УДК 621.39

Моделирование действий злоумышленника при ведении сетевой разведки с использованием инфраструктуры комплексной системы синхронизации и доставки шкалы времени

А. К. Канаев[1], Е. В. Опарин[2], Е. В. Опарина[1]

[1]Петербургский государственный университет путей сообщения Императора Александра I, Российская Федерация, 190031, Санкт-Петербург, Московский пр., 9
[2]ЗАО «Институт телекоммуникаций», Российская Федерация, 194100, Санкт-Петербург, Кантемировская, д. 5, К. 5, лит. М

Для цитирования: *Канаев А. К., Опарин Е. В., Опарина Е. В.* Моделирование действий злоумышленника при ведении сетевой разведки с использованием инфраструктуры комплексной системы синхронизации и доставки шкалы времени // Известия Петербургского университета путей сообщения. — СПб.: ПГУПС, 2025. — Т. 22. — Вып. 1. — С. 263–273. DOI: 10.20295/1815-588X-2025-1-263-273

Аннотация

Цель: Оценка показателей, характеризующих защищенность и уязвимость комплексной системы синхронизации и доставки шкалы времени при организации злоумышленником сетевой разведки с использованием ее инфраструктуры. **Методы:** Сбор, систематизация и анализ научно-технической информации; методы теории сетей и графов, математического моделирования, теории вероятностей. **Результаты:** В статье приведены результаты моделирования действий злоумышленника при организации сетевой разведки в сетях связи с использованием оборудования систем частотно-временного обеспечения, для чего построены полумарковская и имитационная модели действий злоумышленника, в которых отражены все этапы противоборства между организованным злоумышленником и системой информационной безопасности. Сформированные полумарковская и имитационные модели позволяют отразить вероятностно-временные характеристики процессов, отражающих противоборство организованного злоумышленника и системы информационной безопасности, произвести оценку указанных характеристик в зависимости от состава, количества и качества ресурсов, которыми располагает злоумышленник и система информационной безопасности. С помощью построенной полумарковской модели проведена верификация сформированной имитационной модели. **Практическая значимость:** Построенные модели могут быть применены для анализа процесса противоборства систем информационной безопасности и организованных злоумышленников, оценки деятельности злоумышленника и системы информационной безопасности, а также состояния систем частотно-временного обеспечения в зависимости от результатов противоборства. Полученные результаты по итогам моделирования могут быть учтены специалистами систем информационной безопасности при построении, модернизации и проектировании средств защиты систем точного времени и частоты.

Ключевые слова: Телекоммуникационная система, частотно-временное обеспечение, сетевая разведка, полумарковская модель, имитационная модель, атака, злоумышленник.

Введение

Стабильность и устойчивость процесса функционирования телекоммуникационных систем (ТКС) должны обеспечиваться непрерывным поддержанием режима синхронизации оборудования связи. Применение и использование современных телекоммуникационных средств и технологий требует использования как систем тактовой сетевой синхронизации (ТСС), так и систем, позволяющих обеспечить формирование, передачу и доставку сигналов единого времени (СЕВ). Следует отметить, что в настоящее время наблюдается комплексная трансформация инфраструктуры ТКС на новые сетевые технологии, которые характеризуются переходом от технологии коммутации каналов (PDH, SDH) к технологии коммутации пакетов (Ethernet/MPLS/IP), активным внедрением мобильных систем связи следующих поколений (например, 5G и 6G), а также непрерывным ужесточением требований к качественным характеристикам сигналов единого времени и частоты, что влечет за собой и трансформацию подходов к решению задач частотно-временного обеспечения (ЧВО). Дополнительные требования к качеству частотно-временных сигналов возникают в системах технологического назначения, например в сети связи железнодорожного транспорта, к которой предъявляются особые требования по обеспечению надежности, живучести и устойчивости процесса функционирования.

Комплексная система синхронизации и доставки шкалы времени необходима для формирования, хранения, передачи и доставки до целевых потребителей сигналов единого времени и частоты требуемой точности и стабильности, чтобы обеспечить устойчивость процесса функционирования всей телекоммуникационной системы [1–3].

Современные системы формирования, хранения, передачи и доставки сигналов единого времени и частоты представляют собой сложные гетерогенные неоднородные структуры, которые включают в свой состав подсистемы ТСС и СЕВ, обеспечивающие потребителей необходимыми сигналами в сетях как коммутацией каналов, так и в сетях с коммутацией пакетов [1–5].

Комплексная система синхронизации и доставки шкалы времени в структуре ТКС представляет собой взаимоувязанный комплекс, обеспечивающий целостность процесса функционирования всей ТКС. Учитывая данный аспект, комплексная система синхронизации и доставки шкалы времени представляет собой один из первостепенных объектов атаки со стороны организованного злоумышленника. Нарушив процесс функционирования комплексной системы синхронизации и доставки шкалы времени, злоумышленник впоследствии может нарушить процесс функционирований всей ТКС. Начальным этапом действий злоумышленника является сетевая разведка, от успешности проведения которой зависит результативность всей атаки в целом.

