Подход по выявлению кибератак в комплексной системе синхронизации и доставки шкалы времени с использованием фрактального анализа диагностической информации

А. К. Канаев, Е. В. Опарина

Петербургский государственный университет путей сообщения Императора Александра I

kanaevak@mail.ru, sirayaekaterina@mail.ru

Е. В. Опарин

ЗАО «Институт телекоммуникаций»

onapuh@mail.ru

Аннотация. **Рассмотрен подход по выявлению кибератак в комплексной системе синхронизации и доставки шкалы времени с использованием фрактального анализа диагностической информации на основе оценки показателя Херста и анализа автокорреляционной функции диагностических параметров, с целью повышения устойчивости процесса функционирования систем частотно-временного обеспечения в условиях воздействия дестабилизирующих факторов.**

Ключевые слова: комплексная система синхронизации и доставки шкалы времени, мониторинг, встроенные средства диагностики, показатель Херста

I. Введение

Важным условием обеспечения устойчивости процесса функционирования сетей связи является поддержание режимов синхронизации телекоммуникационного оборудования. Внедрение современных телекоммуникационных технологий требует применения помимо классических систем тактовой сетевой синхронизации также устройств, позволяющих обеспечить передачу сигналов точного времени. Также, в настоящее время наблюдаются изменения инфраструктуры телекоммуникационных систем, которые вызваны переходом на новые сетевые технологии, поэтапным смещением от технологии коммутации каналов к технологии коммутации пакетов, а также постоянно возрастающими требованиями к точности и стабильности сигналов синхронизации и единого времени. Возникновение отказов в системах синхронизации и отклонение характеристик частотно-временных сигналов от требуемых значений способно привести к значительному ухудшению качества передаваемой информации вплоть до полного отказа в предоставлении телекоммуникационных услуг, что особенно критично в технологических сетях связи, таких как технологическая сеть связи ОАО «РЖД», поэтому в настоящее время актуальной является задача создания комплексной системы синхронизации и доставки шкалы времени для крупной распределенной системы технологического назначения, включающей подсистемы тактовой сетевой синхронизации (ТСС) и системы единого времени (СЕВ). Основной задачей комплексной системы синхронизации и доставки шкалы времени будет являться формирование, хранение, передача и доставка до потребителей сигналов синхронизации и единого времени требуемой точности и стабильности, что будет способствовать обеспечению устойчивости процесса функционирования всей телекоммуникационной системы (ТКС) [1–4].

II. Модель процесса функционирования комплексной системы синхронизации и доставки шкалы в условиях воздействий организованного злоумышленника

На основе результатов проведённого системного анализа существующих и перспективных средств формирования, хранения и доставки сигналов синхронизации и единого времени, требований существующих и перспективных потребителей сигналов тактовой сетевой синхронизации и единого времени, а также основных воздействующих дестабилизирующих факторов, разработана модель процесса функционирования комплексной системы синхронизации и доставки шкалы времени в условиях воздействий организованного злоумышленника (рис. 1).

Данная модель (рис. 1) имеет трёхуровневую структуру, на нижнем уровне располагается сеть комплексной системы синхронизации и доставки шкалы времени, включающая все основное оборудование частотно-временной синхронизации. Второй уровень образует система технической эксплуатации (СТЭ), включающая подсистемы контроля, измерений, резервирования, восстановления и ремонта. Третий уровень образует система управления. В совокупности, указанные три уровня образуют комплексную систему синхронизации и доставки шкалы времени [1–4].

