

УДК 621.39

Методика оценки устойчивости комплексной системы синхронизации и доставки шкалы времени, функционирующей в условиях воздействия дестабилизирующих факторов

А. К. Канаев¹, Е. В. Опарин², Е. В. Опарина¹

¹Петербургский государственный университет путей сообщения Императора Александра I, Российская Федерация, 190031, Санкт-Петербург, Московский пр., 9

²ЗАО «Институт телекоммуникаций», Российская Федерация, 194100, Санкт-Петербург, Кантемировская, 5, к. 5, лит. М

Для цитирования: Канаев А. К., Опарин Е. В., Опарина Е. В. Методика оценки устойчивости комплексной системы синхронизации и доставки шкалы времени, функционирующей в условиях воздействия дестабилизирующих факторов // Известия Петербургского университета путей сообщения. — СПб.: ПГУПС, 2025. — Т. 22. — Вып. 3. — С. 790–801. DOI: 10.20295/1815-588X-2025-3-790-801

Аннотация

Цель: Построить методику, позволяющую проводить оценку устойчивости систем частотно-временного обеспечения, подверженных воздействию дестабилизирующих факторов различного характера. **Методы:** Методы системного анализа, положения теории формирования сетей тактовой сетевой синхронизации и систем единого времени, методы анализа надежности, живучести и устойчивости технических систем, а также методы математического моделирования и теории вероятностей. **Результаты:** Построена методика, позволяющая проводить оценку устойчивости систем частотно-временного обеспечения, подверженных воздействию дестабилизирующих факторов, в основе которой лежит оценка показателей надежности и живучести. Построенная методика позволяет отразить качество процесса функционирования систем частотно-временного обеспечения при воздействии различных дестабилизирующих факторов, что в последствии является основой для выработки управленческих решений в условиях дестабилизирующих воздействий. **Теоретическая значимость:** Заключается в расширении области применения теории надежности и живучести систем для оценки устойчивости процесса функционирования сетей электро-связи и систем частотно-временного обеспечения, учитывая при этом тот факт, что устойчивость сетей электро-связи и ее подсистем сложно оценить классическими методами. **Практическая значимость:** Заключается в создании научно обоснованных предложений обеспечения требуемой устойчивости процесса функционирования систем частотно-временного обеспечения в условиях воздействия дестабилизирующих факторов естественного и искусственного характера вследствие отсутствия комплексной проработки вопросов доставки сигналов точного времени и частоты в условиях, отличных от нормативных.

Ключевые слова: Устойчивость, надежность, живучесть, частотно-временное обеспечение, злоумышленник, дестабилизирующий фактор, коэффициент готовности, коэффициент оперативной готовности.

Введение

Устойчивость процесса функционирования современных и перспективных телекоммуникационных систем (ТКС) существенно зависит от системы частотно-временного обеспечения (ЧВО), входящей в ее состав. Современные

тенденции развития ТКС, такие как применение новых сетевых технологий, непрерывный рост абонентов, а также повышение требований к качеству обслуживания, влекут за собой ужесточение требований к процессу функционирования ЧВО.

Современные системы ЧВО включают в свой состав устройства тактовой сетевой синхронизации (ТСС), а также аппаратуру, необходимую для временной или фазовой синхронизации.

Таким образом, при построении современных систем ЧВО актуальна задача построения комплексной системы синхронизации и доставки шкалы времени, концептуальная модель которой приведена на рис. 1.

Эталонным источником сигналов единого времени и частоты для современных и перспективных систем ЧВО является инфраструктура Государственной службы времени, частоты и определения параметров вращения Земли России (ГСВЧ). Ниже по иерархии расположены источники сигналов тактовой сетевой синхронизации и системы единого времени (СЕВ), примеры которых приведены на рис. 1.

Ключевые потребители услуг систем ЧВО в технологических сетях связи также приведены на рис. 1, среди основных потребителей стоит выделить системы электронного документооборота, автоматизированные системы управления, оборудование *IoT (Internet of Things)*, а также дистанционной эксплуатации объектов [1–6].

Процесс функционирования систем ЧВО подвержен воздействию дестабилизирующих факторов различного вида и характера. Нарушение работы систем ЧВО может существенно снизить эффективность функционирования ТКС вплоть до полного прекращения предоставления услуг связи.

1. Влияние дестабилизирующих воздействий на системы частотно-временного обеспечения

Системы частотно-временного обеспечения подвергаются воздействиям дестабилизирующего характера, в результате чего снижается устойчивость как систем ЧВО, так и самих телекоммуникационных систем.

В целом дестабилизирующие факторы можно сгруппировать на дестабилизирующие факторы естественного и искусственного происхождения.

Традиционными воздействиями искусственного происхождения являются действия организованного злоумышленника (рис. 2), среди которых следует выделить:

- манипулирование синхросигналами;
- спуфинг;
- подмену роли устройств в сетях синхронизации и единого времени;
- DoS-атаки различных видов;
- атаки непосредственно против протоколов систем ЧВО [1, 7, 8].

Следует отметить, что отказ или нарушение процесса функционирования отдельных источников сигналов единого времени и частоты может привести к отказам элементов ЧВО, расположенных ниже по иерархии. Принимая во внимание указанный факт, злоумышленники, как правило, пытаются воздействовать на узлы, имеющие самый высокий уровень иерархии.