В статье приведены разработанные модели действий злоумышленника при ведении сетевой разведки с использованием инфраструктуры комплексной системы синхронизации и доставки шкалы времени, которые включают в себя все ключевые этапы сетевой разведки и перечень при этом деструктивных воздействий [1, 6].

Полумарковская модель действий злоумышленника при организации сетевой разведки с использованием инфраструктуры систем частотно-временного обеспечения

Особым видом атаки в системах частотно-временного обеспечения является сетевая разведка, при которой злоумышленник может использовать результаты атаки, такие как информация о сетевых адресах и местоположениях источников сигналов ЧВО, сетевые задержки сигналов, частота сигналов или время, в которое они отправлены и

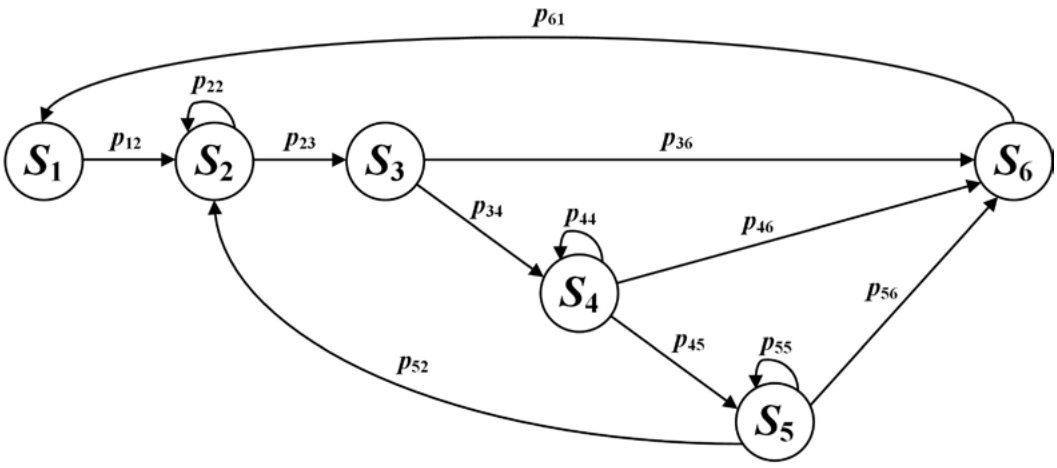

Рис. 1. Модель действий злоумышленника при ведении сетевой разведки в системах частотно-временного обеспечения

приняты. На основе данных сведений злоумышленник может построить топологию сети, идентифицировать узлы, даже если сетевые адреса скрыты или недоступны для просмотра.

Следует отметить, что сетевая разведка в системах частотно-временного обеспечения представляет собой частный случай проведения сетевой разведки в ТКС. Сетевая разведка в системах ЧВО может быть проведена при помощи прослушивания трафика сигналов единого времени и частоты, а также путем отправки вредоносных пакетов и сбора ответов.

Процесс сетевой разведки в комплексной системе синхронизации и доставки шкалы времени содержит следующие этапы:

– организация доступа к системе частотно-временного обеспечения;

– сбор необходимых данных;

– маскировка действий по ведению сетевой разведки.

Примем, что злоумышленник для ведения сетевой разведки в системах ЧВО обладает комплексом сетевой разведки, реализующим процессы сетевого сканирования, чтения информационных потоков, поиска, технического анализа, контроля трафика и местоопределения источников трафика.

Организация доступа при ведении сетевой разведки в комплексной системе синхронизации и доставки шкалы времени является предварительным этапом и включает в себя следующие действия:

– сбор исходных данных о комплексной системе синхронизации и доставки шкалы времени;

– планирование ведения сетевой разведки;

– организация доступа к интересующим сегментам комплексной системы синхронизации и доставки сигналов времени, а также к необходимой информации.

Таким образом, обобщенная модель действий злоумышленника при ведении сетевой разведки примет следующий вид (рис. 1).

Разработанная модель (рис. 1) включает все основные этапы ведения сетевой разведки в системах ЧВО, в том числе сетевое сканирование, чтение сетевых потоков, определение источников трафика ЧВО. Построенная модель (рис. 1) содержит в себе следующие состояния [7–9]:

– S_1 — начальное состояние, при котором злоумышленник проводит сбор исходных данных, подключение комплекса сетевой разведки к целевому сегменту объекта атаки;

– S_2 — сетевое сканирование;

– S_3 — анализ результатов сетевого сканирования и построение злоумышленником топологии системы ЧВО на основе результатов сетевого сканирования;

– S_4 — состояние осуществления чтения информационных потоков протоколов передачи сообщений сигналов единого времени и частоты;

– S_5 — анализ результатов чтения информационных потоков и местоопределение целевых узлов системы ЧВО по сетевым задержкам и содержимому сообщений сигналов единого времени и частоты;

– S_6 — состояние обобщения полученной информации для проведения более сложных и разрушительных атак.

Оценку стационарных характеристик процесса сетевой разведки, таких как вероятность нахождения в каждом состоянии и среднее время атаки, можно произвести с использованием аппарата полумарковских процессов, исходными данными при этом выступают переходные вероятности и функции распределения условных случайных времен пребывания в каждом состоянии [7–9].

