

# ОБОБЩЕННАЯ МОДЕЛЬ ДЕЙСТВИЙ ЗЛОУМЫШЛЕННИКА ПРИ МАНИПУЛИРОВАНИИ СООБЩЕНИЯМИ, СОДЕРЖАЩИМИ СИГНАЛЫ ТОЧНОГО ВРЕМЕНИ

DOI: 10.36724/2072-8735-2022-16-6-31-37

**Канаев Андрей Константинович,**  
ФГБОУ ВО ПГУПС, г. Санкт-Петербург, Россия,  
[kanaevak@mail.ru](mailto:kanaevak@mail.ru)

**Manuscript received** 11 May 2022;  
**Accepted** 27 May 2022

**Опарин Евгений Валерьевич,**  
"Гипротранссыгналсвязь – филиал АО Росжелдорпроект",  
г. Санкт-Петербург, Россия, [OparinH@mail.ru](mailto:OparinH@mail.ru)

**Опарина Екатерина Владимировна,**  
ФГБОУ ВО ПГУПС, Санкт-Петербург, Россия,  
[sirayaekaterina@mail.ru](mailto:sirayaekaterina@mail.ru)

**Ключевые слова:** Полумарковская модель, система единого времени, телекоммуникационная система, атака, уязвимость, злоумышленник, манипуляция

В данной статье приводится место и роль системы единого времени в составе телекоммуникационной системы, дан обзор процесса функционирования системы единого времени с указанием основных средств передачи сигналов точного времени. На основе анализа процесса функционирования системы единого времени выделены основные риски возникновения отказов в технологических и автоматизированных системах при нарушении точности передачи сигналов единого времени. В результате анализа возникающих рисков акцентировано внимание на основных типах угроз для системы единого времени при реализации атак со стороны организованных злоумышленников. Особое место среди угроз занимает манипулирование сообщениями, содержащими сигналы точного времени. Для анализа данной угрозы сформирована полумарковская модель действий злоумышленника при манипуляции сообщениями, содержащими сигналы точного времени. Выделены основные этапы процесса проведения атаки. Используя метод миноров производится вычисление основных стационарных характеристик процесса проведения атаки, таких как вероятность нахождения процесса атаки на различных этапах её проведения, а также среднее время длительности атаки и среднее время восстановления системы единого времени от последствий реализации атаки. Данная информация служит также основой для определения коэффициента исправного действия системы единого времени. Полученные результаты могут найти отражение при формировании стратегий защиты системы единого времени от атак организованных злоумышленников.

**Канаев Андрей Константинович**, д.т.н., профессор кафедры "Электрическая связь" ФГБОУ ВО ПГУПС, г. Санкт-Петербург, Россия  
**Опарин Евгений Валерьевич**, к.т.н., инженер I категории "Гипротранссыгналсвязь – филиал АО Росжелдорпроект", г. Санкт-Петербург, Россия  
**Опарина Екатерина Владимировна**, к.т.н., доцент кафедры "Механика и прочность материалов и конструкций" ФГБОУ ВО ПГУПС, г. Санкт-Петербург, Россия

## Для цитирования:

Канаев А.К., Опарин Е.В., Опарина Е.В. Обобщенная модель действий злоумышленника при манипулировании сообщениями, содержащими сигналы точного времени // T-Comm: Телекоммуникации и транспорт. 2022. Том 16. №6. С. 31-37.

## For citation:

Kanaev A.K., Oparin E.V., Oparina E.V. (2022) Generalized model of actions by an attacker when manipulating messages containing precise time signals. *T-Comm*, vol. 16, no. 6, pp. 31-37. (in Russian)

## Введение

Устойчивое функционирование телекоммуникационных систем (ТКС) обеспечивается множеством подсистем, среди которых одной из наиболее важных является система единого времени (СЕВ).

В процессе функционирования ТКС требуется решение ряда задач, таких как документирование времени поступления и выдачи информационных сообщений, анализ проходящих сообщений (очередность, время поступления и выдачи, длительность). На основе данной информации в последующем решаются задачи прогнозирования и принятия управлений решений.

Особенно остро вопросы функционирования СЕВ стоят в территориально-распределенных информационных системах вследствие передачи сигналов точного времени на значительные расстояния [1-3].

