Полумарковская модель действий злоумышленника при атаке на систему управления сетью тактовой сетевой синхронизации

Semi-Markov model of an attacker's actions in an attack on a network management system of clock network synchronization

Канаев / Kanaev A.
Андрей Константинович
(Kanaev@itian.ru)
доктор технических наук, профессор.
ЗАО «Институт телекоммуникаций»,
заместитель генерального директора по спецпроектам.
г. Санкт-Петербург

Сахарова / Sakharova M.
Мария Александровна
(Saharova@itian.ru)
кандидат технических наук.
ЗАО «Институт телекоммуникаций»,
начальник отдела разработки средств связи.
г. Санкт-Петербург

Опарин / Oparin E.
Евгений Валерьевич
кандидат технических наук.
Институт «Гипротранссигналсвязь» – филиал
АО «Росжелдорпроект», инженер I категории.
г. Санкт-Петербург

Ключевые слова: полумарковская модель – Semi-Markov model; сеть тактовой сетевой синхронизации – clock network synchronization network; телекоммуникационная система – telecommunication system; система управления – control system; атака – attack; уязвимость – vulnerability; злоумышленник – attacker; система обеспечения информационной безопасности – information security system.

В данной статье приводится обобщенный анализ угроз информационной безопасности для сети тактовой сетевой синхронизации (ТСС) в контексте обобщенной модели предметной области функционирования сети ТСС. В особый класс угроз выделены угрозы при реализации атак на систему управления (СУ) ТСС. Приведена оценка защищенности сети ТСС телекоммуникационной системы от действий организованного злоумышленника при атаке на СУ сетью ТСС, которая реализует угрозу перестроения структуры сети ТСС. Предлагается обобщённая полумарковская модель процесса, отражающего основные этапы реализации атаки организованного злоумышленника с выделением состояний, характеризующихся отличительным набором воздействий на СУ сети ТСС и элементы сети ТСС. На основе разработанной полумарковской модели производится вычисление стационарных характеристик защищенности сети ТСС.

This article provides a generalized analysis of information security threats to a clock network synchronization network (CNS) in the context of a generalized model of the domain of operation of the CNS network. Threats during the implementation of attacks on the control system (CS) of the CNS are distinguished into a special class of threats. An assessment of the security of the CNS network of a telecommunication system (TCS) from the actions of an organized attacker during an attack on the CS by the CNS network, which implements the threat of rebuilding the structure of the CNS network, is given. A generalized semi-Markov model of the process is proposed that reflects the main stages of an attack by an organized attacker with the allocation of states characterized by a distinctive set of influences on the CS of the CNS network and elements of the CNS network. On the basis of the developed semi-Markov model, the stationary characteristics of the TSS network security are calculated.

4-2020.indd 46 24.12.2020 16:48:45

Введение

Потребность в точных сигналах времени и частоты возникает в различных производственных и экономических отраслях деятельности. В зависимости от конкретных целей уровень требуемой точности может находиться в пределах от 10^{-9} до 1 с. [1]. Деятельность любого крупного промышленного комплекса напрямую зависит от слаженной работы всех его структур и подразделений, поэтому для обеспечения устойчивого и надёжного функционирования различных технологических и информационных процессов требуется решить задачу частотно-временной синхронизации. Особенно актуальна указанная задача в системах передачи информации, обработки данных и измерительных систем, а также в системах хронометрирования событий, электронного документооборота и часофикации объектов.

Требования к точности сигналов для различных сфер применения представлены в таблице 1 [1].

Внедрение современных информационных и телекоммуникационных технологий, в том числе пакетных асинхронных технологий требует повышения внимания

Таблица 1

Потребители частотно-временных сигналов и предъявляемые ими требования

Применение	Требования по частоте	Требования по времени
CDMA2000	$\pm 50\times10^{-9}$	± 3 мкс по отношению к системному времени CDMA (который является прослеживаемым и синхронным с UTC) ± 10 мкс по отношению к системному времени CDMA в течение периода не менее 8 часов (когда внешний источник системного времени CDMA отключен)
TD-SCDMA	$\pm 50\times10^{-9}$	±1.5 мкс Максимальное отклонение 3 мкс во времени начала кадра между любыми парами ячеек на той же частоте, которые имеют перекрывающиеся зоны покрытия
GSM	$\pm 50\times10^{-9}$	n/a
WCDMA	$\pm 50\times10^{-9}$	В режиме TDD относительная разность фаз сигналов синхронизации на входе любого узла в синхронизированной области не должна превышать 2,5 пс
W-CDMA MBSFN	$\pm 50\times10^{-9}$	12,8 мкс для MBMS по одной частотной сети, где передача NodeB тесно синхронизирована по времени с общим опорным временем
LTE (FDD)	$\pm 50\times10^{-9}$	n/a
LTE (TDD)	$\pm 50\times10^{-9}$	±1.5 мкс (<3 км радиус ячейки) ±5 мкс (>3 радиус ячейки) Максимальное абсолютное отклонение в синхронизации начала кадра между любыми парами ячеек на той же частоте, которые имеют перекрывающиеся зоны покрытия
LTE-A MBSFN	$\pm 50\times10^{-9}$	±1 to 5 мкс Зависит от реализации приложений: • Агрегация операторов • Согласованная многоточечная передача (Network-MIMO) • Функция ретрансляции
LTE-A CoMP	$\pm 50\times10^{-9}$	
LTE-A elClC	$\pm 50\times10^{-9}$	
Мониторинг задержки сети IP	n/a	Требование зависит от уровня качества, который должен контролироваться. В качестве примера требование ± 100 мкс относительно общей временной привязки (например, UTC).
Биллинг и сигнализация	n/a	± 100 мс относительно общей ссылки времени (например, UTC)
Small Cells	$\pm 100\times10^{-9}$	n/a (FDD) ±1.5 мкс (TDD) ±1 to 5 мкс (elClC)
Home Cells	$\pm 250\times10^{-9}$	n/a (FDD) ±1.5 мкс (TDD)