Стационарная вероятность пребывания в конкретном состоянии сетевой разведки можно определить по выражению (1) [9–12]:

$$\pi_i = \frac{P_i T_i}{\sum\limits_{j \in S} P_j T_j}, \tag{1}$$

где P_i, P_j — стационарная вероятность пребывания вложенной однородной марковской цепи в соответствующих состояниях;

T_i, T_j — математические ожидания времени пребывания в конкретном состоянии сетевой разведки;

S — число состояний.

Среднее времени проведения сетевой разведки можно оценить при помощи метода миноров, используя выражения (2) и (3) [9]:

$$P_i = \frac{D_i}{\sum\limits_{j=1}^{n} D_j}, \tag{2}$$

где $D_i(D_j)$ — соответствующий минор, образуемый при обработке строк и столбцов матрицы D.

$$D = \begin{pmatrix} 1-p_{11} & -p_{12} & \dots & -p_{17} \\ -p_{21} & 1-p_{22} & \dots & -p_{27} \\ \dots & \dots & \dots & \dots \\ -p_{71} & -p_{72} & \dots & 1-p_{77} \end{pmatrix}. \tag{3}$$

Таким образом, среднее время сетевой разведки можно оценить по формуле (4) [9, 13–15]:

$$T_A = \frac{\sum\limits_{i \in S_A} P_i T_i}{\sum\limits_{i \in S_+} P_i \sum\limits_{j \in \overline{S_A}} p_{ij}}, \tag{4}$$

где S_+ — множество пограничных состояний.

Для проведения моделирования в качестве исходных данных примем матрицу переходных вероятностей (5):

$$\Pi = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0{,}1 & 0{,}9 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0{,}9 & 0 & 0{,}1 \\ 0 & 0 & 0 & 0{,}1 & 0{,}2 & 0{,}7 \\ 0 & 0{,}1 & 0 & 0 & 0{,}1 & 0{,}8 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{5}$$

Дополнительно примем, что функции распределения условных случайных времен пребывания в каждом состоянии сетевой разведки $F_{ij}(t)$ распределены по экспоненциальному закону согласно матрице интенсивностей (6):

$$A = \begin{pmatrix} 0 & 0{,}005 & 0 & 0 & 0 & 0 \\ 0 & 0{,}2 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0{,}05 & 0 & 4 \\ 0 & 0 & 0 & 0{,}05 & 0{,}1 & 4 \\ 0 & 0{,}2 & 0 & 0 & 0{,}1 & 4 \\ 0{,}02 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \text{ч}^{-1}. \tag{6}$$

Путем проведения вычислений получены следующие вероятности нахождения в состояниях процесса сетевой разведки в случайный момент времени (7):

$$\pi_i = (0,729 \;\; 0,004 \;\; 0,067 \;\; 0,016 \;\; 0,001 \; 0,182\;). \quad (7)$$

Среднее время сетевой разведки составляет (8):

$$T_A = \frac{\sum\limits_{i \in S_A} P_i T_i}{\sum\limits_{i \in S_+} P_i \sum\limits_{i \in \overline{S}_A} p_{ij}} = \frac{\left(P_1T_1 + P_2T_2 + P_3T_3 + P_4T_4 + P_5T_5\right)}{\left(P_3p_{36} + P_4p_{46} + P_5p_{56}\right)} = 224,17\text{ч} \approx 9,34\text{ сут}. \quad (8)$$

Злоумышленник будет способен проводить сетевую разведку в комплексной системе синхронизации и доставки шкалы времени в течение 9,34 суток. Следует заметить, что в указанное время входит как активный процесс сетевой разведки путем прослушивания, отправки запросов и получения ответов, так и предварительный сбор исходных данных, а также настройка комплекса сетевой разведки.

Построенная модель позволяет произвести оценку влияния интенсивности действий злоумышленника на среднее время сетевой разведки. Интенсивность действий злоумышленника определяется его технической оснащенностью и уровнем подготовки. При большем количестве ресурсов и технической оснащенности злоумышленника атаки становятся более интенсивными, что влечет снижение времени прохождения конкретного рубежа защиты [13–15].

Зависимости, отражающие оценку влияния интенсивности действий злоумышленника на среднее время сетевой разведки, приведены на рис. 2–5.

Кроме того, следует отметить, что переходные вероятности в разработанной модели характеризуют стратегию атаки злоумышленника, а также соотношение сил и ресурсов злоумышленника и систем информационной безопасности.