Проведенный анализ сценариев потенциальных атак на системы ЧВО показал, что наиболее деструктивными являются атаки на систему управления (СУ) ЧВО. Современные системы ЧВО проектируются таким образом, что отказы отдельных их элементов не приводят сразу к отказу всей системы ЧВО. В то же время реализация атаки на СУ ЧВО способно молниеносно привести к приостановлению процесса функционирования всей системы [1, 7, 8].

2. Оценка устойчивости комплексной системы синхронизации и доставки шкалы времени

Учитывая высокое количество внутренних и внешних дестабилизирующих воздействий на элементы системы частотно-временного обеспечения, большую актуальность приобретает задача обеспечения ее устойчивости. В соответ-

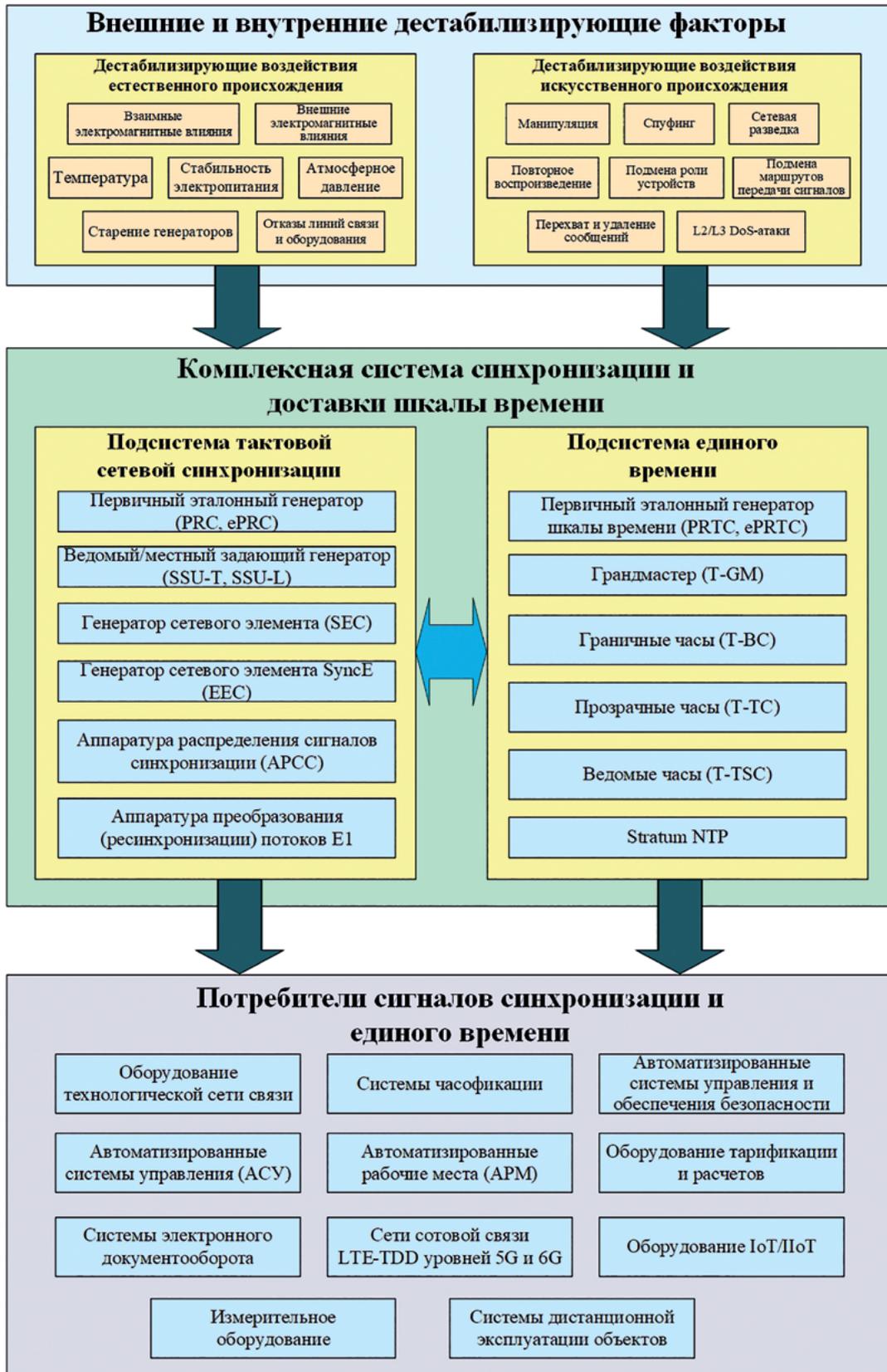


Рис. 1. Модель системы частотно-временного обеспечения, функционирующей в составе распределенной ТКС технологического назначения



Рис. 2. Модель информационного воздействия организованного злоумышленника на комплексную систему синхронизации и доставки шкалы времени

ствии с ГОСТ Р 53111—2008 устойчивость комплексной системы синхронизации и доставки шкалы времени будем представлять как ее способность выполнять функции частотно-временного обеспечения в случае возникновения отказов в результате воздействия дестабилизирующих факторов.

Способность противостоять внутренним дестабилизирующим факторам определяется надежностью системы ЧВО, а способность противостоять внешним дестабилизирующим факторам — живучестью системы ЧВО.