4-2020.indd 47 24.12.2020 16:48:46

к организации процесса передачи частотно-временных сигналов.

Одной из основных подсистем ТКС является сеть тактовой сетевой синхронизации, которая выполняет функции формирования, передачи и распределения сигналов синхронизации, необходимых для поддержания работоспособного состояния всех цифровых устройств ТКС. Сеть ТСС находится в тесной взаимосвязи с другими подсистемами ТКС, оказывает существенное влияние на их работу и на функционирование всей ТКС в целом. Местоположение подсистемы ТСС в системе ТКС представлено на рис. 1 [2–4].

Показатели качества услуг электросвязи неразрывно связаны с показателями качества функционирования сети ТСС, а сигналы синхронизации и полезные информационные сигналы передаются, как правило, в одних и тех же цифровых потоках и по одним и тем же направляющим системам. Возникновение отказов на сети ТСС способно привести к значительному ухудшению качества передаваемой информации вплоть до полного отказа в предоставлении телекоммуникационных услуг [2–4].

В силу указанных особенностей, сеть ТСС является потенциально привлекательным местом проникновения в ТКС со стороны организованных злоумышленников с целью оказать деструктивное и разрушающее воздействие.

Особая опасность воздействия на сеть ТСС состоит в том, что влияние носит косвенный характер, при котором разрушение сети ТСС приводит к последующему разрушению ТКС. При возникновении подобных ситуаций могут возникать значительные затруднения по восстановлению процесса функционирования ТКС, так как зачастую невозможно достоверно определить причину возникновения отказов.

Обзор основных угроз информационной безопасности для сети ТСС со стороны организованного злоумышленника в рамках системного анализа процесса функционирования сети ТСС

Современные сети ТСС являются сложными гетерогенными структурами, которым присущ ряд атрибутивных свойств, анализ которых важен с точки зрения процесса их функционирования, в также организации потенциальной атаки злоумышленником. В первую очередь сеть ТСС характеризуют статические свойства, определяющие параметры сети ТСС в каждый произвольный момент времени. Среди статических свойств можно выделить целостность, открытость, внутреннюю неоднородность и структурированность [5].

Целостность сети ТСС подразумевает тот факт, что сеть ТСС представляет собой единый комплекс,