В качестве эталонных источников сигналов синхронизации и единого времени для комплексной системы синхронизации и доставки шкалы времени используется инфраструктура Государственной службы времени, частоты и определения параметров вращения Земли России. Далее в соответствии с уровнями иерархии комплексной системы синхронизации и доставки шкалы времени производится подключение объединенных источников ТСС и СЕВ. В качестве оборудования ТСС выступает оборудование первичных эталонных генераторов (ПЭГ), вторичных задающих генераторов (ВЗГ), местных задающих генераторов (МЗГ) и генераторов сетевых элементов, а в качестве оборудования СЕВ в зависимости от типа используемого протокола передачи меток времени выступают сервера

времени соответствующего уровня и узлы, поддерживающие функционирование протоколов. Средствами доставки сигналов комплексной системы синхронизации и доставки шкалы времени являются волоконно-оптические магистральные системы передачи на базе оборудования *SDH*, *DWDM* и *IP*/*MPLS* на уровне первичных и вторичных источников, а также глобальная навигационная спутниковая система ГЛОНАСС, использование сигналов которой повышает надежность и точность комплексной системы синхронизации и доставки шкалы времени, а также предоставляет дополнительные сервисы потребителям [1–4].

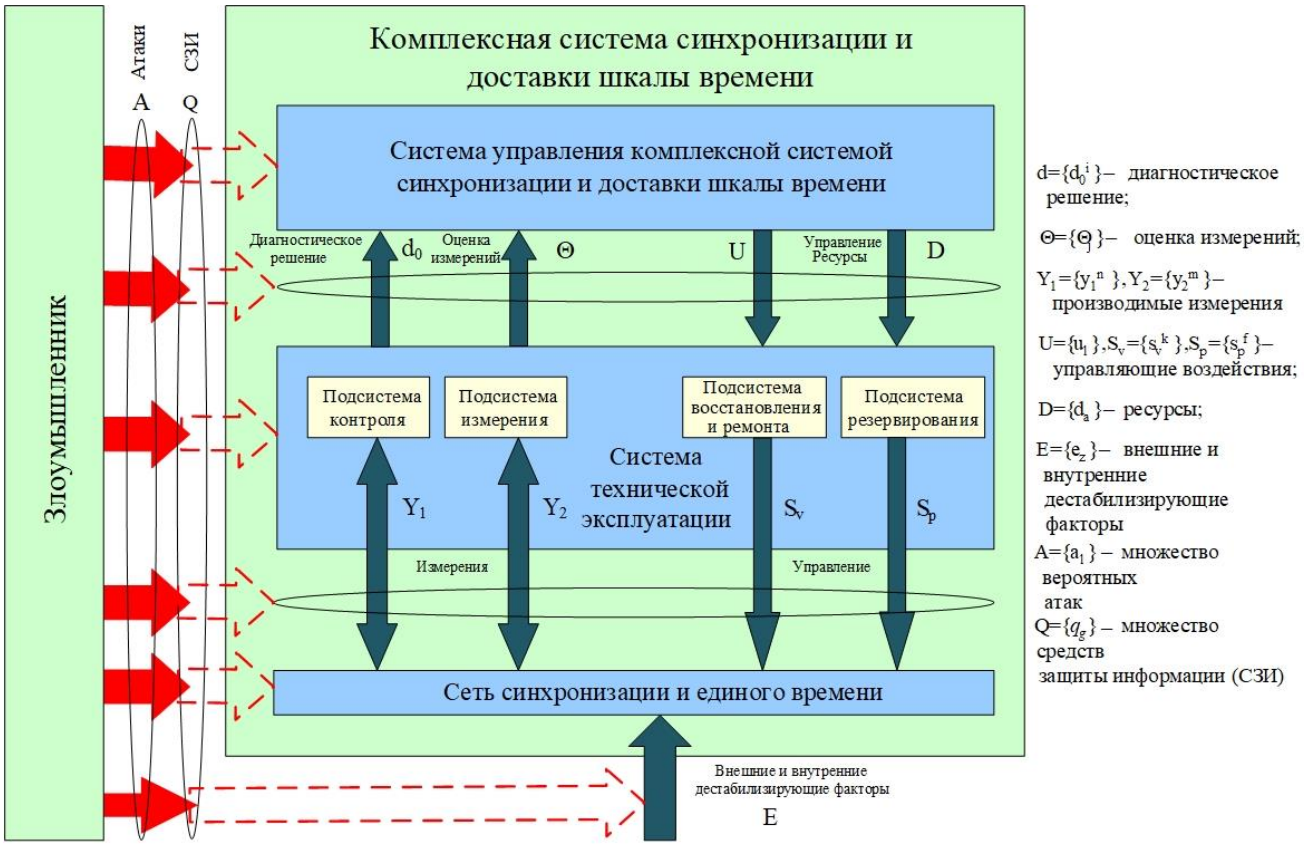

Рис. 1. Модель процесса функционирования комплексной системы синхронизации и доставки шкалы времени в условиях воздействий организованного злоумышленника

Комплексная система синхронизации и доставки шкалы времени в процессе своего функционирования подвергается дестабилизирующим воздействиям, направленным на снижение ее устойчивости. В общем виде дестабилизирующие воздействия на комплексную систему синхронизации и доставки шкалы времени можно классифицировать на воздействия естественного происхождения и воздействия искусственного происхождения. Среди воздействий искусственного происхождения стоит выделить информационные воздействия организованного злоумышленника [1–4].

Анализ различных потенциальных вариантов атак на комплексную систему синхронизации и доставки шкалы времени показал, что наиболее опасной атакой, способной нанести максимальный ущерб при её реализации является атака на систему управления комплексной системы синхронизации и доставки шкалы времени. При четком соблюдении нормативных документов по построению подсистем тактовой сетевой синхронизации и системы единого времени отказы отдельных элементов даже высокого уровня иерархии, а также направляющих систем, систем размножения, распределения и восстановления сигналов синхронизации и единого времени не приводят моментально к отказу всей комплексной системы синхронизации и доставки шкалы времени. В то же время как получение