Первоначальный этап оценки устойчивости функционирования систем ЧВО заключается в определении ущерба от дестабилизирующих факторов на основе установленных критериев ущерба. Для систем ТСС в соответствии с утвержденными нормативными документами [1–4] выделяются три категории качества синхронизации:

a, b и *c*. Категория качества *a* соответствует режиму функционирования ТСС с показателями качества, соответствующими нормативным значениям. Категория качества *b* соответствует режиму незначительных отказов. Категория качества *c* недопустима и предназначена для работ по монтажу и перестройке цепей синхронизации.

Требования к процессу функционирования ТСС в соответствии с принятыми категориями качества приведены в табл. 1.

Дополнительно стоит отметить, что в ТКС возможны следующие режимы работы тактовой синхронизации (рис. 3). Основными являются синхронный и псевдосинхронный режимы.

Для систем единого времени при использовании протоколов *NTP* и *PTP* в составе сетей передачи данных (СПД), учитывая тот факт, что метки времени передаются в составе *IP*-пакетов и *Ethernet* кадров, возможно использование сте-

Таблица 1. Требования к процессу функционирования ТСС в соответствии с принятыми категориями качества синхронизации

| Категория качества | Интенсивность проскальзываний | Значение |
|--------------------|---|---|
| <i>a</i> | Не более 5 проскальзываний за 24 часа | Не менее 98,9% времени функционирования |
| <i>b</i> | Более 5 проскальзываний за 24 часа, но не менее 30 проскальзываний за 1 час | Не более 0,1% времени функционирования |
| <i>c</i> | Более 30 проскальзываний за 1 час | Не более 0,1% времени функционирования |

Рассматриваемый период функционирования ТСС не менее одного года

пеней градации ущерба, указанных в ГОСТ Р 53111—2008, а именно [9]:

- высокий (ущерб до 50%);
- средний (ущерб до 30%);
- низкий (ущерб до 10%).

Следует также отметить, что для оценки показателей устойчивости (надежности и живучести) систем связи в настоящее время широкое распространение получил математический аппарат случайных графов и нахождения связности между элементами графа с помощью метода перебора простых цепей (МППЦ). Недостатками указанного метода для рассматриваемой предметной

области является его повышенная трудоемкость, предполагающая рассмотрение всех возможных вариантов из необходимого числа связанных подграфов, что может значительно усложнить расчеты при рассмотрении сложно разветвленных сетей связи, а также отсутствие учета специфики процесса функционирования систем ЧВО.

Учитывая недостатки метода перебора простых цепей, для оценки показателей надежности и живучести систем ЧВО авторами был применен математический аппарат полумарковских процессов. Математические модели процесса функционирования систем ЧВО с применением аппарата полумарковских процессов при наличии и отсутствии дестабилизирующих воздействий представлены авторами в публикациях [10–13]. В основе разработанных моделей лежит построение графов состояний системы ЧВО, которые представляют собой полумарковские процессы функционирования и восстановления систем ЧВО. Процессы функционирования и восстановления систем ЧВО носят вероятностный характер, данные процессы состоят из конечного множества состояний, которые можно охарактеризовать матрицей переходных вероятностей $P = (p_{i,j})$ и совокупностью времен пребывания в каждом конкретном состоянии t_i . Возможность

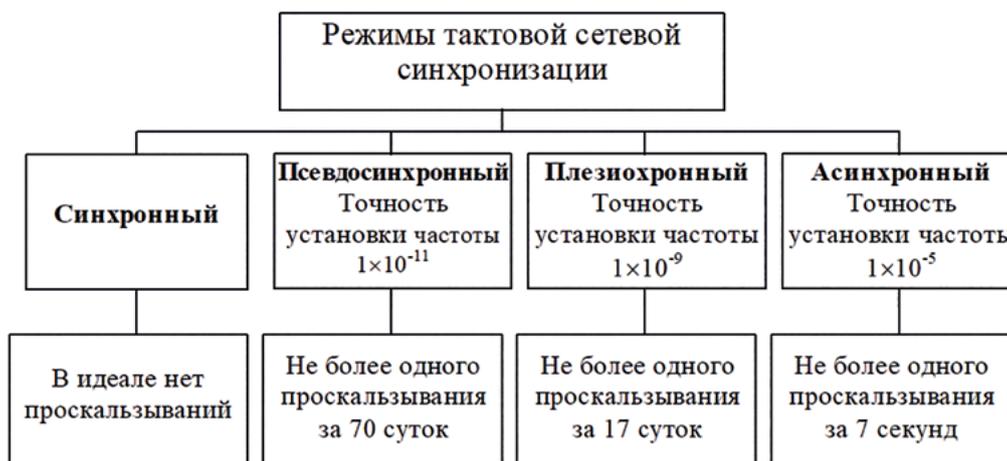


Рис. 3. Режимы работы тактовой сетевой синхронизации

применения аппарата полумарковских процессов обосновывается тем фактом, что имеет место независимость вероятностей перехода из одного состояния S_i в другое S_j от всего предыдущего развития состояний системы ЧВО до попадания в конкретное данное состояние S_p , а также имеет место независимость распределений времен пребывания в состояниях S_i от всего предыдущего развития состояний системы ЧВО [10–13].