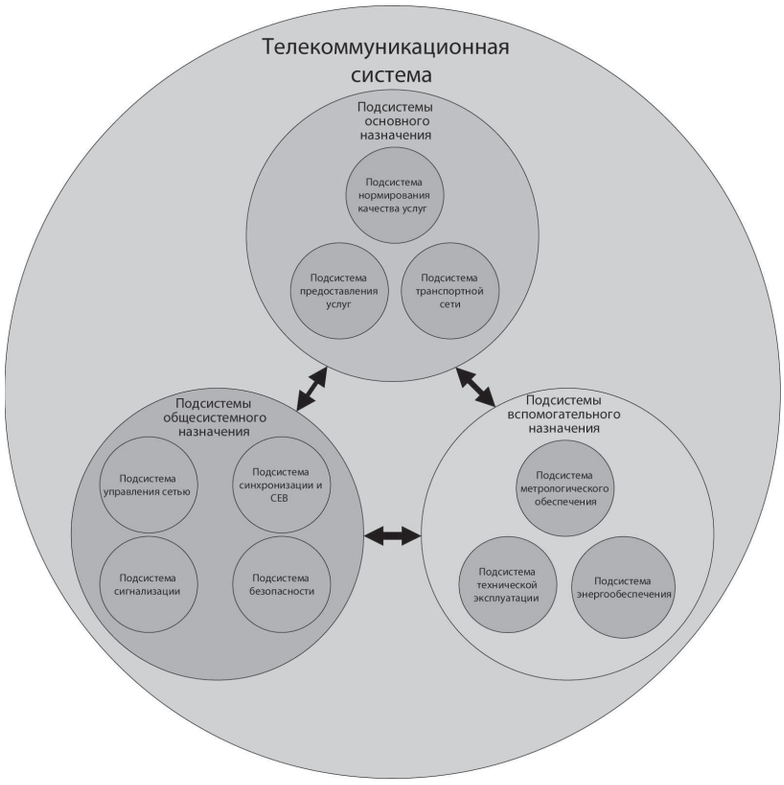

Рис. 1. Основные подсистемы телекоммуникационной системы

4-2020.indd 48 24.12.2020 16:48:46

имеющий границы, за пределами которых располагается среда, которая включает другие подсистемы ТКС и множество дестабилизирующих факторов (рис. 1). Следует отметить, что отказ или разрушение отдельных элементов сети ТСС ведет к отказу всех элементов, находящихся ниже по иерархии распространения сигналов синхронизации. Учитывая данную особенность, злоумышленник может атаковать отдельный узел сети ТСС, имеющий по возможности наибольший уровень иерархии, что способно привести к отказу узлов, находящихся ниже по уровню иерархии атакованного узла.

Установление границ сети ТСС важно с той точки зрения, что границы определяют рамки контролирующего и регулирующего влияния органов управления. Территориально сеть ТСС располагается в рамках определенного региона синхронизации, поэтому злоумышленник может искусственно расширить или сузить регион синхронизации, вывести из-под контроля органов управления отдельные узлы сети ТСС или добавить дополнительные, что приведет к изменению маршрутов доставки синхросигналов или подмене ведущих/ведомых источников синхронизации.

Сеть ТСС является открытой системой и взаимодействует с другими подсистемами и сетями ТКС. Данное взаимодействие осуществляется через стандартные интерфейсы, определяемые рекомендацией G.703 МСЭ-Т и другими рекомендациями, определяющими интерфейсы передачи цифровых сигналов. Данные интерфейсы являются точками обмена информацией между различными подсистемами ТКС. Открытость сети ТСС указывает на то, что она воздействует на другие подсистемы ТКС, в частности, те подсистемы, которым требуются сигналы точного времени и частоты, а также сама подвержена воздействию с их стороны. Эффективное функционирование ТКС определяется указанными связями воздействия, знанием о наличии данных связей или их отсутствии. Ошибки при определении связей воздействия могут привести к потерям времени и ресурсов при организации процесса управления сетью ТСС и всей ТКС. Открытость сети ТСС, как и остальных подсистем ТКС, приводит к всеобщей их взаимосвязи и взаимозависимости [2–5]. Злоумышленник может нарушить данное взаимодействие, закрыть отдельные интерфейсы, перенастроить взаимодействие подсистемы ТСС с другими подсистемами ТКС.

Сети ТСС присуща внутренняя неоднородность, которая выражается в построении иерархии сети (рис. 3), а также в различных типах и видах оборудования. Сеть ТСС включает в себя источники сигналов синхронизации, различающиеся по уровню иерархии (ПЭГ, ВЗГ, МЗГ, ГСЭ), аппаратуру распределения и коммутации сигналов синхронизации, элементы систем передачи и направляющих систем, благодаря которым обеспе-

Рис. 2. Концептуальная модель функционирования ТСС ТКС с учетом воздействия со стороны организованного злоумышленника

4-2020.indd 49 24.12.2020 16:48:47

чивается передача сигналов синхронизации. Неотъемлемыми элементами сети ТСС являются устройства ретайминга и оборудование восстановления характеристик синхросигналов, а также ряд дополнительных устройств конвертирования сигналов синхронизации из сетей TDM в пакетные сети и наоборот. Каждый из выделенных элементов сети ТСС имеет различные свойства и характеристики, а также выполняет свои определённые функции.

Перечисленные элементы сети ТСС, а также подсистемы, обеспечивающие её функционирование, и перечень связей между ними образуют комплексную структуру, обеспечивающую формирование и передачу сигналов синхронизации. Указанное свойство структурности выражается в организации строгой иерархии источников синхросигналов, чётком задании направляющих систем и маршрутов передачи сигналов синхронизации, организацией приоритетов выбора сигналов и исключением колец синхронизации [2–5]. Злоумышленник в состоянии провести атаки на отдельные элементы сети ТСС, нарушить иерархию источников синхросигналов, изменить приоритеты выбора синхросигналов, создать кольца синхронизации (рис. 2).

Рассмотренные статические свойства присущи сети ТСС при различных режимах её функционирования, но с течением времени могут изменяться некоторые её характеристики и параметры, возможно ухудшение показателей МОВИ, ДВИ сигналов синхронизации, изменяться маршруты их передачи, под влиянием дестабилизирующих факторов возможно изменение качества сигналов синхронизации и режимов синхронизации. Указанные изменения характеризуют динамические свойства сети ТСС, среди которых выделяют функциональность, управляемость, существование и изменчивость подсистемы ТСС в изменяющейся среде [2–5].

Функциональность сети ТСС подразумевает тот факт, что сеть ТСС выполняет определённый набор функций. Среди функций сети ТСС выделяют формирование сигналов синхронизации, которое выполняется источниками различного уровня иерархии; передачу сигналов синхронизации по направляющим системам с использованием систем передачи; восстановление сигналов синхронизации с применением оборудования ретайминга; преобразование синхросигналов из сетей TDM в пакетные сети и наоборот; распределение и размножение сигналов синхронизации, а также способность восстанавливать заданные показатели функционирования сети ТСС при воздействии дестабилизирующих факторов различного характера [2–4]. Злоумышленник способен изменить набор функций, выполняемых сетью ТСС, добавить новые функции, не свойственные подсистеме ТСС, что приведет к дополнительной нагрузке на её ресурсы, или устранить выполнение основополагающих функций.