контроля злоумышленником над системой управления комплексной системы синхронизации и доставки шкалы времени способно моментально привести к значительным отказам и приостановке её процесса функционирования. При проведении атак на систему управления комплексной системы синхронизации и доставки шкалы времени злоумышленник способен непосредственно внедриться в систему управления, модифицировать процесс проведения измерений и аудит в комплексной системе синхронизации и доставки шкалы времени, внести изменения в оценки проведенных измерений, в управляющие команды. Наиболее опасными действиями со стороны злоумышленника являются установка вредоносного программного обеспечения, а также модификация модулей выработки управляющих решений системы управления [1–4].

III. Мониторинг технического состояния комплексной системы синхронизации и доставки шкалы времени

Основными целями при управлении комплексной системой синхронизации и доставки шкалы времени являются снижение затрат всех видов ресурсов на техническое обслуживание оборудования без понижения показателей надёжности, а также обеспечение

восстановления сети комплексной системы синхронизации и доставки шкалы времени в максимально короткие сроки, используя при этом рациональное число ресурсов. Указанные задачи решает система СТЭ. В сферу задач, решаемых СТЭ, также входит поддержание в исправном и работоспособном состоянии комплексной системы синхронизации и доставки шкалы времени, мониторинг и контроль показателей эффективности функционирования, а также выполнение планов, задаваемых системой управления, по поддержанию показателей эффективности функционирования в рамках существующих норм.

Следует отметить, что измерение отдельных частотно-временных параметров элементов комплексной системы синхронизации и доставки шкалы времени встроенными средствами диагностики может быть затруднено, так как для проведения подобных измерений необходимо построение специальных схем измерения и использование специализированных приборов (ИВО-1М, *OSA* 5565 *STS*), однако при использовании встроенных средств диагностики в соответствие с концепцией «менеджер-агент» и с применением протокола *SNMP* существует возможность получить общую статистику процесса функционирования элементов комплексной системы синхронизации и доставки шкалы времени.

В соответствии с концепцией «менеджер-агент» результаты диагностирования элементов комплексной системы синхронизации и доставки шкалы времени встроенными средствами диагностики могут периодически передаваться от «агента» к «менеджеру» или выдаваться по запросу «менеджера». При этом реализация обмена информацией в рамках концепции «менеджер-агент» реализуется при наличии специализированных *MIB* (*MIB – Management Information Base*) [1–4].

