единого времени. Приведены основные риски для систем связи при нарушении процесса функционирования. На основе анализа процесса функционирования и выделенных рисков сформированы основные угрозы системам единого времени со стороны организованных злоумышленников. В особый класс угроз выделены атаки спуфинга. Для атак спуфинга разработана типовая модель действий злоумышленника при реализации атаки. Для разработки данной модели использовался аппарат полумарковских процессов. Представленная модель спуфинга послужила основой для оценки стационарных характеристик процесса проведения атаки. Данная модель также использовалась для анализа процесса противоборства систем безопасности и организованных злоумышленников. В процессе анализа были рассмотрены различные сценарии противоборства в зависимости от имеющихся в наличии противоборствующих сторон ресурсов. Показателем ресурсов при проведении моделирования использовалась интенсивность воздействий противоборствующими сторонами. Результаты моделирования позволили отразить конечный итог противоборства, оценить деятельность противоборствующих сторон, а также состояние системы единого времени в зависимости от результатов противоборства.

Ключевые слова: полумарковская модель, система единого времени, телекоммуникационная система, атака, уязвимость, злоумышленник, спуфинг

A Semi-Markov Model of Attacker Activity When Implementing Spoofing Attacks in a Common Time Subsystem

A. K. Kanayev, *Dr. Sci. (Engineering), Prof., kanaevak@mail.ru*
Emperor Alexander I St. Petersburg State Transport University, St. Petersburg, Russian Federation
E. V. Oparin, *Cand. Sci. (Engineering), onapuh@mail.ru*
Giprotranssignalsvyaz — branch of JSC "Roszheldorproject", St. Petersburg, Russian Federation
E. V. Oparina, *Cand. Sci. (Engineering), Associate Professor, sirayaekaterina@mail.ru*
Emperor Alexander I St. Petersburg State Transport University, St. Petersburg, Russian Federation

Abstract. The article analyzes the process of functioning of common time systems as a part of telecommunications system. The main means of generating, distributing, and transmitting single time signals are given. The main risks for communications systems in case of violating the process of functioning are presented. Based on the analysis of the process of functioning and identified risks, the main threats to common time systems from organized attackers are formed. Spoofing attacks are singled out as a special class of threats. A typical model of an attacker's actions during an attack is developed for spoofing attacks. The semi-Markov process apparatus was used to develop this model. The presented spoofing model was used as the basis for estimating the stationary characteristics of the attack process. This model was also applied to analyze the process of confrontation between security systems and organized attackers. The analysis considered different confrontation scenarios depending on the resources available to the confronting parties. The resource metric used in the simulation was the intensity of the opposing parties. The results of the simulation allowed us to reflect the outcome of the confrontation and assess the activities of the opposing parties, as well as the state of a common time system depending on the results of the confrontation.

Keywords: semi-Markov model, common time system, telecommunications system, attack, vulnerability, attacker, spoofing

Введение

Система единого времени (СЕВ) является одной из ключевых и значимых подсистем современных и перспективных сетей связи, определяющих их надежное и устойчивое функционирование.

Многие процессы, происходящие в телекоммуникационных системах (ТКС), зависят от моментов времени и очередности прохождения информационных сигналов, а также от их длительности. При этом различие показаний времени в различных информационных автоматизированных системах снижает эффективность и надежность их функционирования, сводит к минимуму их совместимость и возможность интеграции. Функционирование подсистемы СЕВ влияет также на качество принятия управленческих решений и решения задач по прогнозированию процесса функционирования ТКС.

Сложную задачу представляет собой организация процесса функционирования подсистемы СЕВ в территориально-распределенных комплексах, поскольку необходимо передавать сигналы точного времени на значительные расстояния [1, 2].

В настоящее время число устройств и узлов в телекоммуникационных системах непрерывно возрастает, а также возрастает число систем, при эксплуатации которых необходимы сигналы точного времени. При возникновении отказов в подсистеме СЕВ нарушается процесс функционирования различных технологических систем, снижается уровень их управляемости, возможна потеря данных контроля и мониторинга, возникают дополнительные ошибки в системах передачи, анализа и обработки информации [3–5].

Из-за указанных свойств подсистемы СЕВ данная подсистема является вероятным объектом атаки со стороны организованных злоумышленников. Опасность воздействия на подсистему СЕВ заключается в том, что нарушение процесса функционирования подсистемы СЕВ приводит к последующим отказам ТКС или отдельных ее частей.