Эффективное осуществление функций сети ТСС возможно только при организации системы управления,

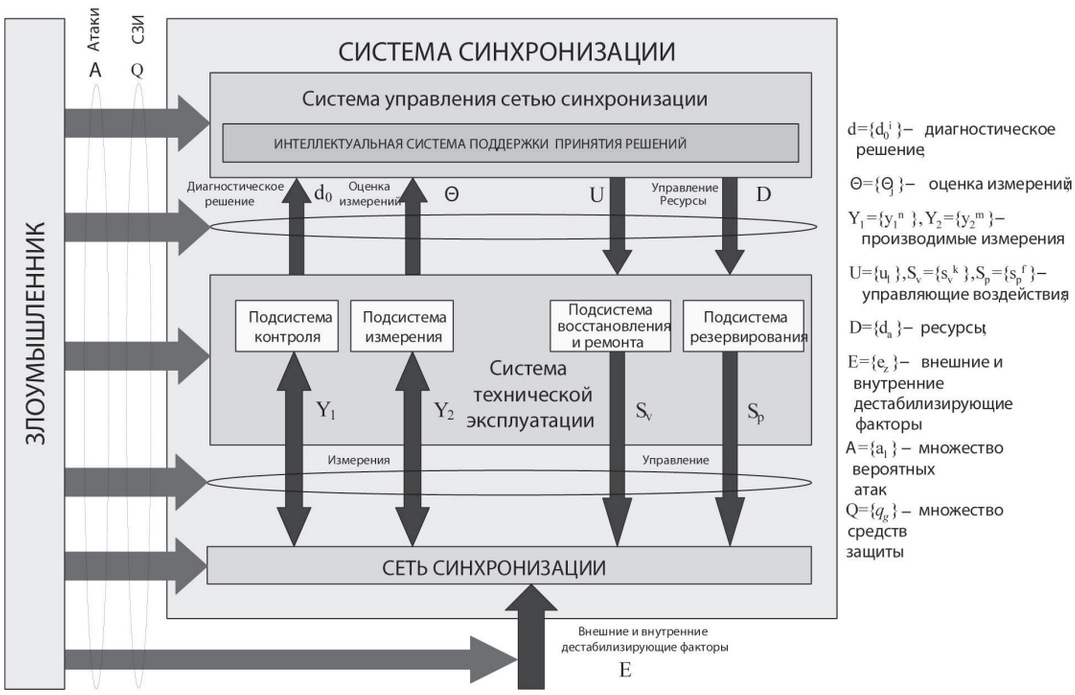

Рис. 3. Обобщённая модель предметной области функционирования ТСС с учетом воздействия организованного злоумышленника

4-2020.indd 50 24.12.2020 16:48:47

способной применить целенаправленные воздействия к сети ТСС для её оптимального функционирования. Данный факт выражается свойством управляемости. Управление на сети ТСС, как правило, имеет многоуровневую иерархическую структуру, сеть ТСС разбивается на регионы, имеющие свои органы управления, координирующие работу сети в пределах заданного региона. Комплексное управление сети ТСС осуществляется центральным органом [2–4]. Злоумышленник способен внедриться в систему управления ТСС, в данном случае он будет обладать полной свободой действий по управлению сетью ТСС.

В сети ТСС с течением времени могут происходить различные изменения, что выражается свойством изменчивости [5]. Данные изменения происходят как под влиянием органов управления, так и под влиянием дестабилизирующих факторов и воздействий. Злоумышленник способен вносить изменения как путем организации атаки на СУ ТСС, так и искусственной модификацией физической среды, управлением дестабилизирующими факторами, такими как влияние температуры, нестабильности электропитания, электромагнитных воздействий. Изменения могут носить как стремительный характер, например в случае отказа направляющий системы или источника синхронизации верхнего уровня, так и монотонный, в случае постепенного дрейфа частоты в генераторах сетевых элементов. Изменения возможны в составе и структуре сети ТСС, которые могут носить как качественный, так и количественный характер, что может выражаться увеличением или уменьшением состава оборудования, а также их техническими характеристиками. Изменения могут носить внезапный характер, в случае внезапного отказа, или детерминированный. Если злоумышленник будет способен управлять данными изменениями, он способен создавать отказы в сети ТСС, которые будут являться труднообнаруживаемыми и трудноустранимыми.