При функционировании устройств комплексной системы синхронизации и доставки шкалы времени большинство из них содержат в своём составе «агенты» (программные элементы), отслеживающие состояния данных устройств. «Агент» может представлять собой отдельную программу или элемент операционной системы. «Агент» предоставляет «менеджеру» информацию о состоянии контролирующих элементов устройства, отслеживая различные рабочие параметры и характеристики.

В случае запроса со стороны «менеджера» и передачи информации со стороны «агента», «менеджер» должен понимать, информацию какого вида передает «агент». Для этого существуют специальные *MIB* файлы, где приводится спецификация различных переменных, отражающих характеристики процесса функционирования устройств.

Большинство стандартных параметров и характеристик устройств, поддерживающих стек протоколов *TCP*/*IP* (например, таких характеристик и параметров, как скорость интерфейса, число отправленных и принятых байтов и т. д.), определены стандартными *MIB* (например, *MIB*-II *RFC* 1213). Дополнительно производители оборудования разрабатывают собственные *MIB* файлы для конкретного оборудования, которые могут быть внедрены в систему управления комплексной системы синхронизации и доставки шкалы времени.

На сети управления комплексной системы синхронизации и доставки шкалы времени в структуре технологической сети связи ОАО «РЖД» в качестве «менеджера» предлагается использовать сервера, расположенные в центрах технического обслуживания (ЦТО) и центрах технического управления (ЦТУ), отвечающие за функционирование сети комплексной системы синхронизации и доставки шкалы времени, а «агенты» – программные элементы, установленные внутри устройств комплексной системы синхронизации и доставки шкалы времени (ПЭГ, ВЗГ, МЗГ, ГСЭ, АРСС, *PRTC, T-GM, T-BC* и т. д.) [1–4].

IV. Использование фрактального анализа диагностической информации комплексной системы синхронизации и доставки шкалы времени для выявления кибератак

При больших масштабах мультисервисной сети, в том числе при масштабах технологической сети связи, по которой передается трафик диагностической информации комплексной системы синхронизации и доставки шкалы времени, можно сделать предположение, что трафик обладает свойством самоподобия. В дополнение, при развертывании централизованной системы управления комплексной системы синхронизации и доставки шкалы времени можно сформировать её таким образом, чтобы трафик диагностической информации, поступающий от устройств системы частотно-временного обеспечения, обладал свойствами самоподобия [5–7].

Указанное свойство самоподобия трафика диагностической информации можно использовать для решения задач информационной безопасности при обнаружени кибератак в комплексной системе синхронизации и доставки шкалы времени. В таком случае трафик диагностической информации можно представить, как временной ряд, состоящий из периодических запросов от менеджера к агенту, по результатам которого менеджер получает значение диагностического параметра [5–7].

В случае, если указанный временной ряд значений диагностических параметров теряет свойство самоподобия, это может свидетельствовать о возможной кибератаке на комплексную систему синхронизации и доставки шкалы времени. Подход по оценке самоподобия временного ряда может включать в себя:

- вычисление показателя Херста H, который является индикатором степени самоподобия рассматриваемого процесса;
- вычисление автокорреляционной функции диагностических параметров комплексной системы синхронизации и доставки шкалы времени.

Показатель Херста H можно вычислить следующим образом (1) [5–7]:

$$H = \log \frac{R/S}{\log(aN)} \quad (1)$$

где a – заданная константа, $a > 0$, N – размер ряда, показатель R представляет собой размах ряда, вычисляемый как разность между максимальным и

минимальным значением ряда, S – стандартное отклонение ряда, вычисляемое как (2) [5–7]:

$$S = \sqrt{1/N \sum_{i=1}^{N} \left(x_i - X_{\text{ср}}\right)^2} \qquad (2)$$

где x_i – конкретное значение диагностического параметра, $X_{\text{ср}}$ – среднее арифметическое рассматриваемого временного ряда.