При воплощенных атаках происходит общее снижение надежности ТКС, а также понижение ее живучести, что в конечном счете сказывается на уменьшении ее устойчивости, причем как структурной, путем изменения топологии и межэлементных связей, так и функциональной, путем снижения качества предоставляемых услуг.

Функционирование подсистемы единого времени под воздействием атак организованных злоумышленников

Для распространения сигналов точного времени используется множество средств, которые включают в себя глобальные навигационные спутниковые системы, системы спутниковой связи, радиостанции длинно- и коротковолнового диапазона, волоконно-оптические линии связи, системы передачи плезиохронной и синхронной цифровой иерархии, а также сети передачи данных с использованием протоколов NTP и PTP [2–4].

Основными угрозами для подсистемы СЕВ со стороны организованных злоумышленников являются: манипуляция и спуфинг временных меток, изменение настроек в устройствах системы единого времени, DoS-атаки, атаки на генераторное оборудование и источники сигналов точного времени, а также сетевая разведка [6, 7].

При описании атаки спуфинга в системах передачи единого времени чаще всего обращают внимание на спуфинг атаки в системах, функционирующих на основе глобальных навигационных спутниковых систем (ГНСС). В основе данных атак лежат воздействия на навигационные сигналы специально сформированными сигналами, которые структурно подобны исходным сигналам. Тем не менее подобного рода атаки могут быть реализованы в различных подсистемах СЕВ, независимо от применяемых источников сигналов точного времени, средств и протоколов распространения сигналов, а также средств формирования и хранения локальных шкал времени.

В данной статье предлагается обобщенная модель действий злоумышленника при реализации атаки спуфинга в подсистеме СЕВ. Данная модель содержит все основные этапы воздействия, независимо от применяемых технологических решений при ее построении.

Следует отметить, что при реализации данной атаки злоумышленник должен иметь в своем распоряжении узел, способный по своим характеристикам выполнять функции полноценного узла подсистемы СЕВ.

При спуфинговых атаках в подсистеме СЕВ функционирует узел-генератор сообщений сигналов точного времени, который маскируется под легитимный узел в сети. Данный узел может создавать сообщения, содержащие сигналы точного времени.

При реализации атаки спуфинга возможны два сценария [8, 9]:

– злоумышленник выдает себя за ведущее устройство, что позволяет ему распространять ложную информацию времени в подсистеме СЕВ;

– злоумышленник выдает себя за подчиненное или промежуточное устройство, что позволяет ему отправлять вредоносные сообщения легитимным ведущим устройствам, и заставлять таким образом ведущие устройства реагировать, что может вызвать нарушения при функционировании ведущих устройств, а также привести к тому, что ведущие устройства впоследствии могут отвечать остальным легитимным устройствам сообщениями, в основе которых лежит ложная информация.

Реализация спуфинговых атак в подсистеме единого времени

Проведенный анализ различных сценариев проведения атаки спуфинга в подсистеме СЕВ позволяет сформировать полумарковскую модель действий злоумышленника, указанную на рис. 1.

Указанная модель отражает все основные этапы атаки спуфинга в подсистеме СЕВ и включает в себя следующие состояния [13]:

S_1 — исходное состояние, характеризуемое функционированием подсистемы СЕВ в соответствии с нормативными значениями;

S_2 — получение злоумышленником исходных данных о структуре СЕВ и принципах ее функционирования;

S_3 — обработка злоумышленником исходных данных и выбор сегмента атаки;

S_4 — разрыв соединения и передачи сообщений в выбранном сегменте атаки;

S_5 — идентификация злоумышленником своего узла в подсистеме СЕВ;

S_6 — злоумышленник осуществляет аутентификацию своего узла в подсистеме СЕВ;

S_7 — злоумышленник осуществляет авторизацию своего узла в подсистеме СЕВ;

S_8 — злоумышленник проводит действия, направленные на поддержание своего легитимного присутствия в подсистеме СЕВ;

S_9 — злоумышленник осуществляет генерирование вредоносных сообщений, содержащих сигналы точного времени, перенаправление проходящего трафика и другие воздействия в соответствии со своими намерениями;

S_{10} — состояние завершения атаки, когда злоумышленник покидает подсистему СЕВ или его действия локализованы.