Например, в состоянии S_2 злоумышленник может провести дополнительное сканирование узлов, а может перейти к следующему этапу по формализации полученных данных для составления сетевой архитектуры. Аналогичным образом в смежных состояниях злоумышленник может

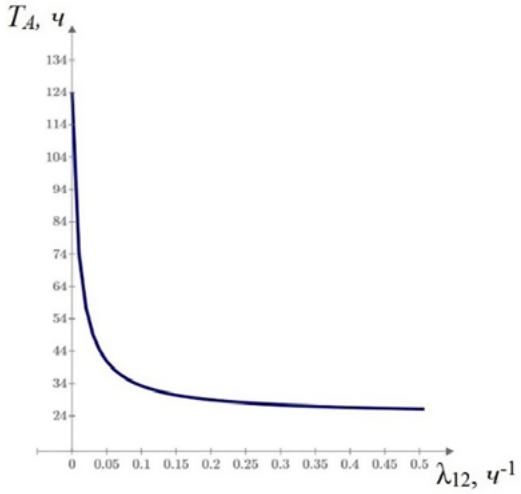

Рис. 2. Зависимость времени сетевой разведки T_A от интенсивности λ_{12}

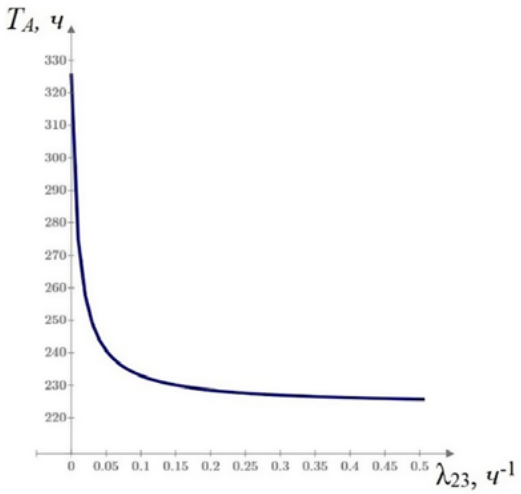

Рис. 3. Зависимость времени сетевой разведки T_A от интенсивности λ_{23}

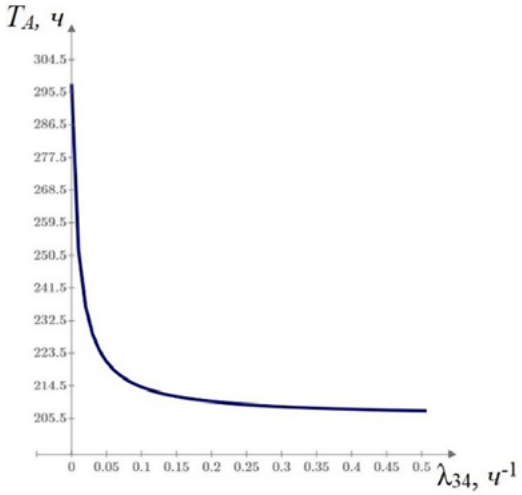

Рис. 4. Зависимость времени сетевой разведки T_A от интенсивности λ_{34}

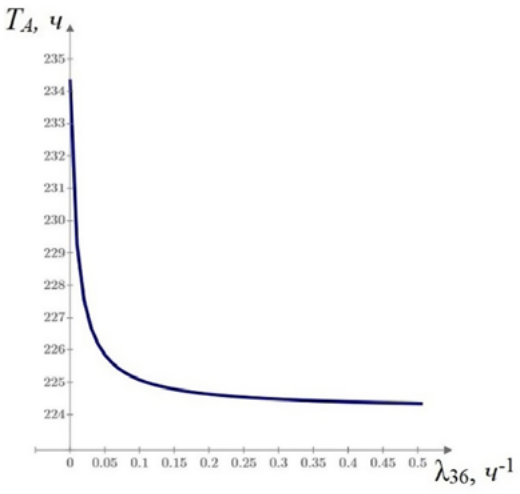

Рис. 5. Зависимость времени сетевой разведки T_A от интенсивности λ_{36}

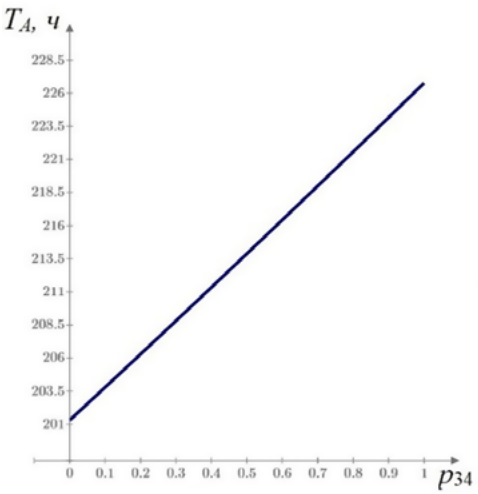

Рис. 6. Зависимость времени сетевой разведки T_A от значения переходной вероятности p_{34}

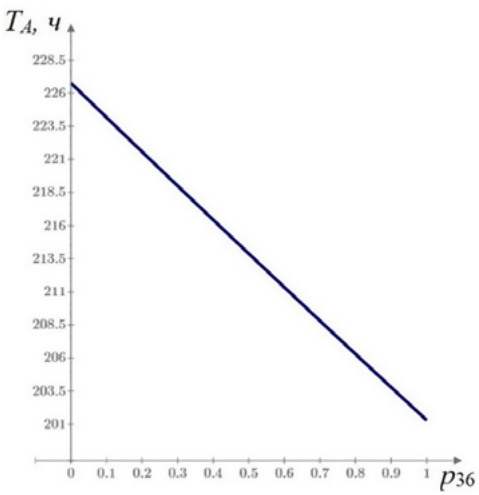

Рис. 7. Зависимость времени сетевой разведки T_A от значения переходной вероятности p_{36}

действовать различным образом, исходя из конкретной ситуации по ведению сетевой разведки.