Анализ различных потенциальных вариантов атак на сеть ТСС, таких как манипуляция синхросигналами, спуфинг в сети ТСС, атака повторного воспроизведения, атака подмены роли устройств и маршрутов в сети ТСС, перехват и удаление сообщений, показал, что наиболее опасной атакой на сеть ТСС, способной нанести максимальный ущерб при её реализации, является атака на СУ ТСС. При четком соблюдении нормативных документов по построению сети ТСС в процессе своего функционирования сеть ТСС является самовосстанавливающей системой. Отказ отдельного элемента сети ТСС даже высокого уровня иерархии, а также направляющих систем, систем размножения, распределения и восстановления сигналов синхронизации не приводит моментально к отказу всей подсистемы ТСС. В то время как получение контроля злоумышленником над СУ ТСС способно моментально привести к значительным отказам и приостановке процесса функционирования всей подсистемы ТСС.

Основными целями при управлении сети ТСС являются снижение затрат всех видов ресурсов на техническое обслуживание оборудования ТСС без понижения показателей надёжности, а также восстановление сети ТСС в максимально короткие сроки, используя при этом рациональное число ресурсов.

Указанные задачи решает система технической эксплуатации (СТЭ). В сферу задач, решаемых СТЭ, также входит поддержание в исправном и работоспособном состоянии системы ТСС, мониторинг и контроль показателей эффективности функционирования системы ТСС, а также выполнение планов, задаваемых органами управления по поддержанию показателей эффективности функционирования сети ТСС в рамках существующих норм [2–4]. Обобщённая модель предметной области управления сетью ТСС примет вид, показанный на рис. 3.

Данная модель (рис. 3) имеет трёхуровневую структуру, на нижнем уровне располагается сеть ТСС, включающая все основное оборудование синхронизации. Второй уровень образует система технической эксплуатации сети ТСС, включающая подсистемы контроля, измерений, резервирования, восстановления и ремонта. Третий уровень образует интеллектуальная система управления сетью ТСС. В совокупности указанные три уровня образуют систему ТСС.

Злоумышленник способен непосредственно внедриться в сами элементы сети ТСС, модифицировать процесс проведения измерений и аудит сети ТСС, внести изменения в оценки проведенных измерений, в управляющие команды. Наиболее опасными действиями со стороны злоумышленника являются установка вредоносного ПО в СУ ТСС и модификация ИСППР СУ ТСС. Обобщённая модель предметной области функционирования ТСС с учетом воздействия на неё организованного злоумышленника показана на рис. 3. Злоумышленник, получивший доступ к СУ сетью ТСС, способен значительно снизить качество передаваемых синхросигналов и сигналов точного времени, что приведет к снижению качества предоставляемых услуг связи.

Наиболее вероятной атакой на СУ сетью ТСС со стороны организованных злоумышленников является атака по перестроению структуры сети синхронизации и изменению маршрутов доставки синхросигналов. Реализация данного вида атаки способна нанести значительный урон сети ТСС за максимально короткое время и привести к значительным отказам в ТКС [2, 6, 7].

Модель действий злоумышленника при атаке на систему управления сетью ТСС, которая реализует угрозу перестроения структуры сети ТСС

Проведенный анализ процесса проведения атак позволил сформировать следующую полумарковскую

4-2020.indd 51 24.12.2020 16:48:47

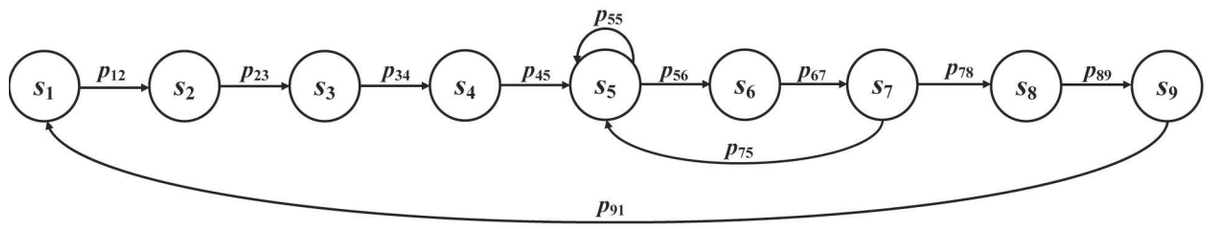

Рис. 4. Полумарковская модель действий злоумышленника при атаке на систему управления сетью ТСС, которая реализует угрозу перестроения структуры сети ТСС

модель действий злоумышленника при реализации атаки по перестроению структуры сети ТСС (рис. 4).

Данная модель отражает все основные действия организованного злоумышленника. Несмотря на множество сценариев возможных атак и инструментов по их реализации, модель действий злоумышленника при реализации атаки по перестроению структуры сети ТСС [2, 6, 7].

s_1 – Злоумышленник определяет цель атаки по получению доступа к СУ сетью ТСС.

s_2 – Подготовка к атаке на СУ сетью ТСС.

s_3 – Получение доступа к СУ сети ТСС.

s_4 – Анализ злоумышленником существующей структуры сети ТСС и маршрутов доставки синхросигналов.

s_5 – Расчет злоумышленником структуры сети ТСС и маршрутов доставки синхросигналов по целевому критерию.

s_6 – Перестроение злоумышленником структуры сети ТСС и маршрутов передачи синхросигналов по произведенному расчету.

s_7 – Оценка злоумышленником результатов своей атаки.

s_8 – Сокрытие следов присутствия в СУ сетью ТСС.

s_9 – Выход злоумышленника из СУ сети ТСС.