В современных и перспективных сетях связи постоянно возрастают число устройств и систем, которые при своем функционировании, а также при подготовке и принятии решений обслуживающим персоналом используют сигналы единого времени.

В случае расхождения или неконтролируемого ухода времени непременно возникают риски отказов во всех технологических системах и автоматизированных системах управления (АСУ). Данные риски могут привести к утрате данных, потере управляемости систем, а также повлиять на безопасность и устойчивость технологических процессов. Наиболее вероятными рисками являются [2, 4, 5]:

1. расхождение времени при работе серверов, а также времени рабочих станций и серверов в информационно-управляющих системах (ИУС);
2. потеря возможности авторизации в системах, а также возможная потеря взаимодействия рабочих узлов с системами, основанными на такой авторизации;
3. возникновение отказов в информационных системах, связанных с нарушением очереди поступления сообщений;
4. отказы в системах протоколирования, анализа и обработки событий, а также в системах мониторинга и администрирования;
5. вероятность восприятия информационно-управляющими системами информации об одном событии, как о двух или более, что в последствии может привести к их некорректной обработке и анализу;
6. восприятие произошедшего состояния в ИУС, как актуального, и, как следствие, возможность формирования управлений решения, не соответствующего текущей ситуации;
7. разрыв при установлении соединений между узлами с последующей потерей информации;
8. возникновение ошибок при формировании отчетов по предоставлению услуг связи и их стоимости;
9. несоблюдение графиков технологических процессов;
10. риск несанкционированного доступа;
11. искажение информации для потребителей услуг связи.

Таким образом, система единого времени является вероятным местом воздействия на телекоммуникационную систему. Злоумышленники таким могут провести значительное число атак, имея намерения разрушить ТКС.

### **1. Процесс функционирования системы единого времени в условиях воздействия организованных злоумышленников**

Для распространения эталонных сигналов единого точного времени Государственная служба времени и частоты может использовать следующие средства [1-4]:

1. глобальные навигационные спутниковые системы (ГНСС);
2. цезиевые, рубидиевые и водородные стандарты;
3. вещательные радиостанции длинно- и коротковолнового диапазона;
4. системы спутниковой связи;
5. средства проводной связи;
6. волоконно-оптические системы передачи (ВОСП);
7. системы синхронной цифровой иерархии (СЦИ) и плезиохронной цифровой иерархии (ПЦИ);
8. коаксиальные линии связи;
9. использование протоколов NTP и PTP в сетях передачи данных (СПД).

Для фиксированных участков телекоммуникационных систем построение системы единого времени реализуется на основе ВОСП. При этом узлы системы единого времени совмещаются с узлами ТКС. Для реализации наибольшей точности сигналов единого времени и экономической целесообразности проектирования систем СЕВ данные системы строятся по иерархическому принципу. Число уровней иерархии, необходимая точность сигналов единого времени на каждом уровне устанавливаются по требованиям пользователей услуг связи.

Рассмотрим основные виды угроз со стороны организованных злоумышленников, характерные для системы СЕВ. Систему СЕВ могут атаковать различные типы злоумышленников, в общем виде классифицируем их на внутренних и внешних. Внутренние злоумышленники могут иметь доступ к доверенному сегменту сети и иметь ключи шифрования или аутентификации при условии, что протокол передачи сигналов точного времени защищен механизмом шифрования или механизмом аутентификации. Внутренний злоумышленник может злонамеренно вмешиваться в легитимный трафик в сети, а также создавать собственный трафик, сделать его легитимным для атаки на узлы системы СЕВ.

Внешние злоумышленники не имеют ключей шифрования и аутентификации, а имеют доступ только к зашифрованному или аутентифицированному передаваемому трафику.

При отсутствии каких-либо механизмов безопасности, в том числе механизмов шифрования и аутентификации, в общем случае нет различия между внутренними и внешними злоумышленниками, так как фактически все атакующие являются внутренними.