Разработанная полумарковская модель позволяет произвести оценку стационарных характеристик процесса проведения сетевой разведки в зависимости от значений переходных вероятностей, а значит, от выбранных стратегий противоборства злоумышленника и системы информационной безопасности. На рис. 6, 7 приведены зависимости времени сетевой разведки от значений вероятностей переходов p_{34} и p_{36}.

Анализ полученных результатов показывает, что с ростом интенсивности действий злоумышленника снижается время проведения сетевой разведки, однако существует определенный предел, при котором рост интенсивности действий злоумышленника не приносит ему ожидаемых результатов. Кроме того, разработанная полумарковская модель позволяет проводить оценку стационарных характеристик сетевой разведки от интенсивности, стратегии и технической оснащенности действий злоумышленника и служб

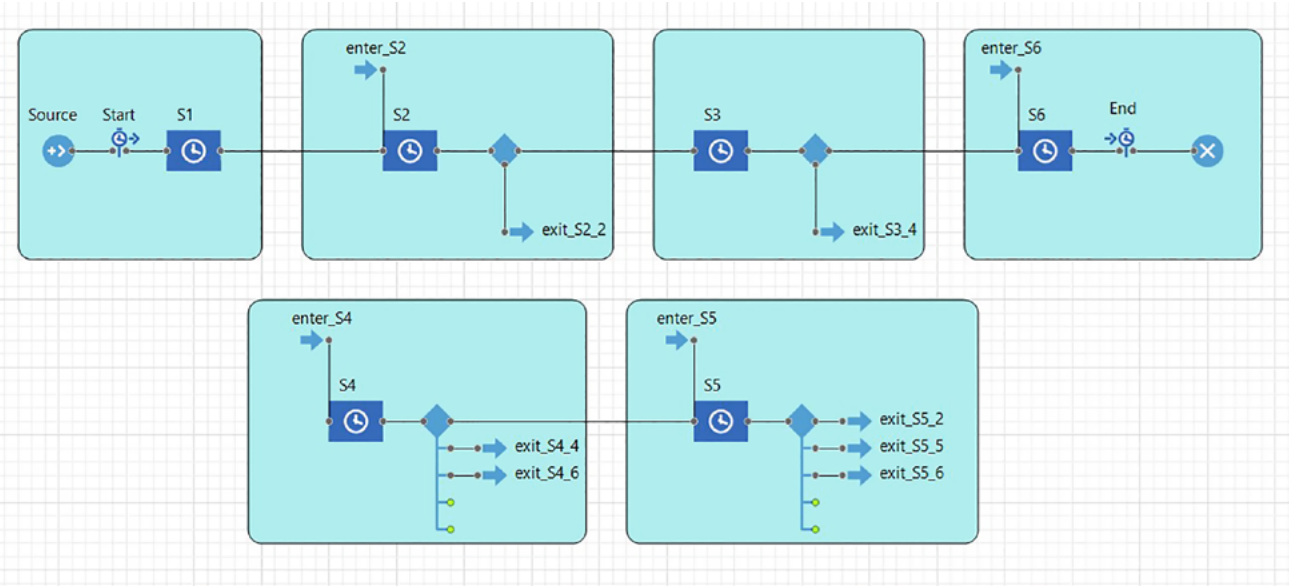

Рис. 8. Имитационная модель процесса проведения сетевой разведки организованным злоумышленником в системах частотно-временного обеспечения

информационной безопасности. Также следует отметить, что получаемые результаты могут быть основой при проведении модернизации средств защиты систем частотно-временного обеспечения.

Имитационная модель действий злоумышленника при ведении сетевой разведки с использованием инфраструктуры систем частотно-временного обеспечения

Аппарат полумарковских процессов сложен с точки зрения увеличения числа исходных данных и перечня состояний, поэтому с целью применения большего набора исходных данных была разработана имитационная модель действий злоумышленника при ведении сетевой разведки в системах ЧВО. Имитационная модель построена в среде *AnyLogic* (рис. 8).

С помощью построенной полумарковской модели была проведена верификация имитационной модели. Исходные данные для верификации соответствуют исходным данным согласно расчетам по разработанной полумарковской модели. В результате проведенного имитационного моделирования получена следующая гистограмма времени реализации сетевой разведки (рис. 9).

Результаты имитационного моделирования: среднее время реализации атаки составляет 220 часов, что составляет примерно 9,17 суток. Как видно, результаты имитационного моделирования в целом соответствуют расчетам согласно разработанной полумарковской модели.

Таким образом, с помощью полумарковской модели проведена верификация имитационной модели процесса проведения сетевой разведки в комплексной системе синхронизации и доставки шкалы времени. Дальнейшее использование имитационной модели позволит расширить объем вычислений, перечень используемых вероятностных распределений и перечень состояний процесса проведения атаки.