Действия злоумышленника в подсистеме СЕВ при реализации атаки спуфинга следующие. В исходном состоянии S_1 подсистема СЕВ работоспособна и функционирует в соответствии с нормативными значениями. Примем, что злоумышленник имеет в своем распоряжении узел связи, способный выполнять функции узла СЕВ, пропускать через себя трафик СЕВ и генерировать временные метки. В состоянии S_2 злоумышленник осуществляет сбор исходных данных об объекте атаки, включая технологические решения и методы передачи сигналов времени. В состоянии S_3 осуществляется выбор сегмента атаки в соответствии с целями и задачами,

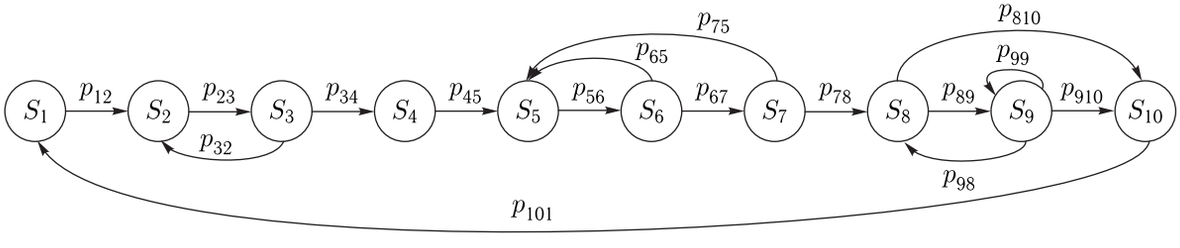

Рис. 1. Модель действий злоумышленника, реализующего атаку спуфинга в подсистеме СЕВ

которые ставит перед собой злоумышленник. Состояние S_4 характеризуется тем, что злоумышленник разрывает соединение в выбранном сегменте с целью внедрения в цепь передачи сигналов времени своего узла. Например, при атаках на ГНСС системы злоумышленник транслирует поддельный сигнал с аналогичными характеристиками, но с более высоким уровнем передачи, чем истинный. При использовании других средств доставки сигналов точного времени злоумышленником может быть использована атака «человек посередине». Действия злоумышленника в состояниях S_5, S_6 и S_7 направлены на то, чтобы легитимизировать свой узел в структуре СЕВ. В состоянии S_5 узел злоумышленника идентифицируется в системе СЕВ, далее аутентифицируется и авторизуется с ролью ведущего или ведомого устройства. Например, в атаках на ГНСС системы атакуемое устройство настроено таким образом, что осуществляет выбор сигнала с лучшим качеством; таким образом, злоумышленник перехватывает управление. При использовании других технологий злоумышленники подбирают ключи шифрования и аутентификации. Чтобы не допустить своего обнаружения, злоумышленнику необходимо постоянно следить за текущей ситуацией в системе СЕВ, корректируя свои воздействия, данному состоянию соответствует состояние S_8. В ГНСС системах это соответствует тому, что злоумышленник изменяет местоположение шаг за шагом, чтобы атакуемое устройство не заблокировало злоумышленника как источника помех. При передаче сигналов точного времени в локальных сетях СПД злоумышленник может изменять файлы регистрации событий, добавлять на узлы дополнительные файлы, организовывая при этом тайные сетевые каналы. Состояние S_9 представляет собой наиболее активную фазу атаки, в которой злоумышленник генерирует вредоносные сообщения и отправляет их смежным узлам, перенаправляет и видоизменяет проходящий трафик, задерживает сообщения, содержащие сигналы точного времени. Действия злоумышленника продолжаются до состояния S_{10}, пока не будут достигнуты поставленные цели или злоумышленник не будет обнаружен и локализован, после чего система СЕВ возвращается к исходному режиму работы до атаки.

Оценка стационарных характеристик процесса атаки спуфинга

Выделим необходимые стационарные характеристики процесса реализации атаки спуфинга:

– вероятности π_i нахождения в каждом из состояний S_i,

– среднее время атаки T_{A}.

Для вычисления указанных стационарных характеристик необходимо иметь в наличии следующие исходные данные:

1. Матрицу переходных вероятностей $\Pi = (p_{ij})$.