Исходным состоянием является состояние s_1, когда злоумышленник ставит цель по получению доступа к СУ ТСС и перестроению структуры сети ТСС. В состоянии s_2 злоумышленник осуществляет подготовку к атаке на СУ сети ТСС: проводит сбор исходных данных, касающихся СУ сети ТСС, используя методы социальной инженерии и данные из открытых источников; вычисляет активные сервера и узлы СУ сети ТСС; определяет точки входа в СУ сетью ТСС и проводит анализ уязвимостей точек входа; обходит системы обеспечения информационной безопасности (СОИБ) [2, 6, 7].

На следующем этапе в состоянии s_3 злоумышленник получает доступ к СУ сетью ТСС. Получение доступа к СУ сетью ТСС может быть реализовано в общем случае посредством сетевых атак, а также атак на Web-приложения, операционные системы и программное обеспечение СУ сетью ТСС. К сетевым методам получения доступа можно отнести реализации атаки снифинга, атаки спуффинга или атаки отказа в обслуживании. При реализации атак на программное обеспечение злоумышленник может использовать методы переполнения буфера, атаки на пароли и атаки на Web-приложения [2, 6, 7].

Получив доступ к СУ сетью синхронизации в состоянии s_4 злоумышленник проводит анализ её структуры и маршрутов передачи синхросигналов при помощи встроенных в СУ сетью ТСС механизмов технической диагностики и мониторинга.

Полученная в состоянии s_4 информация является исходными данными для расчета злоумышленником в состоянии s_5 варианта перестроения структуры сети ТСС и маршрутов передачи синхросигналов. Перед проведением атаки злоумышленник имеет определенную цель по перестроению сети ТСС, которая характеризуется набором критериев. Данные критерии будут являться основанием для последующего расчета изменения маршрутов передачи синхросигналов и внесения дополнительных задержек. Ограничивающими факторами для злоумышленника на данном этапе являются ресурс времени и мощность вычислительной аппаратуры, находящейся в его распоряжении.

По итогам пятого этапа в состоянии s_6 злоумышленнику остается реализовать полученный план действий по перестроению сети ТСС путем подачи управляющих команд на аппаратуру сети ТСС и в итерационном режиме корректировать реализацию своего плана действий.

В состоянии s_7 злоумышленник будет оценивать итоги своей деятельности и при необходимости повторять процедуры перестроения сети ТСС.

Добившись поставленной цели, злоумышленник в состоянии s_8 будет стремиться к тому, чтобы максимально скрыть следы своего присутствия. Чтобы избежать обнаружения системами СОИБ, злоумышленник изменит файлы регистрации событий в СУ сетью ТСС, удалив определенные события, связанные с получением доступа, повышением привилегий, установкой RootKit и «черных ходов». Также злоумышленник будет использовать механизмы сокрытия следов в СУ сетью ТСС, которые включают создание файлов и каталогов с особыми именами или атрибутами. Для сокрытия сетевой активности злоумышленник применит механизмы туннелирования [2, 6, 7].

4-2020.indd 52 24.12.2020 16:48:48

Добившись определенных результатов при реализации атаки, а также под воздействием противодействия со стороны систем СОИБ, злоумышленник будет вынужден в состоянии s_9 свернуть свою деятельность и покинуть СУ сетью ТСС.

Определение стационарных характеристик процесса, описывающего действия злоумышленника при реализации атаки по перестроению структуры сети ТСС

Основными стационарными характеристиками, определяющими защищенность сети ТСС, будут являться [7, 8]:

– стационарные вероятности $(\pi_i), i = 1,...,9; i \in S$ пребывания в произвольный момент времени в каждом из состояний s_i, характеризуемых определенным набором действий злоумышленника;

– среднее время реализации атаки T_A и среднее время восстановления сети ТСС от последствий реализации атаки T_B.

Исходными данными для оценки стационарных характеристик процесса, описывающего действия злоумышленника при реализации атаки по перестроению структуры сети ТСС, будут являться [7, 8]:

1. Матрица переходных вероятностей из одного состояния в другое $\Pi = (p_{ij})$.

2. Матрица функций распределения условных случайных времен пребывания рассматриваемого процесса атаки в каждом из s_i состояний $F_{ij}(t)$.

Стационарную вероятность пребывания рассматриваемого процесса атаки в произвольный момент времени в каждом из состояний s_i можно вычислить по следующей формуле [7, 8]:

$$\pi_i = \frac{P_i T_i}{\sum_{j \in S} P_j T_j} (i, j = 1,...,9; i, j \in S; \sum_{i \in S} \pi_i = 1), \quad (1)$$

где P_i, P_j – стационарная вероятность пребывания вложенной однородной марковской цепи в состоянии s_i и s_j, T_i, T_j – математическое ожидание безусловного времени пребывания процесса атаки в каждом состоянии, S – общее число состояний.

Для оценки математического ожидания безусловного времени пребывания процесса реализации атаки в каждом состоянии воспользуемся следующими выражениями [7, 8] (2, 3):

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

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

где T_{ij} – математическое ожидание условного времени пребывания в каждом состоянии процесса реализации атаки.