В качестве показателя надежности подсетей комплексной системы синхронизации и доставки шкалы времени можно применить коэффициент готовности K_r , определяемый выражением (1) [7–9]:

$$K_r = \frac{T_0}{T_0 + T_b}, \quad (1)$$

где T_0 — среднее время наработки на отказ подсети комплексной системы синхронизации и доставки шкалы времени;

T_b — среднее время восстановления ее процесса функционирования.

В качестве показателя живучести подсети комплексной системы синхронизации и доставки шкалы времени можно применить коэффициент оперативной готовности $K_{o,r}$, определяемый выражением (2) [7–9]:

$$K_{o,r} = P(T) K_r, \quad (2)$$

где K_r — коэффициент готовности;

$P(T)$ — вероятность сохранения работоспособности при воздействии внешних дестабилизирующих факторов.

Таким образом, устойчивость комплексной системы синхронизации и доставки шкалы времени можно оценить следующими показателями: коэффициентом готовности и коэффициентом оперативной готовности.

Для оценки коэффициента готовности K_r комплексной системы синхронизации и доставки

шкалы времени можно использовать модели, разработанные авторами в [10, 14].

Исходными данными для оценки показателей надежности и коэффициента готовности K_r системы ЧВО являются: матрица переходных вероятностей $P = (p_{i,j})$ и матрица функций распределения условных случайных времен пребывания системы ЧВО в каждом из S_i состояний $F_{ij}(t)$. Указанные исходные данные могут быть определены исходя из статистики процесса функционирования систем ЧВО и паспортных данных на применяемое оборудование. В качестве допущения было принято экспоненциальное распределение функций условных случайных времен пребывания системы ЧВО в каждом из S_i состояний $F_{ij}(t)$, а в качестве оборудования систем ЧВО рассматривалось оборудование отечественных производителей, в том числе многофункциональное устройство синхронизации М100 производства ФГУП «ЛО ЦНИИС», аппаратура тактовой сетевой синхронизации «СОНАТА» производства АО НПП «КОМТЕХ», сервер точного времени «ССВ-1Г» производства ООО «КОМСЕТ-сервис».

Для оценки коэффициента оперативной готовности $K_{o,r}$, который характеризует степень противодействия внешним дестабилизирующим факторам, необходимо предварительно выделить воздействующие дестабилизирующие факторы.

Для оценки общей величины $P(T)$ необходимо составить модель воздействия каждого дестабилизирующего фактора и в соответствии с построенной моделью оценить величину $P_i(T)$. Тогда общую величину $P(T)$ можно оценить по следующей формуле (3):

$$P(T) = \prod_{i=1}^n P_i(T), \quad (3)$$

где n — общее число принимаемых во внимание внешних дестабилизирующих факторов.

С целью оценки коэффициента оперативной готовности $K_{o,r}$ рассмотрим модели воздействия

следующих атак: манипулирования, спуфинга, *DoS*-атак и сетевой разведки в комплексной системе синхронизации и доставки шкалы времени. Указанные модели воздействия были рассмотрены авторами в публикациях [11–13, 15].

В основе разработанных авторами моделей информационных воздействий также лежит применение аппарата полумарковских процессов, при котором производится построение графов состояний, отражающих действия злоумышленника на определенном этапе информационных атак. Разработанные модели [11–13, 15] позволяют определить среднее время атаки и среднее время восстановления работоспособности комплексной системы синхронизации и доставки шкалы от последствий реализации атаки, коэффициент исправного действия систем ЧВО, а также вероятность сохранения работоспособности систем ЧВО от интенсивности воздействий организованного злоумышленника и интенсивности действий систем информационного безопасности. В качестве допущения при расчетах также применялось экспоненциальное распределение функций условных случайных времен пребывания системы ЧВО в каждом из S_i состояний $F_{ij}(t)$ при воздействии организованного злоумышленника.

Следует отметить, что разработанные модели информационных воздействий [11–13, 15] отличаются учетом всех основных этапов противоборства организованного злоумышленника и систем информационной безопасности комплексной системы синхронизации и доставки шкалы времени и позволяют оценивать вероятностно-временные характеристики процесса противоборства, а также степень защищенности комплексной системы синхронизации и доставки шкалы времени, причем как совместно, так и для каждого отдельного рубежа защиты систем ЧВО.

Согласно таблице 3 ГОСТ Р 53111—2008 [9], для рассматриваемых систем ЧВО возможно применение также следующих градаций вероятности

сохранения работоспособности элементов систем ЧВО $P(T)$ исходя из причиненного ущерба:

- ущерб до 50 % ($P(T) = 0,5$);
- ущерб до 30 % ($P(T) = 0,7$);
- ущерб до 10 % ($P(T) = 0,9$).

Расчету показателей надежности комплексной системы синхронизации и доставки шкалы времени должен предшествовать этап нормирования технических показателей надежности сети электросвязи, в которой функционирует система ЧВО. Для сетей передачи данных, в которых организовано функционирование протоколов *NTP* и *RTP*, значение коэффициента готовности K_T должно составлять не менее 0,99 [9].

На основании результатов моделирования процесса функционирования и восстановления сети ТСС, рассмотренных авторами в публикациях [10, 14], был вычислен коэффициент готовности комплексной системы синхронизации и доставки шкалы времени ($K_T = 0,998$).