2. Матрицу функций распределения условных случайных времен нахождения в каждом из S_i состояний $F_{ij}(t)$;

Стационарную вероятность нахождения в каждом из состояний S_i определим по формуле (1) [14]:

$$\pi_i = \frac{P_i T_i}{\sum\limits_{j \in S} P_j T_j} \quad (i, j = 1, \ldots, 10; i, j \in S; \sum_{i \in S} \pi_i = 1), \tag{1}$$

где P_i, P_j — стационарные вероятности пребывания вложенной однородной марковской цепи в состояниях S_i и S_j, T_i, T_j — математические ожидания безусловного времени пребывания процесса атаки спуфинга в каждом состоянии.

Для оценки математических ожиданий используем следующие выражения (2), (3) [14]:

$$T_i = \sum_{j \in S} p_{ij} T_{ij}, \tag{2}$$

$$T_{ij}(t) = \int_0^\infty [1 - F_{ij}(t)]\, dt, \tag{3}$$

где T_{ij} — математическое ожидание условного времени нахождения в каждом из состояний.

Для оценки стационарных вероятностей пребывания вложенной однородной марковской цепи в S_i состояниях используем следующие выражения (4), (5) [14]:

$$P_i = \frac{D_i}{\sum\limits_{j=1}^{n} D_j}, \tag{4}$$

где $D_i(D_j)$ — минор, получаемый вычеркиванием соответствующих строк и столбцов матрицы D

$$D = \begin{pmatrix} 1-p_{11} & -p_{12} & \dots & -p_{110} \\ -p_{21} & 1-p_{22} & \dots & -p_{210} \\ \dots & \dots & \dots & \dots \\ -p_{101} & -p_{102} & \dots & 1-p_{1010} \end{pmatrix}. \quad (5)$$

Для вычисления среднего времени атаки разделим множество состояний S на два непересекающихся подмножества: состояния, в которых злоумышленник проводит активные действия, $S_{\text{А}} \subset S$, и состояния, в которых злоумышленник пассивен, $\overline{S_{\text{А}}} \subset S$.

Множество $S_{\text{А}}$ будет включать в себя состояния S_1–S_9, а множество $\overline{S_{\text{А}}}$ соответственно состояние S_{10}.

Таким образом, среднее время атаки и среднее время восстановления от последствий проведения атаки можно вычислить по следующим выражениям (6), (7):

$$T_{\text{А}} = \frac{\sum\limits_{i \in S_{\text{А}}} P_i T_i}{\sum\limits_{i \in S_+} P_i \sum\limits_{j \in \overline{S_{\text{А}}}} p_{ij}}, \quad (6)$$

$$T_{\text{В}} = \frac{\sum\limits_{i \in \overline{S_{\text{А}}}} P_i T_i}{\sum\limits_{i \in S_-} P_i \sum\limits_{j \in S_{\text{А}}} p_{ij}}, \quad (7)$$

где S_+ и S_- — подмножество граничных состояний между множествами $S_{\text{А}}$ и $\overline{S_{\text{А}}}$.

Подмножество S_+ включает состояния S_8 и S_9. Подмножество граничных состояний S_- определяется состоянием S_{10}.

Стационарные вероятности π_i позволяют определить коэффициент исправного действия $K_{\text{и}}$ подсистемы СЕВ, который характеризует ее устойчивость в процессе нормального функционирования и под воздействием атак [6]. В этой связи коэффициент исправного действия K_u подсистемы СЕВ равен (8):

$$K_{\text{и}} = \sum_{i=1,\dots,9} \pi_i. \quad (8)$$

В состоянии S_{10} подсистема СЕВ не функционирует вследствие проведения восстановительных и настроечных работ.

В качестве примера приводится оценка стационарных характеристик процесса атаки спуфинга. Матрица П имеет следующий вид (9):

$$\Pi = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0{,}1 & 0 & 0{,}9 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0{,}1 & 0 & 0{,}9 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0{,}1 & 0 & 0 & 0{,}9 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0{,}7 & 0{,}3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0{,}1 & 0{,}45 & 0{,}45 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \quad (9)$$

В качестве распределений времени пребывания в состояниях принято экспоненциальное распределение со следующей матрицей интенсивностей переходов (10):

$$\Lambda = \begin{pmatrix} 0 & 0{,}005 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0{,}0055 & 0 & 10 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 5{,}5 & 0 & 6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 5{,}8 & 0 & 0 & 0{,}4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0{,}008 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0{,}45 & 2 & 0{,}008 \\ 0{,}05 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad \text{ч}^{-1}. \quad (10)$$