Для систем СЕВ характерны следующие виды угроз со стороны организованных злоумышленников [6-8]:

- манипуляция сообщениями, содержащими сигналы точного времени;
- спуфинг в системах СЕВ, при чем спуфинг может подразделяться, на вариант, злоумышленник выдает себя за ведущее устройство и на вариант, когда злоумышленник выдает себя за ведомое или промежуточное устройство;
- угроза атаки повторного воспроизведения сигналов точного времени;

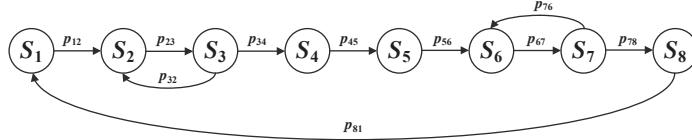
- угроза атаки подмены роли устройств в системе СЕВ;
- перехват и удаление сообщений, содержащих сигналы точного времени;
- манипуляция с задержкой сообщений, содержащих сигналы точного времени;
- DoS-атаки на узлы и сегменты СЕВ, например L2/L3 DoS-атаки;
- DoS-атаки с использованием криптографических процедур;
- DoS-атаки непосредственно против протоколов передачи сигналов точного времени;
- атака на источник сигналов точного времени высокого уровня.
- использование уязвимостей в протоколе передачи сигналов точного времени;
- сетевая разведка.

В данной статье рассматривается модель действий злоумышленника при атаке на систему СЕВ путем манипуляции сообщениями, содержащими сигналы точного времени. Данная атака возникает, когда злоумышленник, используя тактику «человек посередине» получает сообщение протокола передачи сигнала точного времени, изменяет его и передает данное сообщение в пункт назначения. Реализация данной атаки позволяет злоумышленнику нарушить режим передачи сигналов точного времени, что может привести к ситуации, когда протокол передачи сигналов точного времени функционирует, но значительно снижается качество процесса функционирования системы СЕВ [9-10].

Однако некоторые ограничения механизмов безопасности непосредственно самих протоколов передачи сигналов точного времени, при развертывании реальных систем СЕВ данные механизмы дополняются архитектурно-сетевыми механизмами обеспечения безопасности.

## 2. Обобщенная модель действий злоумышленника при реализации атаки манипуляции сообщениями, содержащими сигналы точного времени

Проведенный анализ угрозы манипуляции сообщениями, содержащими сигналы точного времени позволил сформировать следующую полумарковскую модель действий злоумышленника (рис. 1).



**Рис. 1.** Модель действий злоумышленника при реализации атаки манипуляции сообщениями, содержащими сигналы точного времени

На модели (рис. 1) указаны основные этапы атаки реализации атаки путем манипуляции сообщениями единого времени. Данные этапы включают: [4, 11-14]:

$S_1$  – исходное состояние, при котором система СЕВ функционирует согласно нормативным значениям, однако в данном состоянии злоумышленник определяется с целью атаки;

$S_2$  – злоумышленник получает исходные данные о структуре системы СЕВ и свойствах метода передачи сигналов точного времени;

$S_3$  – злоумышленник проводит анализ полученных данных и выбирает сегмент атаки системы СЕВ;

$S_4$  – злоумышленник проводит разрыв соединения в выбранном сегменте атаки;

$S_5$  – злоумышленник проводит подмену в выбранном сегменте системы СЕВ путем обозначения своего узла как легитимного;

$S_6$  – злоумышленник проводит прослушивание передаваемого трафика сигналов точного времени в выбранном сегменте системы СЕВ;

$S_7$  – злоумышленник проводит модификацию содержимого сообщений, содержащих информацию точного времени;

$S_8$  – злоумышленник завершает атаку самостоятельно или под воздействием систем безопасности.

Процесс действий злоумышленника при реализации угрозы манипуляции сообщениями, содержащими сигналы точного времени выглядит следующим образом. Исходным состоянием является состояние  $S_1$ . В данном состоянии система СЕВ обеспечивает сигналами точного времени потребителей в соответствии с заданным качеством, однако в определенный момент она становится целью со стороны организованного злоумышленника, который решил использовать деструктивное воздействие путем манипуляции сигналами точного времени.

В последующем злоумышленник начинает сбор исходных данных о структуре системы СЕВ, методах передачи сигналов, используемых протоколах и оборудовании. Получив достаточное количество информации в состоянии  $S_2$  злоумышленник, учитывая иерархическую структуру построения систем СЕВ, наличие необходимых ресурсов проведения атаки, проводит в состоянии  $S_3$  выбор сегмента атаки. Как правило, сегменты высоких уровней более защищены, но их разрушение может нанести наибольший урон. В то же время сегменты низших уровней могут быть более доступны, однако их повреждение может не принести злоумышленнику желаемого результата.