На основе выражения (3) можно вычислить вероятность $P(T)$ при воздействии выделенных внешних дестабилизирующих факторов согласно выражению (4). Отдельные вероятности сохранения работоспособности $P(T)$ при реализации рассматриваемых видов атак были рассмотрены авторами в публикациях [11–13, 15].

$$\begin{aligned} P(T) &= \prod_{i=1}^n P_i(T) = \\ &= K_{\text{и}}^{\text{ман}} \cdot K_{\text{и}}^{\text{спуф}} \cdot K_{\text{и}}^{\text{DoS}} \cdot K_{\text{и}}^{\text{развед}} = \\ &= 0,983 \cdot 0,946 \cdot 0,889 \cdot 1 = 0,827, \end{aligned} \quad (4)$$

где $K_{\text{и}}^{\text{ман}}$ — коэффициент исправного действия системы ЧВО при манипулировании сообщениями, содержащими сигналы частотно-временного обеспечения;

$K_{\text{и}}^{\text{спуф}}$ — коэффициент исправного действия системы ЧВО при реализации атаки спуфинга;

$K_{\text{и}}^{\text{DoS}}$ — коэффициент исправного действия системы ЧВО при реализации *DoS*-атак;

$K_{\text{и}}^{\text{развед}}$ — коэффициент исправного действия системы ЧВО при ведении сетевой разведки, данный коэффициент принят равным единице, при допущении, что при ведении злоумышленником сетевой разведки дестабилизирующих воздействий, нарушающих процесс передачи частотно-временных сигналов, не оказывается.

На основании выражения (4) можно вычислить коэффициент оперативной готовности $K_{\text{о.г}}$ по выражению (5):

$$K_{\text{о.г}} = P(T)K_{\text{г}} = 0,827 \cdot 0,998 = 0,825. \quad (5)$$

В ГОСТ Р 53111—2008 проведено деление потребителей услуг сетей связи на обычных потребителей и спецпотребителей 1-й, 2-й и 3-й категорий, включающих центральные, региональные, местные органы государственного управления, а также органы управления субъектов Российской Федерации. Следует отметить, что разработанная методика оценки устойчивости комплексной системы синхронизации и доставки шкалы времени вполне применима как для обычных потребителей, так и для спецпотребителей.

Учитывая тот факт, что расчет устойчивости комплексной системы синхронизации и доставки шкалы времени проведен для категории обычных потребителей, коэффициент оперативной готовности $K_{\text{о.г}}$ системы ЧВО должен быть не ниже 0,8 для низкого уровня ущерба [9]. В нашем случае $K_{\text{о.г}}$ составляет 0,825, что удовлетворяет указанным в ГОСТ Р 53111—2008 требованиям и соответствует низкому уровню нанесенного ущерба.

Следует также отметить, что для достижения требуемого уровня устойчивости комплексной системы синхронизации и доставки шкалы времени необходима соответствующая система резервирования. Учет системы резервирования выполнен путем включения в разработанную авторами модель процесса функционирования и восстановления системы ЧВО [10, 14] ряда

дополнительных состояний: выбор узла размещения и включение альтернативного первичного источника синхронизации; диагностирование элементов ЧВО встроенными средствами технической диагностики и их восстановление согласно результатам; перестроение ЧВО со структурой, оптимальной по интегральному критерию качества.

Блок-схема разработанной методики оценки устойчивости комплексной системы синхронизации и доставки шкалы времени представлена на рис. 4.

Представленная методика (рис. 4) представляет собой структурированную последовательность действий, включающую в себя предварительное определение критериев уровней ущерба для комплексной системы синхронизации и доставки шкалы времени (блок 1), определение градаций ущерба (блок 2), сбор необходимых исходных данных для построения модели процесса функционирования системы ЧВО (блок 3) и моделей воздействия дестабилизирующих факторов (блок 7), формирования указанных моделей (блоки 4, 5, 8, 9) и вычисления показателей, на основе которых производится оценка устойчивости (блоки 6, 9).

Заключение

Комплексная система синхронизации и доставки шкалы времени является основополагающим элементом ТКС. В данной статье на основе проведенных исследований изложена методика, позволяющая провести оценку ее устойчивости через оценку надежности и живучести. В качестве показателя надежности предложено использование коэффициента готовности $K_{\text{г}}$ комплексной системы синхронизации и доставки шкалы времени, в качестве показателя живучести предложено использование коэффициента оперативной готовности $K_{\text{о.г}}$ комплексной системы синхронизации и доставки шкалы времени.