После дальнейшего расчета получены следующие стационарные вероятности пребывания в каждом из состояний S_i (11):

$$\pi_i = (0{,}54 \;\; 1{,}5 \cdot 10^{-3} \;\; 0{,}05 \;\; 5{,}4 \cdot 10^{-4} \;\; 8{,}34 \cdot 10^{-4} \;\; 5{,}61 \cdot 10^{-4} \;\; 6{,}8 \cdot 10^{-3} \;\; 0{,}12 \;\; 0{,}22 \;\; 0{,}05). \quad (11)$$

Среднее время атаки равно (12):

$$T_{\text{А}} = \frac{\sum\limits_{i \in S_{\text{А}}} P_i T_i}{\sum\limits_{i \in S_+} P_i \sum\limits_{j \in \overline{S_{\text{А}}}} p_{ij}} =$$

$$= \big(P_1T_1 + P_2T_2 + P_3T_3 + P_4T_4 + P_5T_5 + P_6T_6 + P_7T_7 + P_8T_8 + P_9T_9\big)/\big((P_8 + P_9)(p_{89} + p_{810})\big) = 179{,}2 \text{ ч} \approx 7{,}5 \text{ сут}. \quad (12)$$

Среднее время восстановления составляет (13):

$$T_{\text{В}} = \frac{\sum\limits_{i \in \overline{S_{\text{А}}}} P_i T_i}{\sum\limits_{i \in S_{\_}} P_i \sum\limits_{j \in S_{\text{А}}} p_{ij}} = \frac{P_{10}T_{10}}{P_{10}p_1} = 20 \text{ ч}. \quad (13)$$

Таким образом, для выбранных для примера расчета переходных вероятностей атака будет осуществляться в течение 7,5 сут. По истечении данного времени предполагается обнаружение злонамеренных действий и восстановление нормативного процесса функционирования. Среднее время восстановления последствий атаки, согласно (13), составит 20 ч.

Коэффициент исправного действия $K_{\text{и}}$ системы СЕВ составляет (14):

$$K_{\text{и}} = \sum_{i=1,\ldots,9} \pi_i = 0{,}95. \quad (14)$$

Оценим влияние интенсивности действий злоумышленника на среднее время атаки и влияние интенсивности деятельности службы безопасности на среднее время восстановления системы. Результаты моделирования приведены на рис. 2–3.

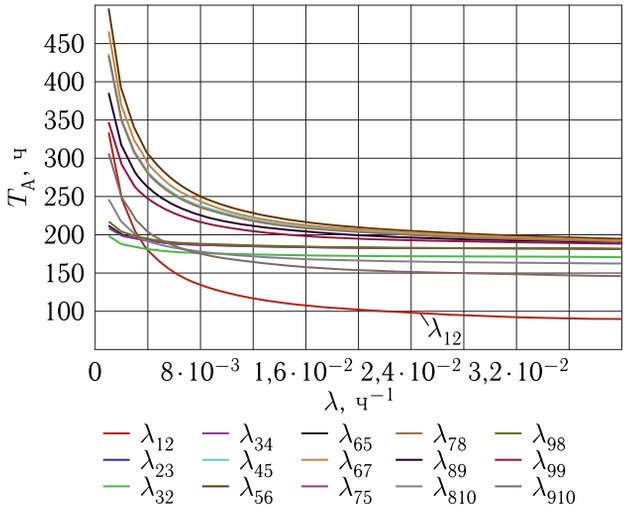

Рис. 2. Зависимость среднего времени атаки от активности деятельности злоумышленника

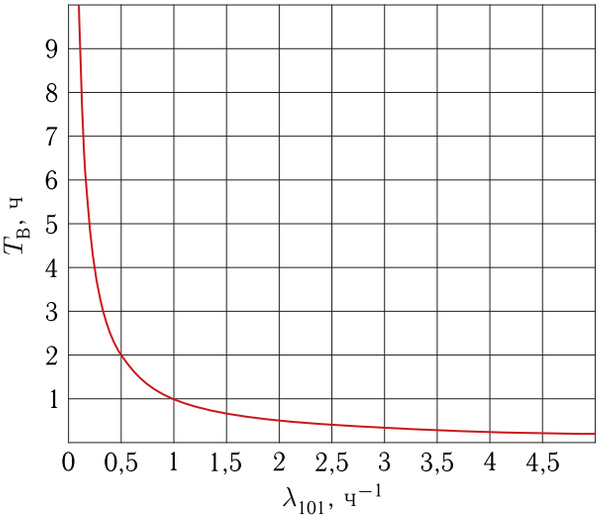

Рис. 3. Зависимость времени восстановления системы СЕВ от активности деятельности служб безопасности

Исследования зависимостей коэффициента исправного действия системы СЕВ от интенсивности атаки и интенсивности реакции службы безопасности приведены на рис. 4–5.