Для оценки стационарной вероятности пребывания вложенной однородной марковской цепи в состоянии s_i используем следующее выражение [7, 8] (4, 5):

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

где $D_i(D_j)$ – минор, получаемый вычеркиванием $i(j)$-й строки и $i(j)$-го столбца матрицы D.

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

Для оценки среднего времени реализации атаки T_A и среднего времени восстановления сети ТСС от последствий реализации атаки T_B конечное множество состояний S процесса реализации атаки (рис. 5) разделим на два непересекающихся подмножества состояний: состояний в которых сеть ТСС обеспечивает выполнение возложенных на неё функций $S_{TCC} \subset S$ и состояний, в которых сеть ТСС подвержена активному деструктивному воздействию $\overline{S_{TCC}} \subset S$. Отметим, что $S_{TCC} \cup \overline{S_{TCC}} = 0$. будут являться состояния s_1, s_2, s_3, s_4, s_5 и s_9. $\overline{S_{TCC}}$ будут являться состояния s_6, s_7 и s_8.

При наличии указанных исходных данных среднее время реализации атаки T_A и среднее времени восстановления сети ТСС от последствий реализации атаки T_B можно найти по следующим выражениям [7, 8]:

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

$$T_B = \frac{\sum_{i \in \overline{S_{TCC}}} P_i T_i}{\sum_{i \in S} P_i \sum_{j \in S_{TCC}} p_{ij}}, \quad (7)$$

где S_+ и $S_$ – подмножество граничных состояний, обуславливающих переход из подмножества S_{TCC} в подмножество $\overline{S_{TCC}}$ и наоборот.

Подмножеством граничных состояний S_+ является состояние s_5. Подмножеством граничных состояний $S_$ является состояния s_7 и s_8.

Оценив стационарные вероятности π_i пребывания процесса реализации атаки в произвольный момент времени в каждом из состояний s_i (рис. 4) можно определить коэффициент исправного действия Ки СУ сети ТСС.

Коэффициент исправного действия $К_и$ СУ сети ТСС является показателем, характеризующим устойчивость СУ сети ТСС в процессе её функционирования,

4-2020.indd 53 24.12.2020 16:48:49

в том числе в условиях воздействия атак организованных злоумышленников [9].

$$К_и = \sum_{i \in S_I} \pi_i . \quad (8)$$

Расчет численных значений стационарных характеристик процесса, описывающего действия злоумышленника при реализации атаки по перестроению структуры сети ТСС

В качестве примера ниже приведена оценка стационарных характеристик процесса, описывающего действия злоумышленника при реализации атаки по перестроению структуры сети ТСС. В качестве исходных приняты следующие данные. Матрица переходных вероятностей имеет следующий вид (9):

$$П = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.2 & 0.8 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0.2 & 0 & 0 & 0.8 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \quad (9)$$

В качестве распределения условных случайных времен пребывания в каждом из s_i состояний $F_{ij}(t)$ принято экспоненциальное распределение со следующей матрицей интенсивностей переходов (10):

$$\Lambda = \begin{pmatrix} 0 & \frac{1}{72} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{6} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{3} & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{3} & 0 & 0 & \frac{1}{3} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \\ \frac{1}{24} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, ч^{-1} . \quad (10)$$

Таким образом, после последующего расчёта на основе предложенного подхода и разработанной полумарковской модели действий злоумышленника при реализации атаки по перестроению структуры сети ТСС были получены следующие результаты. Матрица математических ожиданий условных времен пребывания в каждом состоянии примет следующий вид (11):

$$T_{ij} = \begin{pmatrix} 0 & 72 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \\ 24 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, ч . \quad (11)$$

Вектор математических ожиданий безусловных времен пребывания в каждом состоянии примет следующий вид (12):

$$T_i = \begin{pmatrix} 71.99 & 6 & 2 & 4 & 1.4 & 1 & 3 & 0.5 & 24 \end{pmatrix}, ч . \quad (12)$$

Вектор стационарных вероятностей пребывания вложенной однородной марковской цепи в состояниях s_i примет следующий вид (13):

$$P_i = \begin{pmatrix} 0.099 & 0.099 & 0.099 & 0.099 & 0.155 \\ 0.124 & 0.124 & 0.099 & 0.099 \end{pmatrix} . \quad (13)$$

Таким образом, будут получены следующие стационарные вероятности пребывания в произвольный момент времени в каждом из состояний s_i (14):

$$\pi_i = \begin{pmatrix} 0.628 & 0.052 & 0.017 & 0.026 & 0.019 \\ 0.011 & 0.033 & 4.36 \times 10^{-3} & 0.209 \end{pmatrix} . \quad (14)$$

Данные вероятности π_i показывают, что в любой случайный момент времени организованный злоумышленник проводит свои действия, характеризуемые одним из состояний s_i.