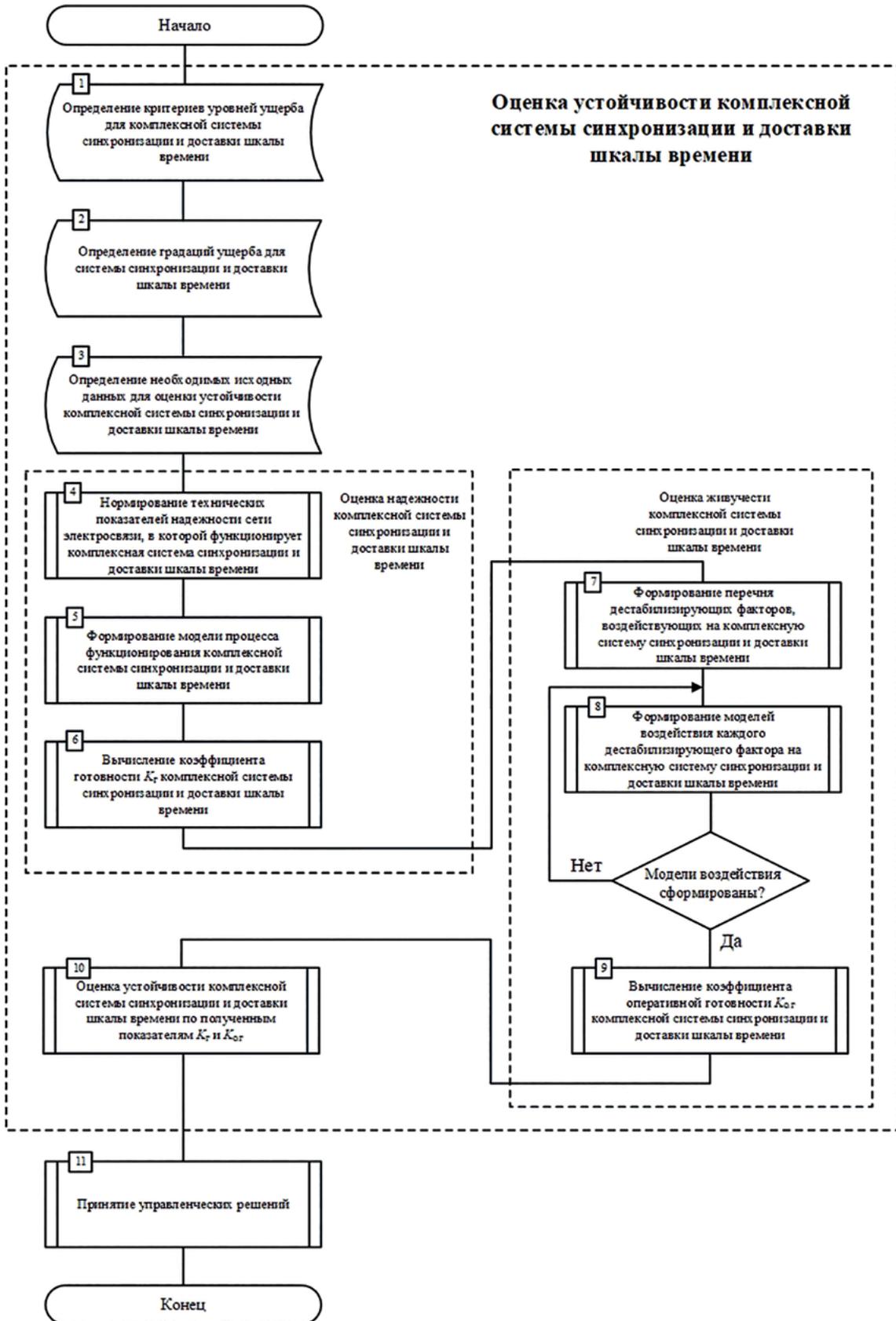


Рис. 4. Блок-схема методики оценки устойчивости комплексной системы синхронизации и доставки шкалы времени

Построенная методика позволяет оценить качество процесса функционирования комплексной системы синхронизации и доставки шкалы времени в условиях воздействия дестабилизирующих факторов, что впоследствии может найти отражение в принятии обоснованных решений по ее управлению.

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. Мазуренко Д. К. Аспекты построения системы частотно-временной сетевой синхронизации сигналов / Д. К. Мазуренко // Т-Comm — Телекоммуникации и Транспорт. — 2017. — Т. 11. — № 8. — С. 4–8.
3. Мазуренко Д. К. Эксплуатация оборудования системы синхронизации сигналов в сетях, построенных на технологии коммутации пакетов и в сетях 5G / Д. К. Мазуренко, Д. А. Пальцин, А. С. Фень // Электро-связь. — 2022. — № 12. — С. 14–17.
4. Рыжков А. В. Частотно-временное обеспечение в сетях электросвязи / А. В. Рыжков, А. Ю. Насонов // Системы синхронизации, формирования и обработки сигналов. — 2019. — Т. 10. — № 1. — С. 49–52.
5. Рыжков А. В. Современные тенденции развития систем сетевой синхронизации в сетях электросвязи. От плезихронных до когерентных сетей / А. В. Рыжков, М. Л. Шварц // Системы синхронизации, формирования и обработки сигналов. — 2021. — Т. 12. — № 4. — С. 27–38.
6. Канаев А. К. Рекомендации МСЭ-Т в области синхронизации инфотелекоммуникационных систем / А. К. Канаев, А. К. Тоцев // Автоматика, связь, информатика. — 2018. — № 10. — С. 8–14.
7. Коцыняк М. А. Обеспечение устойчивости информационно-телекоммуникационных сетей в условиях информационного противоборства / М. А. Коцыняк, А. И. Осадчий, М. М. Коцыняк, О. С. Лаута и др. — СПб.: Типография Военной академии связи имени Маршала Советского Союза С. М. Буденного, 2014. — 126 с.
8. Лаута О. С. Методика повышения устойчивости ИТКС в условиях воздействия противника на основе определения опорного варианта / О. С. Лаута, С. А. Багрецов, Э. А. Бударин, М. В. Митрофанов // Электро-связь. — 2020. — № 9. — С. 64–68.
9. ГОСТ Р 53111—2008. Устойчивость функционирования сети связи общего пользования. Требования и методы проверки.
10. Канаев А. К. Формирование модели процесса функционирования и восстановления сети тактовой сетевой синхронизации в условиях применения автоматизированной системы поддержки принятия решений. Электронный ресурс / А. К. Канаев, Е. В. Опарин, А. К. Тоцев // Бюллетень результатов научных исследований. — 2011. — № 1. — С. 41–55.
11. Канаев А. К. Обобщенная модель действий злоумышленника при манипулировании сообщениями, содержащими сигналы точного времени / А. К. Канаев, Е. В. Опарин, Е. В. Опарина // Т-Comm — Телекоммуникации и Транспорт. — 2022. — Т. 16. — № 6. — С. 31–37.
12. Опарин Е. В. Обобщенная модель действий злоумышленника при реализации DoS-атаки на комплексную систему синхронизации и доставки шкалы времени / Е. В. Опарин // Информация и космос. — 2024. — № 2. — С. 93–101.
13. Канаев А. К. Полумарковская модель деятельности злоумышленника при реализации атаки спуфинга в подсистеме единого времени / А. К. Канаев, Е. В. Опарин, Е. В. Опарина // Ракетно-космическое приборостроение информационные системы. — 2022. — Т. 9. — № 4. — С. 9–16.
14. Канаев А. К. Имитационная модель процесса функционирования и восстановления сети тактовой сетевой синхронизации / А. К. Канаев, Е. В. Опарин, М. А. Сахарова // Информатизация и связь. — 2020. — № 4. — С. 83–90.
15. Канаев А. К. Имитационная модель процесса реализации атаки на систему управления сетью синхронизации / А. К. Канаев, Е. В. Опарин, Е. В. Опарина, М. А. Сахарова // Информация и космос. — 2023. — № 1. — С. 112–118.