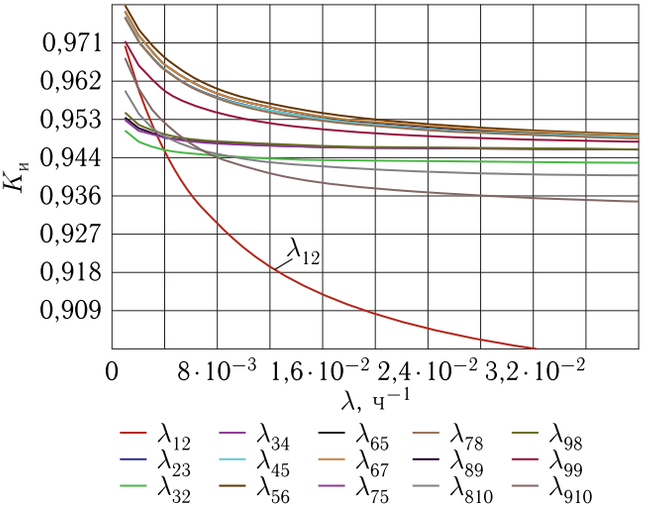

Рис. 4. Зависимость коэффициента исправного действия системы СЕВ от активности деятельности злоумышленника

По результатам моделирования можно сделать следующие выводы:

– анализ рисунков показывает, что увеличение интенсивности действий злоумышленника снижает коэффициент исправного действия системы СЕВ

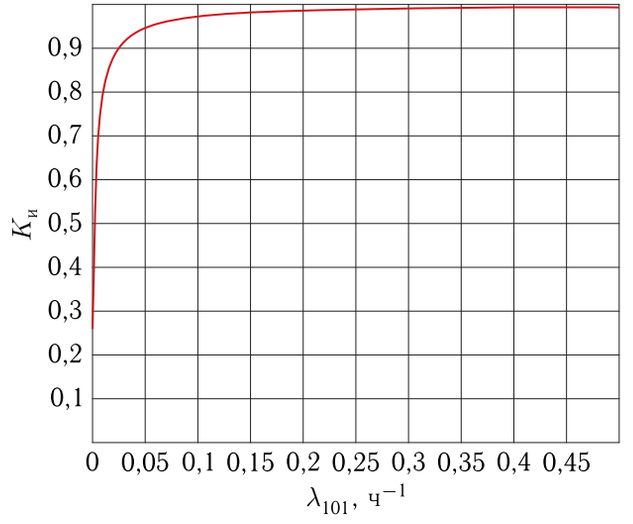

Рис. 5. Зависимость коэффициента исправного действия системы СЕВ от активности деятельности систем безопасности

в процессе ее функционирования, а также снижает время реализации атаки, тем не менее можно заметить, что при достижении определенного предела увеличение интенсивности действий злоумышленника не приносит ощутимых результатов;

– анализируя полученные зависимости, можно сделать вывод, что наибольший вклад в снижение времени, по истечении которого атака будет осуществлена, а также, достижение цели максимального понижения коэффициента исправного действия вносит сбор исходных данных и генерирование вредоносных сообщений;

– полученные результаты могут служить основой, анализируя которые администраторы информационной безопасности могут оптимально распределять имеющиеся в своем распоряжении ресурсы, чтобы наиболее эффективно блокировать действия организованного злоумышленника.