В дальнейшем в состоянии  $S_4$  злоумышленник проводит разрыв соединения в выбранном сегменте системы СЕВ. Разрыв соединения необходим злоумышленнику с целью внедрения в цепь передачи сообщений сигналов точного времени. Разорвав соединение, злоумышленник, зная структуру системы СЕВ и методы передачи сигналов, в состоянии  $S_5$  легитимизирует свой узел. Узлам верхних уровней он обозначается как нижний, а узлам низших уровней как верхний. Внедрившись в цепь передачи сигналов точного времени, в состоянии  $S_6$  злоумышленник осуществляет прослушивание передаваемого трафика, а в необходимые моменты в состоянии  $S_7$  проводит подмену содержимого сообщений сигналов точного времени.

Указанные действия продолжаются до состояния  $S_8$ , то есть до тех пор, пока злоумышленник не добьется желаемых целей и не завершит атаку самостоятельно, или завершит ее под влиянием служб безопасности. Состояние  $S_8$  представляет собой конечное состояние, когда система СЕВ восстанавливается и очищается от дестабилизирующих воздействий злоумышленника.

### 3. Определение стационарных характеристик процесса, описывающего действия злоумышленника при реализации атаки манипуляции сообщениями, содержащими сигналы точного времени

Основными стационарными характеристиками, определяющими деятельность злоумышленника при реализации атаки являются [15]:

- вероятности нахождения  $\pi_i$  в каждом конкретном состоянии  $S_i$  при реализации атаки;
- среднее время длительности атаки  $T_A$ .

Исходными данными для оценки стационарных характеристик процесса, описывающего действия злоумышленника будут являться [15]:

1. Матрица вероятностей перехода  $P$  согласно разработанной модели (рис. 1) из одного состояния в другое;

2. Матрица функций распределения условных случайных времен пребывания в состояниях  $F_{ij}(t)$ ;

Используя метод миноров вероятность нахождения в каждом из состояний  $S_i$  при проведении атаки определяется по выражению (1) [15]:

$$\pi_i = \frac{P_i T_i}{\sum_{j \in S} P_j T_j} (i, j = 1, \dots, 8; i, j \in S; \sum_{i \in S} \pi_i = 1) \quad (1)$$

где  $P_i$ ,  $P_j$  – стационарная вероятность пребывания однородной вложенной марковской цепи в состоянии  $S_i$  и  $S_j$ ,  $T_i$ ,  $T_j$  – математическое ожидание безусловного времени пребывания в выделенных состояниях.

Для нахождения  $T_i$ ,  $T_j$  пользуемся формулами (2, 3) [15]:

$$T_i = \sum_{j \in S} p_{ij} T_{ij} \quad (2)$$

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

где  $T_{ij}$  – математическое ожидание условного времени нахождения в каждом состоянии.

Для вычисления  $P_i$  используем следующие выражения [15]:

$$P_i = \frac{D_i}{\sum_{j=1}^n D_j} \quad (4)$$

где  $D_i(D_j)$  – минор, определяемый удалением  $i(j)$  столбца и  $i(j)$  строки матрицы  $D$ .

$$D = \begin{pmatrix} 1-p_{11} & -p_{12} & \dots & -p_{1n} & & & & \\ -p_{21} & 1-p_{22} & \dots & -p_{2n} & & & & \\ \dots & \dots & \dots & \dots & & & & \\ -p_{n1} & -p_{n2} & \dots & 1-p_{nn} & & & & \end{pmatrix} \quad (5)$$

Для вычисления среднего времени длительности атаки множество  $S$  разделим на два подмножества: состояния, в которых злоумышленник проводит активные действия  $S_A \subset S$  и состояний, в которых злоумышленник пассивен  $\overline{S_A} \subset S$ . Отметим, что  $S_A \cup \overline{S_A} = S$ .

$S_A$  будут являться состояния  $S_1, S_2, S_3, S_4, S_5, S_6, S_7$ .  $\overline{S_A}$  будет являться состояние  $S_8$ .