Дата поступления: 29.03.2025

Решение о публикации: 18.05.2025

Контактная информация:

КАНАЕВ Андрей Константинович — д-р техн. наук, проф.; kanaevak@mail.ru
ОПАРИН Евгений Валерьевич — канд. техн. наук, доц.; ОпаринH@mail.ru
ОПАРИНА Екатерина Владимировна — канд. техн. наук, доц.; syrayaekaterina@mail.ru

Assessing the Stability of an Integrated Timescale Synchronization and Delivery System Operating Under the Influence of Destabilizing Factors

A. K. Kanaev¹, E. V. Oparin², E. V. Oparina¹

¹Emperor Alexander I Petersburg State Transport University, 9, Moskovsky pr., Saint Petersburg, 190031, Russian Federation

²JSC “Institute of Telecommunications”, 5, bld. 5, lit. M, Kantemirovskaya str., Saint Petersburg, 194100, Russian Federation

For citation: Kanaev A. K., Oparin E. V., Oparina E. V. Assessing the Stability of an Integrated Timescale Synchronization and Delivery System Operating under the Influence of Destabilizing Factors // *Proceedings of Petersburg State Transport University*, 2025, vol. 22, iss. 3, pp. 790–801. (In Russian) DOI: 10.20295/1815-588X-2025-3-790-801

Summary

Purpose: To develop a methodology for assessing the stability of time-frequency support systems exposed to various destabilizing factors. **Methods:** System analysis methods, the theory of network clock synchronization and unified time systems, methods for analyzing reliability, survivability and stability of technical systems, methods of mathematical modelling, and probability theory. **Results:** A methodology has been developed for evaluating the stability of time-frequency support systems exposed to destabilizing factors, based on reliability and survivability assessment. The developed methodology makes it possible to reflect the quality of time-frequency support system functioning under the influence of various destabilizing factors. Subsequently, it will form the basis for managerial decision-making under conditions of destabilizing influences. **Theoretical significance:** This methodology will allow a wide application of the system reliability and survivability theory ensuring the functional stability of telecommunication networks and time-frequency systems, as the stability of telecommunication networks and its subsystems is difficult to assess using traditional methods. **Practical significance:** The scientifically-based proposals mentioned above focus on ensuring the required stability of the functioning of time-frequency support systems under the influence of destabilizing factors, both natural and artificial, due to the lack of comprehensive study of the accurate time and frequency signal delivery outside of regular environments.

Keywords: Stability, reliability, survivability, time-frequency support, attacker, destabilizing factor, readiness coefficient, operational readiness coefficient.

References

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

2. Mazurenko D. K. Aspekty postroeniya sistemy chastotno-vremennoy setevoy sinkhronizatsii signalov [Aspects of building a frequency-time network signal synchronization system]. *T-Comm — Telekommunikatsii i*

Transport [T-Comm — Telecommunications and Transport]. 2017, vol. 11, Iss. 8, pp. 4–8. (In Russian)

3. Mazurenko D. K., Pal'tsin D. A., Fen' A. S. Ekspluatatsiya oborudovaniya sistemy sinkhronizatsii signalov v setyakh, postroennykh na tekhnologii kommutatsii paketov i v setyakh 5G [Operation of signal synchronization system equipment in networks built on packet switching technology and in 5G networks]. *Elektrosvyaz'* [Electrosvyaz]. 2022. Iss. 12, pp. 14–17. (In Russian)