Заключение

Возрастание потребности в частотно-временных сигналах в современных и перспективных сетях связи, активное применение и рас-

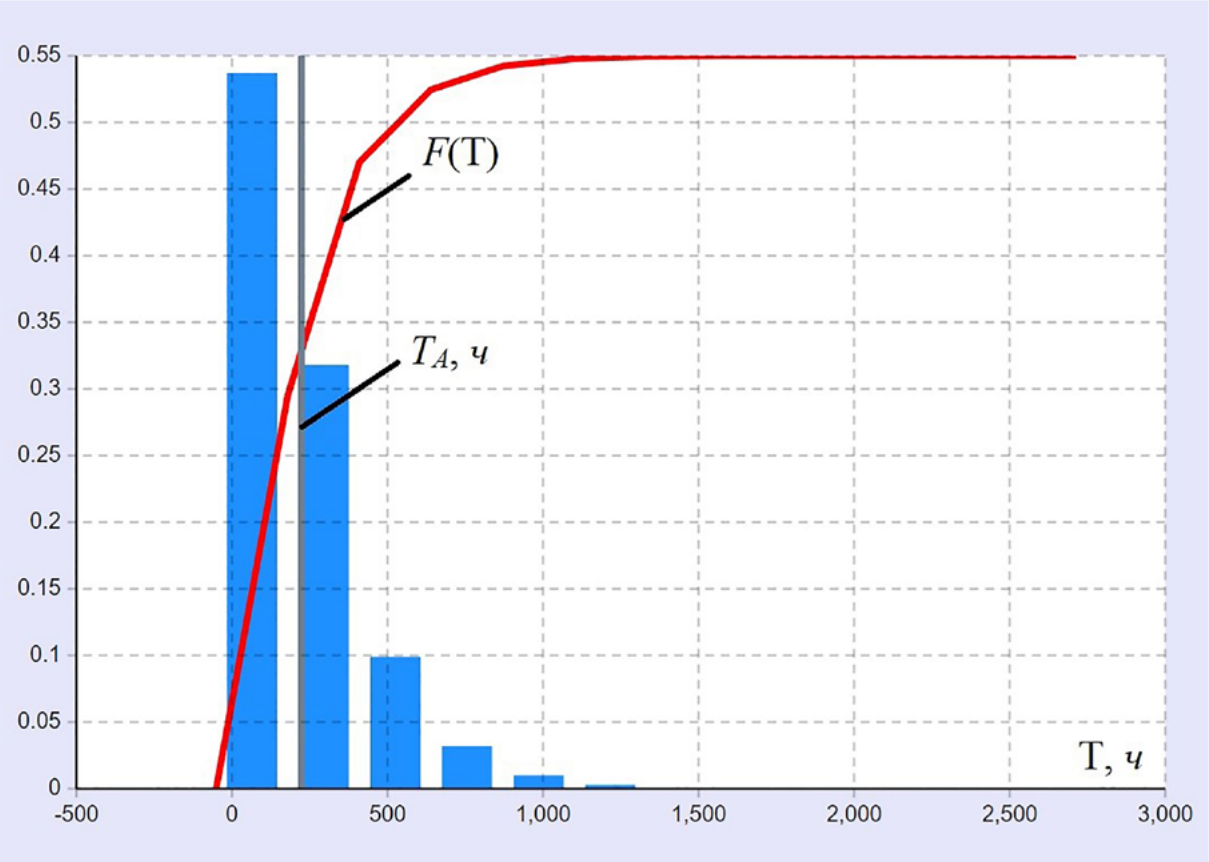

Рис. 9. Гистограмма времени реализации сетевой разведки организованным злоумышленником в системах частотно-временного обеспечения

пространение аппаратуры частотно-временного обеспечения влечет за собой поэтапное возрастание угроз и потенциальных атак на комплексную систему синхронизации и доставки шкалы времени. Одной из наиболее опасных атак на системы частотно-временного обеспечения является сетевая разведка, реализация которой возможна в сетях связи, построенных на различных сетевых технологиях и с применением различных систем передачи. Для оценки деятельности злоумышленника при ведении сетевой разведки в системах ЧВО разработаны соответствующие полумарковская и имитационная модели. С помощью полумарковской модели была верифицирована имитационная модель.

Построенные модели универсальны и позволяют производить оценку действий злоумышленника на всех этапах сетевой разведки. Разработанные полумарковская и имитационная модели информационных воздействий отличаются учетом качественного и количественного состава ресурсов противоборствующих сторон в процессе реализации атаки, которые выражаются через интенсивности и вероятности переходов между состояниями.

Полученные при моделировании результаты могут быть учтены при построении систем информационной безопасности комплексной системы синхронизации и доставки шкалы времени.

Список источников

1. Рыжков А. В. Частотно-временное обеспечение в сетях электросвязи: учебное пособие для вузов / А. В. Рыжков. — М.: Горячая линия — Телеком, 2021. — 270 с.

2. Ванчиков А. С. Синхронизация в современных сетях операторского класса / А. С. Ванчиков // Автоматика, связь, информатика. — 2018. — № 8. — С. 19–20.

3. Канаев А. К. Рекомендации МСЭ-Т в области синхронизации инфотелекоммуникационных систем / А. К. Канаев, А. К. Тощев // Автоматика, связь, информатика. — 2018. — № 10. — С. 8–14.