Таким образом среднее время длительности атаки и среднее время восстановления работоспособности системы СЕВ можно вычислить по формулам (6, 7) [4, 15]:

$$T_A = \frac{\sum_{i \in S_A} P_i T_i}{\sum_{i \in S_+} P_i \sum_{j \in S_A} p_{ij}} \quad (6)$$

$$T_B = \frac{\sum_{i \in S_A} P_i T_i}{\sum_{i \in S_-} P_i \sum_{j \in S_A} p_{ij}} \quad (7)$$

где  $S_+$  и  $S_-$  – множество граничных состояний перехода.

Множеством состояний  $S_+$  будет состояние  $S_7$ . Множеством состояний  $S_-$  является состояние  $S_8$ .

Проведя данные вычисления, можно определить коэффициент исправного действия  $K_u$  системы СЕВ.

Коэффициент  $K_u$  системы СЕВ определяет устойчивость системы СЕВ, в том числе под воздействием атак организованных злоумышленников [7]. Считаем, что система СЕВ функционирует в состояниях  $S_1, S_2, S_3, S_4, S_5, S_6, S_7$ , хотя и под воздействием организованного злоумышленника, и с пониженными показателями качества. В состоянии  $S_8$  в системе СЕВ проводятся восстановительные и настроочные работы. Исходя из этого  $K_u$  равен (8).

$$K_u = \sum_{i=1, \dots, 7} \pi_i \quad (8)$$

### 4. Расчет численных значений стационарных характеристик процесса, описывающего действия злоумышленника при реализации атаки манипуляции сообщениями, содержащими сигналы точного времени

Проведем оценку стационарных характеристик процесса, описывающего действия злоумышленника при реализации атаки манипуляции сообщениями, содержащими сигналы точного времени. Примем следующую матрицу вероятностей перехода  $P$ :

$$P = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.1 & 0 & 0.9 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0.9 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad (9)$$

В качестве  $F_{ij}(t)$  примем экспоненциальное распределение по данной матрице интенсивностей переходов (10):

$$\Lambda = \begin{pmatrix} 0 & 0.001 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.005 & 0 & 10 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.5 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.5 & 0 & 0.008 \\ 0.05 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad \gamma^{-1} \quad (10)$$

При проведении расчётов на основе метода ( ) предложенного подхода и модели (рис. 1) получены следующие стационарные вероятности нахождения в произвольный момент времени в каждом состоянии (11):

$$\pi_i = (0.841 \quad 4.674 \cdot 10^{-4} \quad 0.019 \quad 2.103 \cdot 10^{-4} \quad 1.683 \cdot 10^{-3} \quad 4.207 \cdot 10^{-4} \quad 0.12 \quad 0.017) \quad (11)$$

Среднее время реализации атаки составит (12):

$$T_A = \frac{\sum P_i T_i}{\sum P_i \sum_{j \in S_A} p_{ij}} = \frac{P_1 T_1 + P_2 T_2 + P_3 T_3 + P_4 T_4 + P_5 T_5 + P_6 T_6 + P_7 T_7}{P_7 p_{78}} = \frac{1.169 \times 10^3 \text{ч}}{P_7 p_{78}} \approx 49 \text{сум.} \quad (12)$$

Среднее время восстановления от последствий атаки составит (13):

$$T_B = \frac{\sum_{i \in S_A} P_i T_i}{\sum_{i \in S_A} P_i \sum_{j \in S_A} p_{ij}} = \frac{P_8 T_8}{P_8 p_{81}} = 20 \text{ ч} \quad (13)$$

Данные значения показывают, что злоумышленник будет осуществлять свои злонамеренные действия в течение 49 суток, по истечении данного времени администраторы безопасности обязаны его обнаружить и приступить к восстановлению нормативного процесса функционирования системы СЕВ. Восстановление системы СЕВ должно быть завершено ориентировочно за 20 часов.

Соответственно коэффициент исправного действия  $K_u$  системы СЕВ примет следующее значение (14):

$$K_u = \sum_{i=1, \dots, 7} \pi_i = 0.983 \quad (14)$$

Коэффициент исправного действия  $K_u$  системы СЕВ имеет хоть и незначительно, но пониженное значение, что вызвано действиями злоумышленника на одном сегменте системы СЕВ. При атаке на нескольких сегментах, коэффициент исправного действия будет еще ниже.