4. Ryzhkov A. V., Nasonov A. Yu. Chastotno-vremennoe obespechenie v setyakh elektrosvyazi [Frequency-time support in telecommunications networks]. *Sistemy sinkhronizatsii, formirovaniya i obrabotki signalov* [Systems of synchronization, formation and processing of signals]. 2019, vol. 10, Iss. 1, pp. 49–52. (In Russian)
5. Ryzhkov A. V., Shvarts M. L. Sovremennye tendentsii razvitiya sistem setevoy sinkhronizatsii v setyakh elektrosvyazi. Ot plizokhronnykh do kogerentnykh setey [Modern trends in the development of network synchronization systems in telecommunications networks. From plesiochronous to coherent networks]. *Sistemy sinkhronizatsii, formirovaniya i obrabotki signalov* [Systems of synchronization, formation and processing of signals]. 2021, vol. 12, Iss. 4, pp. 27–38. (In Russian)
6. Kanaev A. K., Toshchev A. K. Rekomendatsii MSE-T v oblasti sinkhronizatsii infotelekomunikatsionnykh 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)
7. Kotsynyak M. A., Osadchiy A. I., Kotsynyak M. M., Lauta O. S. et al. *Obespechenie ustoychivosti informatsionno-telekomunikatsionnykh setey v usloviyakh informatsionnogo protivoborstva* [Ensuring the stability of information and telecommunication networks in conditions of information confrontation]. Saint Petersburg: Tipografiya Voennoy akademii svyazi imeni Marshala Sovetskogo Soyuz S. M. Budennogo Publ., 2014, 126 p. (In Russian)
8. Lauta O. S., Bagretsov S. A., Budarin E. A., Mitrofanov M. V. Metodika povysheniya ustoychivosti ITKS v usloviyakh vozdeystviya protivnika na osnove opredeleniya opornogo varianta [Methodology for increasing the stability of ITNS under enemy influence based on determining the reference option]. *Elektrosvyaz'* [Electrosvyaz]. 2020. Iss. 9, pp. 64–68. (In Russian)
9. GOST R 53111—2008. *Ustoychivost' funktsionirovaniya seti svyazi obshchego pol'zovaniya. Trebovaniya i metody proverki* [GOST R 53111—2008. Stability of operation of public communication network. Requirements and verification methods]. (In Russian)
10. Kanaev A. K., Oparin E. V., Toshchev A. K. Formirovanie modeli protsessa funktsionirovaniya i vosstanovleniya seti taktovoy setevoy sinkhronizatsii v usloviyakh primeneniya avtomatizirovannoy sistemy podderzhki prinyatiya resheniy Formation of a model of the functioning and recovery process of the clock network synchronization network under conditions of using an automated decision support system [Electronic resource]. *Byulleten' rezultatov nauchnykh issledovaniy* [Bulletin of research results]. 2011. Iss. 1, pp. 41–55. (In Russian)
11. Kanaev A. K., Oparin E. V., Oparina E. V. Obobshchennaya model' deystviy zloupotrebiteleya pri manipulirovaniy soobshcheniyami, sodержashchimi signaly tochnogo vremeni [Generalized model of attacker actions when manipulating messages containing precise time signals]. *T-Comm — Telekommunikatsii i Transport* [T-Comm — Telecommunications and Transport]. 2022, vol. 16, Iss. 6, pp. 31–37. (In Russian)
12. Oparin E. V. Obobshchennaya model' deystviy zloupotrebiteleya pri realizatsii DoS-ataki na kompleksnyuyu sistemu sinkhronizatsii i dostavki shkaly vremeni [Generalized model of attacker actions when implementing a DoS attack on a complex synchronization and time scale delivery system]. *Informatsiya i kosmos* [Information and space]. 2024. Iss. 2, pp. 93–101. (In Russian)
13. Kanaev A. K., Oparin E. V., Oparina E. V. Polumarkovskaya model' deyatel'nosti zloupotrebiteleya pri realizatsii ataki spufinga v podsysteme edinogo vremeni [Semi-Markov model of attacker activity when implementing a spoofing attack in the unified time subsystem]. *Raketno-kosmicheskoe priborostroenie informatsionnye sistemy* [Rocket and space instrumentation information systems]. 2022, vol. 9, Iss. 4, pp. 9–16. (In Russian)
14. Kanaev A. K., Oparin E. V., Sakharova M. A. Imitatsionnaya model' protsessa funktsionirovaniya i vosstanovleniya seti taktovoy setevoy sinkhronizatsii [Simulation model of the functioning and recovery process of the clock network synchronization network]. *Informatizatsiya i svyaz'* [Informatization and communications]. 2020, Iss. 4, pp. 83–90. (In Russian)
15. Kanaev A. K., Oparin E. V., Oparina E. V., Sakharova M. A. Imitatsionnaya model' protsessa realizatsii ataki na sistemu upravleniya set'yu sinkhronizatsii [Simulation model of the process of implementing an attack on a synchronization network control system]. *Informatsiya i kosmos* [Information and space]. 2023. Iss. 1, pp. 112–118. (In Russian)

Received: March 29, 2025

Accepted: May 18, 2025

Author's information:

Andrey K. KANAEV — Dr. Sci. in Engineering,

Professor; kanaevak@mail.ru

Evgeniy V. OPARIN — PhD in Engineering, Associate

Professor; OnapuH@mail.ru

Ekaterina V. OPARINA — PhD in Engineering, Associate

Professor; syrayaekaterina@mail.ru