Заключение

Учитывая возрастающую потребность современных и перспективных сетей связи в сигналах точного времени, повсеместном распространении устройств и аппаратуры, позволяющих генерировать, передавать и потреблять сигналы точного времени, возрастает число угроз и потенциальных атак на системы, предоставляющие услуги по распространению сигналов точного времени. Анализ предполагаемых атак показал, что наиболее вероятной, способной нанести максимальный урон является атака спуфинга в системах единого времени. Особая угроза подобных атак заключается в том, что данные атаки возможны в любых системах передачи сигналов точного времени, не зависят от применяемых технологий распространения сигналов точного времени, а также представляют значительную сложность по блокированию злонамеренных действий и полноценному восстановлению процесса функционирования систем единого времени. В результате проделанной работы сформирована модель действий организованного злоумышленника при проведении атаки спуфинга в системах единого времени. При построении данной модели использовался аппарат полумарковских процессов, преимуществом которого является способность анализа деятельности злоумышленника в каждом состоянии вне зависимости от предыдущих путей перехода в данное состояние. Достоинством данной модели является независимость моделирования от применяемых средств и технологий доставки сигналов точного времени, что представляет возможность ее применения для различных систем. Данная модель является универсальной и позволяет производить оценку деятельности злоумышленника на всех этапах проведения атаки в зависимости от имеющихся в его распоряжении ресурсов, а также позволяет оценить способность администраторов безопасности блокировать данные атаки. Полученные результаты могут быть применены в действующих и проектируемых системах единого времени при построении средств информационной безопасности.

Список литературы

1. *Ванчиков А.С.* Синхронизация в современных сетях операторского класса // Автоматика, связь, информатика, 2018, № 8. С. 19–20.
2. *Канаев А.К.*, *Тощев А.К.* Рекомендации МСЭ-Т в области синхронизации инфотелекоммуникационных систем // Автоматика, связь, информатика, 2018, № 10. С. 8–14.
3. *Рыжков А.В.*, *Новожилов Е.О.* Средства и способы обеспечения единого точного времени // Автоматика, связь, информатика, 2018, № 12. С. 7–11.

4. *Гапанович В. А.*, *Слюняев А. Н.* Система единого времени ОАО «РЖД» // Автоматика, связь, информатика, 2018, № 12. С. 2–6.

5. *Ефремов М. А.*, *Калуцкий И. В.*, *Таныгин М. О.*, *Фрундин А. Г.* Обзор подходов к определению актуальных угроз информации телекоммуникационным системам и предложения по их совершенствованию // Телекоммуникации, 2017, № 5. С. 27–33.

6. *Коцыняк М. А.*, *Осадчий А. И.*, *Коцыняк М. М.*, *Лаута О. С.*, *Дементьев В. Е.*, *Васюков Д. Ю.* Обеспечение устойчивости информационно-телекоммуникационных сетей в условиях информационного противоборства. СПб.: ЛО ЦНИИС, 2014. 126 с.

7. *Ефремов М. А.*, *Калуцкий И. В.*, *Таныгин М. О.*, *Фрундин А. Г.* Обзор подходов к определению актуальных угроз информации телекоммуникационным системам и предложения по их совершенствованию // Телекоммуникации, 2017, № 5. С. 27–33.

8. *Добрышин М. М.* Предложение по совершенствованию систем противодействия DDoS-атакам // Телекоммуникации, 2018, № 10. С. 32–38.

9. *Добрышин М.М.* Моделирование процессов деструктивных воздействий на компьютерную сеть связи с применением компьютерной атаки типа «человек посередине» // Телекоммуникации, 2019, № 11. С. 32–36.

10. *Добрышин М. М.* Модель разнородных компьютерных атак, проводимых одновременно на узел компьютерной сети связи // Телекоммуникации, 2019, № 12. С. 31–35.

11. *Саенко И. Б.*, *Лаута О. С.*, *Карпов М. А.*, *Крибель А. М.* Модель угроз ресурсам ИТКС как ключевому активу критически важного объекта инфраструктуры // Электросвязь, 2021, № 1. С. 36–44.

12. *Котенко И. В.*, *Саенко И. Б.*, *Лаута О. С.*, *Крибель А. М.* Метод раннего обнаружения кибератак на основе интеграции фрактального анализа и статистических методов // Первая миля, 2021, № 6. С. 64–71.

13. *Канаев А. К.*, *Опарин Е. В.*, *Сахарова М. А.* Полумарковская модель действий злоумышленника при атаке на систему управления сетью тактовой сетевой синхронизации // Информация и космос, 2020, № 4. С. 46–56.

14. *Шубинский И. Б.* Структурная надежность информационных систем. Методы анализа // Надежность, 2012. 216 с.