Оценим также влияние интенсивностей действий злоумышленника на разных этапах атаки, а также влияние

указанных интенсивностей на среднее время атаки и время восстановления.

В результате проведенного моделирования были получены следующие результаты (рис. 2-3).

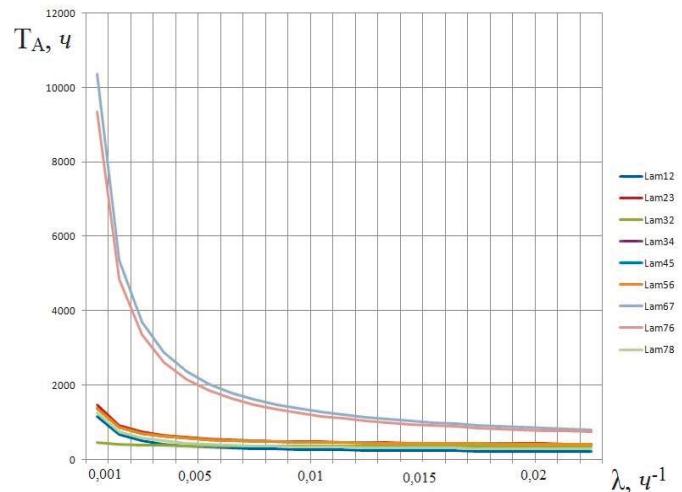


Рис. 2. Зависимость времени процесса реализации атаки от интенсивности деятельности злоумышленника на различных этапах её осуществления

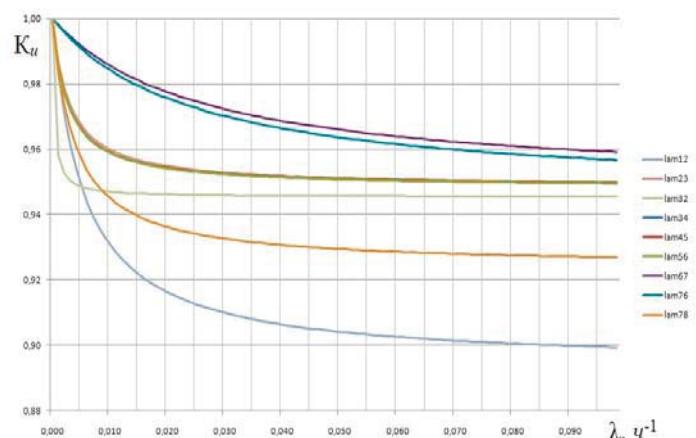


Рис. 3. Зависимость коэффициента исправного действия системы СЕВ от интенсивности деятельности злоумышленника на различных этапах осуществления атаки

В результате можно сделать следующие выводы:

– Рост интенсивностей деятельности злоумышленника снижает коэффициент исправного действия  $K_u$  процесса функционирования системы СЕВ и снижает время осуществления атаки, но до определенного момента, достигнув которого увеличение интенсивности не приносит ощутимых результатов;

– Влияние интенсивности деятельности злоумышленника различно на разных этапах осуществления атаки. Наибольший вклад в снижение времени атаки и снижение коэффициента исправного действия системы СЕВ вносят этапы сбора исходных данных и непосредственной модификации содержания сообщений точного времени. Злоумышленник добьется наибольших результатов, сконцентрировав свои усилия именно на данных этапах.

### Заключение

Система СЕВ является одной из ключевых подсистем ТКС, определяющих качество предоставления услуг связи, а значит одной из наиболее вероятных объектов атаки со стороны организованных злоумышленников. В результате анализа процесса функционирования системы СЕВ в составе ТКС выделены основные риски отказов, способные привести к существенному ущербу. Одной из наиболее вероятных атак на систему СЕВ, способную нанести наибольший ущерб, является манипуляция сообщениями, содержащими сигналы точного времени. В связи с чем в данной статье разработана полумарковская модель действий злоумышленника при реализации данной атаки. В результате проведенного моделирования получены оценки стационарных характеристик процесса ведения атаки: время атаки и коэффициент исправного действия системы СЕВ. Приведены зависимости указанных характеристик от интенсивности действия организованного злоумышленника. Полученные результаты позволяют на основе анализа отдельных средств защиты системы СЕВ, анализа статистики отраженных и завершенных атак, а также определенных методов тестирования оценить показатели защищенности и уязвимости системы СЕВ, а, следовательно, сделать вывод о целесообразности использования или внедрения отдельного вида средств защиты.