4. Рыжков А. В. Средства и способы обеспечения единого точного времени / А. В. Рыжков, Е. О. Новожилов // Автоматика, связь, информатика. — 2018. — № 12. — С. 7–11.

5. Мазуренко Д. К. Аспекты построения системы частотно-временной сетевой синхронизации сигналов / Д. К. Мазуренко // T-Comm — Телекоммуникации и Транспорт. — 2017. — Т. 11. — № 8. — С. 4–8.

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

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

8. Канаев А. К. Обеспечение информационной безопасности системы тактовой сетевой синхронизации на основе ее энтропийного анализа / А. К. Канаев, Е. В. Опарин, Е. В. Опарина // Известия Петербургского университета путей сообщения. — 2022. — Т. 19. — № 3. — С. 505–514.

9. Шубинский И. Б. Структурная надежность информационных систем. Методы анализа / И. Б. Шубинский. — Ульяновск: Областная типография «Печатный двор», 2012. — 216 с.

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

11. Смирнов Р. А. Анализ методик оценки угроз безопасности информации / Р. А. Смирнов, С. Н. Новиков // Телекоммуникации. — 2023. — № 7. — С. 24–27.

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

13. Котенко И. В. Метод раннего обнаружения кибератак на основе интеграции фрактального анализа и статистических методов / И. В. Котенко, И. Б. Саенко, О. С. Лаута и др. // Первая миля. — 2021. — № 6. — С. 64–71.

14. Саенко И. Б. Модели компьютерных атак на программно-конфигурируемые сети / И. Б. Саенко, И. В. Котенко, О. С. Лаута и др. // Наукоемкие технологии в космических исследованиях Земли. — 2023. — Т. 15. — № 1. — С. 37–47.

15. Коцыняк М. А. Обеспечение устойчивости информационно-телекоммуникационных сетей в условиях информационного противоборства / М. А. Коцыняк, А. И. Осадчий, М. М. Коцыняк и др. — СПб.: ЛО ЦНИИС, 2014. — 126 с.

Дата поступления: 20.12.2024
Решение о публикации: 19.02.2025

Контактная информация:
КАНАЕВ Андрей Константинович — д-р техн. наук, проф.
ОПАРИН Евгений Валерьевич — канд. техн. наук, ведущий специалист; onapuh@mail.ru
ОПАРИНА Екатерина Владимировна — канд. техн. наук, доц.

Modelling Attacker Network Reconnaissance Using the Environment of an Integrated Time Scale Synchronization and Delivery System

A. K. Kanaev[1], E. V. Oparin[2], E. V. Oparina[1]

[1]Emperor Alexander I St. Petersburg State Transport University, 9, Moskovsky pr., Saint Petersburg, 190031, Russian Federation
[2]JSC "Institute of Telecommunications", 5, K. 5, lit. M, Kantemirovskaya, Saint Petersburg, 194100, Russian Federation

For citation: Kanaev A. K., Oparin E. V., Oparina E. V. Modelling Attacker Network Reconnaissance Using the Environment of an Integrated Time Scale Synchronization and Delivery System // *Proceedings of Petersburg State Transport University*, 2025, vol. 22, iss. 1, pp. 263–273. (In Russian) DOI: 10.20295/22 23-9987-2025-1-263-273

Summary

Purpose: To assess the security and vulnerability techniques for a complex system of time scale synchronization and delivery in case of attacker network reconnaissance in the net environment. **Methods:** Collection, systematization and analysis of scientific and technical information; methods of network and graph theory, mathematical modelling, and probability theory. **Results:** This paper presents the results of modelling attacker actions during network reconnaissance in communication networks using time-frequency support systems. A semi-Markov and simulation models of attacker behaviour were built reflecting all phases of the confrontation between an organised attacker and an information security system. The semi-Markov and simulation models make it possible to illustrate probability and time characteristics of processes reflecting the confrontation between an organized attacker and an information security system as well as to evaluate these characteristics depending on the content, quantity and quality of the resources available to the attacker and the information security system. The verification of the generated simulation model was carried out using the constructed semi-Markov model. **Practical significance:** The constructed models can be used to analyze the process of confrontation between information security systems and organized intruders, to assess attacker activities and those of the information security system, as well as to evaluate the time-frequency support systems judging by the results of the confrontation. The simulation results obtained can be used by information security specialists in building, modernizing, and designing security tools for time and frequency reference systems.

Keywords: Telecommunication system, time-frequency support, network reconnaissance, semi-Markov model, simulation model, attack, attacker.