При расчете показателя Херста для сравнительно краткосрочных временных рядов обычно применяется значение $a = 0{,}5$.

Для того чтобы рассматриваемый процесс считался самоподобным, необходимо, чтобы показатель Херста принимал значения от 0,5 до 1. Таким образом, в непрерывном режиме, отслеживая значения диагностических параметров элементов комплексной системы синхронизации и доставки шкалы времени встроенными средствами диагностики, возможно отслеживать показатель Херста и по его значениям делать вывод о наличии аномалий в процессе функционирования комплексной системы синхронизации и доставки шкалы времени [5–7].

При наличии графика автокорреляционной функции временного ряда значений диагностических параметров существует возможность выявить тенденции рассматриваемого ряда, например, нарушения периодичности, которые могут свидетельствовать о наличии аномалий. Также следует отметить, что тангенс угла наклона логарифмированной автокорреляционной функции связан с показатель Херста соотношением $\beta = 2H\text{-}2$ и может также рассматриваться как показатель фрактальности.

Следует отметить, что при условии значительного размера комплексной системы синхронизации и доставки шкалы времени, значительного числа входящих в нее элементов, рассматриваемых диагностических параметров, а значит и количества временных рядов, при реализации рассматриваемого подхода стоит изначально снизить размерность рассматриваемых данных, например, с использованием метода главных компонент или с использованием энтропийного анализа [5–7].

V. Заключение

Комплексная система синхронизации и доставки шкалы времени в структуре телекоммуникационной системы представляет собой взаимоувязанный комплекс, обеспечивающий целостность процесса функционирования всей системы связи. 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 телекоммуникационной системы. На современном этапе развития телекоммуникационных систем задачи обнаружения и предотвращения информационных атак организованных злоумышленников постоянно усложняются.

В данной статье предложен подход по обнаружению информационного воздействия на комплексную систему синхронизации и доставки шкалы времени с использованием анализа временных рядов диагностической информации, поступающей от устройств систем частотно-временного обеспечения.

Реализация указанного подхода на действующих и проектируемых системах частотно-временного обеспечения позволит значительно повысить их устойчивость при воздействии кибератак организованного злоумышленника.

Список литературы

[1] Рыжков А.В. Частотно-временное обеспечение в сетях электросвязи. М.: Горячая линия - Телеком, 2021. 270 с.

[2] Мазуренко Д.К. Аспекты построения системы частотно-временной сетевой синхронизации сигналов // T-Comm – Телекоммуникации и Транспорт. 2017. Т. 11, вып. 8. С. 4-8.

[3] Опарин Е.В. Методика формирования комплексной системы синхронизации и доставки шкалы времени для крупной распределенной системы технологического назначения // Известия Петербургского университета путей сообщения. 2023. Т. 20, вып. 3. С. 768-784.

[4] Коцыняк М.А., Осадчий А.И., Коцыняк М.М., Лаута О.С., Дементьев В.Е., Васюков Д.Ю. Обеспечение устойчивости информационно-телекоммуникационных сетей в условиях информационного противоборства. СПб.: Изд-во Типография Военной академии связи имени Маршала Советского Союза С.М. Буденного, 2014. 126 с.

[5] Лаврова Д.С. Математические методы обнаружения и предотвращения компьютерных атак на крупномасштабные системы. М.: Горячая линия - Телеком, 2022. 92 с.

[6] Лаврова Д.С., Струкова Н.Е. Обнаружение сетевых атак на системы интернета вещей с использованием регрессионного анализа // Проблемы информационной безопасности. Компьютерные системы. 2021, вып. 4. С. 39-50.

[7] Локтев А.А., Залетдинов А.В. Использование фракталов в задачах обеспечения информационной безопасности // Вестник Тамбовского университета. Серия «Естественные и технические науки». 2010. Т. 2, вып. 2. С. 442-447.