Следует отметить, что исходные данные для моделирования можно определить из реальной эксплуатации действующих систем, а также путем проведения контрольных тестирований, что позволит получить модель с реальными свойствами. Полученные результаты можно проанализировать с нормативными требованиями, что позволит сформировать эффективные стратегии защиты от атак организованных злоумышленников.

### Литература

1. Рыжков А.В., Новожилов Е.О. Средства и способы обеспечения единого точного времени // Автоматика, связь, информатика. 2018. №12. С. 7-11.
2. Канаев А.К., Тощев А.К. Рекомендации МСЭ-Т в области синхронизации инфотелекоммуникационных систем // Автоматика, связь, информатика. 2018. №10. С. 8-14.

3. Ванчиков А.С. Синхронизация в современных сетях операторского класса // Автоматика, связь, информатика. 2018. № 8. С. 19-20.
4. Гапанович В.А., Слюняев А.Н. Система единого времени ОАО «РЖД» // Автоматика, связь, информатика. 2018. № 12. С. 2-6.
5. Романов В.Н. Системный анализ для инженеров. СПб.: СЗГЗТУ, 2006. 186 с.
6. 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.
7. Коцыняк М.А., Осадчий А.И., Коцыняк М.М., Ляута О.С., Дементьев В.Е., Васюков Д.Ю. Обеспечение устойчивости информационно-телекоммуникационных сетей в условиях информационного противоборства. СПб.: ЛО ЦНИИС, 2014. 126 с.
8. 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.
9. Добрышин М.М. Предложение по совершенствованию систем противодействия DDoS-атакам // Телекоммуникации. 2018. № 10. С. 32-38.
10. Добрышин М.М. Моделирование процессов деструктивных воздействий на компьютерную сеть связи с применением компьютерной атаки типа «Человек посередине» Телекоммуникации. 2019. № 11. С. 32-36.
11. Добрышин М.М. Модель разнородных компьютерных атак, проводимых одновременно на узел компьютерной сети связи // Телекоммуникации. 2019. № 12. С. 31-35.
12. Саенко И.Б., Ляута 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.
13. Котенко И. В., Саенко И.Б., Ляута О.С., Крибель А.М. Метод раннего обнаружения кибератак на основе интеграции фрактального анализа и статистических методов // Первая миля. 2021. № 6. С. 64-71.
14. Kothenko I, Saenko I., Lauta O., Karpov M. Methodology for management of the protection system of smart power supply networks in the context of cyberattacks // Energies. 2021. Vol. 14(18). DOI:10.3390/en14185963.
15. Шубинский И.Б. Структурная надёжность информационных систем. Методы анализа. Ульяновск: Областная типография «Печатный двор», 2012. 216 с.

## GENERALIZED MODEL OF ACTIONS BY AN ATTACKER WHEN MANIPULATING MESSAGES CONTAINING PRECISE TIME SIGNALS

**Andrey K. Kanaev, FSBEI HE PGUPS, St. Petersburg, Russia, kanaevak@mail.ru**

**Evgeniy V. Oparin, "Giprotranssignalsvyaz – a branch of JSC Roszheldorproekt", St. Petersburg, Russia, OnapuH@mail.ru**

**Ekaterina V. Oparina, FSBEI HE PGUPS, St. Petersburg, Russia, sirayaekaterina@mail.ru**

### **Abstract**

This article gives the place and role of the common time system in the telecommunications system, gives an overview of the process of functioning of the common time system, indicating the main means of transmitting accurate time signals. Based on the analysis of the process of functioning of the common time system, the main risks of failures in technological and automated systems in case of violation of the accuracy of the transmission of common time signals are identified. As a result of the analysis of emerging risks, attention is focused on the main types of threats to the single time system when attacks are carried out by organized malefactors. A special place among the threats is occupied by the manipulation of messages containing precise time signals. To analyze this threat, a semi-Markov model of an attacker's actions when manipulating messages containing precise time signals is formed. The main stages of the process of carrying out the attack are singled out. Using the method of minors, the main stationary characteristics of the attack process are calculated, such as the probability of finding the attack process at various stages of its implementation, as well as the average time of the attack duration and the average recovery time of the unified time system from the consequences of the attack. This information also serves as the basis for determining the coefficient of correct operation of the unified time system. The results obtained can be reflected in the formation of strategies for protecting the unified time system from attacks by organized intruders.