References

1. Ryzhkov A. V. *Chastotno-vremennoe obespechenie v setyakh elektrosvyazi: uchebnoe posobie dlya vuzov* [Frequency-time support in telecommunication networks: a textbook for universities]. Moscow: Goryachaya liniya — Telekom Publ., 2021, 270 p. (In Russian)

2. Vanchikov A. S. Sinkhronizatsiya v sovremennykh setyakh operatorskogo klassa [Synchronization in modern carrier-class networks]. *Avtomatika, svyaz', informatika* [Automation, communication, informatics]. 2018, Iss. 8, pp. 19–20. (In Russian)

3. Kanaev A. K., Toshchev A. K. Rekomendatsii MSE-T v oblasti sinkhronizatsii infotelekommunikatsionnykh sistem [ITU-T Recommendations in the field of synchronization of infotelecommunication systems]. *Avtomatika, svyaz', informatika* [Automation, communication, informatics]. 2018, Iss. 10, pp. 8–14. (In Russian)

4. Ryzhkov A. V., Novozhilov E. O. Sredstva i sposoby obespecheniya edinogo tochnogo [Means and methods for ensuring a single exact time]. *Avtomatika, svyaz', informatika* [Automation, communications, informatics]. 2018, Iss. 12, pp. 7–11. (In Russian)

5. Mazurenko D. K. Aspekty postroeniya sistemy chastotno-vremennoy setevoy sinkhronizatsii signalov [Aspects of constructing a system of frequency-time network synchronization of signals]. *T-Comm — Telekommunikatsii i Transport* [T-Comm — Telecommunications and Transport]. 2017, vol. 11, Iss. 8, pp. 4–8. (In Russian)

6. Dobryshin M. M. Predlozhenie po sovershenstvovaniyu sistem protivodeystviya DDoS-atakam [Proposal for improving systems for countering DDoS attacks]. *Telekommunikatsii* [Telecommunications]. 2018, Iss. 10, pp. 32–38. (In Russian)

7. Kanaev A. K., Oparin E. V., Sakharova M. A. Polumarkovskaya model' deystviy zloumyshlennika pri atake na sistemu upravleniya set'yu taktovoy setevoy sinkhronizatsii [Semi-Markov model of an intruder's actions in an attack on a network clock synchronization control system]. *Informatsiya i kosmos* [Information and Space]. 2020, Iss. 4, pp. 46–56. (In Russian)

8. Kanaev A. K., Oparin E. V., Oparina E. V. Obespechenie informatsionnoy bezopasnosti sistemy taktovoy setevoy sinkhronizatsii na osnove ee entropiynogo analiza [Ensuring information security of a network clock synchronization system based on its entropy analysis]. *Izvestiya Peterburgskogo universiteta putey soobshcheniya* [Proceedings of Petersburg Transport University]. 2022, vol. 19, Iss. 3, pp. 505–514. (In Russian)

9. Shubinskiy I. B. *Strukturnaya nadezhnost' informatsionnykh sistem. Metody analiza* [Structural reliability of information systems. Analysis methods]. Ul'yanovsk: Oblastnaya tipografiya "Pechatnyy dvor" Publ., 2012, 216 p. (In Russian)

10. Efremov M. A., Kalutskiy I. V., Tanygin M. O. Obzor podkhodov k opredeleniyu aktual'nykh ugroz informatsii telekommunikatsionnym sistemam i predlozheniya po ikh sovershenstvovaniyu [Review of approaches to identifying current threats to information in telecommunication systems and proposals for their improvement]. *Telekommunikatsii* [Telecommunications]. 2017, Iss. 5, pp. 27–33. (In Russian)

11. Smirnov R. A., Novikov S. N. Analiz metodik otsenki ugroz bezopasnosti informatsii [Analysis of methods for assessing information security threats]. *Telekommunikatsii* [Telecommunications]. 2023, Iss. 7, pp. 24–27. (In Russian)

12. Saenko I. B., Lauta O. S., Karpov M. A. et al. Model' ugroz resursam ITKS kak klyuchevomu aktivu kriticheski vazhnogo ob"ekta infrastruktury [Model of threats to ITCS resources as a key asset of a critical infrastructure facility]. *Elektrosvyaz'* [Telecommunications]. 2021, Iss. 1, pp. 36–44. (In Russian)

13. Kotenko I. V., Saenko I. B., Lauta O. S. et al. Metod rannego obnaruzheniya kiberatak na osnove integratsii fraktal'nogo analiza i statisticheskikh metodov [Method of early detection of cyberattacks based on the integration of fractal analysis and statistical methods]. *Pervaya milya* [The first mile]. 2021, Iss. 6, pp. 64–71. (In Russian)

14. Saenko I. B., Kotenko I. V., Lauta O. S. et al. Modeli komp'yuternykh atak na programmno-konfiguriruemye seti [Models of computer attacks on software-defined networks]. *Naukoemkie tekhnologii v kosmicheskikh issledovaniyakh Zemli* [Science-intensive technologies in space research of the Earth]. 2023, vol. 15, Iss. 1, pp. 37–47. (In Russian)

15. Kotsynyak M. A., Osadchiy A. I., Kotsynyak M. M. et al. *Obespechenie ustoychivosti informatsionno-telekommunikatsionnykh setey v usloviyakh informatsionnogo protivoborstva* [Ensuring the stability of information and telecommunication networks in the conditions of information confrontation]. St. Petersburg: LO TsNIIS Publ., 2014, 126 p. (In Russian)

Received: December 20, 2024
Accepted: February 19, 2025

Author's information:
Andrey K. KANAEV — Dr. Sci. in Engineering, Professor
Evgeny V. OPARIN — PhD in Engineering, Leading Specialist; onapuh@mail.ru
Ekaterina V. OPARINA — PhD in Engineering, Associate Professor