**Keywords:** Semi-Markov model, unified time system, telecommunication system, attack, vulnerability, intruder, manipulation.

### **References**

1. A.V. Ryzhkov, E.O. Novozhilov (2018). Means and methods for ensuring a single exact time. *Automation, communication, informatics*. No. 12, pp. 7-11.
2. A.K. Kanaev, A.K. Toshchev (2018). Recommendations ITU-T in the field of synchronization of infotelecommunication systems. *Automation, communications, informatics*. No. 10, pp. 8-14.
3. A.S. Vanchikov (2018). Synchronization in modern carrier-class networks. *Automation, communication, informatics*. No. 8, pp. 19-20.
4. V.A. Gapanovich, A.N. Slyunyaev (2018). Uniform time system of Russian Railways. *Automation, communication, informatics*. No. 12, pp. 2-6.
5. V.N. Romanov (2006). System analysis for engineers. St. Petersburg: SZGZTU. 186 p.
6. M.A. Efremov, I.V. Kalutsky, M.O. Tanygin, A.G. Frundin (2017). Review of approaches to the definition of actual information threats to telecommunication systems and proposals for their improvement. *Telecommunications*. No. 5, pp. 27-33.
7. M.A. Kotsynyak, A.I. Osadchiy, M.M. Kotsynyak, O.S. Lauta., V.E. Dementiev, D.Yu. Vasukov (2014). Ensuring the stability of information and telecommunication networks in the conditions of information confrontation. St. Petersburg: LO TsNIIS. 126 p.
8. M.A. Efremov, I.V. Kalutsky, M.O. Tanygin, A.G. (2017). Frundin Review of approaches to determining actual information threats to telecommunication systems and proposals for their improvement. *Telecommunications*, pp. 27-33.
9. M.M. Dobryshin (2018). Proposal for improving systems to counter DDoS attacks. *Telecommunications*. No. 10, pp. 32-38.
10. M.M. Dobryshin (2019). Modeling the processes of destructive influences on a computer communication network using a computer attack such as "Man in the middle". *Telecommunications*. No. 11, pp. 32-36.
11. M.M. Dobryshin (2019). Model of heterogeneous computer attacks carried out simultaneously on a node of a computer communication network. *Telecommunications*. No. 12, pp. 31-35.
12. I.B. Saenko, O.S. Lauta, M.A. Karpov, A.M. Kribel (2021). Model of threats to ITC resources as a key asset of a critically important infrastructure object. *Electrosyaz*. No.1, pp. 36-44.
13. I.V. Kotenko, I.B. Saenko, O.S. Lauta, A.M. Kribel. (2021). Method for early detection of cyberattacks based on the integration of fractal analysis and statistical methods. *First mile*. No. 6, pp. 64-71.
14. I. Kothenko, I. Saenko, O. Lauta, M. Karpov (2021). Methodology for management of the protection system of smart power supply networks in the context of cyberattacks. *Energies*. Vol. 14(18). DOI:10.3390/en14185963
15. I. B. Shubinsky (2012). Structural reliability of information systems. Methods of analysis. Ulyanovsk: Regional Printing House "Printing Yard". 216 p.

### **Information about authors:**

**Andrey K. Kanaev**, Doctor of Technical Sciences, Professor of the Department of Electrical Communications, FSBEI HE PGUPS, St. Petersburg, Russia

**Evgeniy V. Oparin**, Ph.D., engineer of the 1st category "Giprotranssignalsvyaz - a branch of JSC Roszheldorproekt", St. Petersburg, Russia

**Ekaterina V. Oparina**, Ph.D., Associate Professor of the Department of Mechanics and Strength of Materials and Structures, FSBEI HE PGUPS, St. Petersburg, Russia