Среднее время реализации атаки T_A и среднее время восстановления сети ТСС от последствий реализации атаки T_B будет вычислено следующим образом (15, 16):

$$T_A = \frac{\sum_{i \in S_{TCC}} P_i T_i}{\sum_{i \in S_+} P_i \sum_{j \in \overline{S_{TCC}}} p_{ij}} = \frac{P_1 T_1 + P_2 T_2 + P_3 T_3 + P_4 T_4 + P_5 T_5 + P_9 T_9}{P_5 p_{56}} =$$

$$= 87.35 ч \approx 3.64 сут. \quad (15)$$

4-2020.indd 54 24.12.2020 16:48:50

$$T_B = \frac{\sum\limits_{i \in S_{TCC}} P_i T_i}{\sum\limits_{i \in S} P_i \sum\limits_{j \in S_{TCC}} p_{ij}} = \frac{P_6 T_6 + P_7 T_7 + P_8 T_8}{\left(P_7 + P_8\right)\left(p_{75} + p_{89}\right)} = 2.037 \text{ ч.} \quad (16)$$

Данные значения показывают, что злоумышленник реализует атаку и перестроит структуру сети ТСС в соответствии со своими целями через 3,64 суток, а через 2,037 часа его деятельность будет локализована системами СОИБ и сеть ТСС восстановит свою функциональность и работоспособность.

Соответственно коэффициент исправного действия $К_и$ сети ТСС при указанном сценарии реализации атаки примет следующее значение (15):

$$К_и = \sum_{i \in S_{TCC}} \pi_i = 0.952 . \quad (15)$$

Оценим также влияние действий злоумышленника и систем СОИБ на коэффициент исправного действия $К_и$ СУ сети ТСС, среднее время реализации атаки T_A и среднее времени восстановления сети ТСС от последствий реализации атаки T_B. В результате проведенного моделирования были получены следующие результаты (рис. 5–6).

По результатам моделирования можно сделать следующие выводы.

1. увеличение интенсивности действий злоумышленника снижает коэффициент исправного действия Ки СУ сети ТСС, а действия систем СОИБ повышают

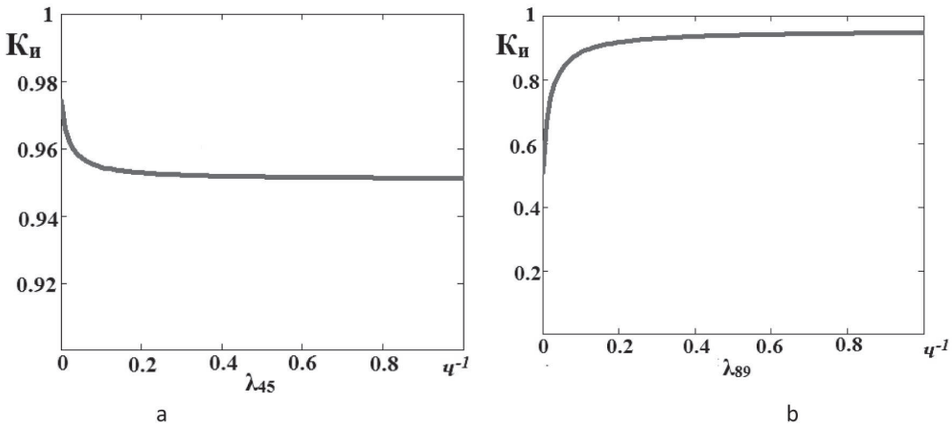

Рис. 5. Зависимость коэффициента исправного действия $К_и$ СУ сети ТСС от показателя вычислительных ресурсов оборудования злоумышленника (a) и от показателя эффективности функционирования систем СОИБ (b)

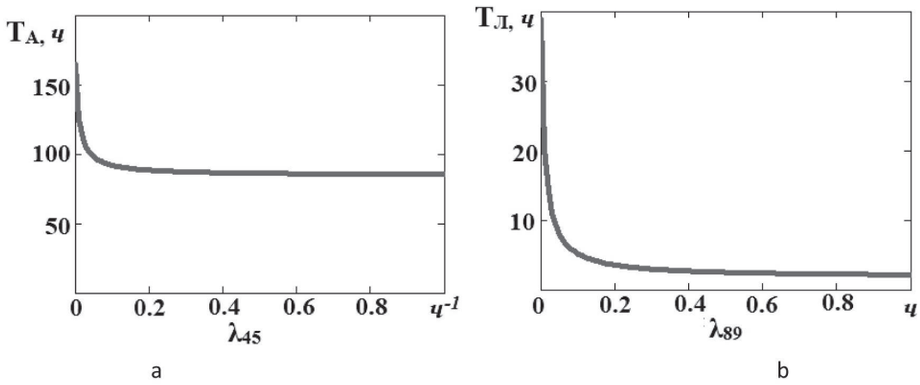

Рис. 6. Зависимость времени реализации атаки от показателя вычислительных ресурсов оборудования злоумышленника (a) и зависимость времени локализации злоумышленника от показателя эффективности функционирования систем СОИБ (b)

4-2020.indd 55 24.12.2020 16:48:51

его. Различные этапы действий злоумышленника и систем СОИБ вносят различный вклад в решение общих задач как для злоумышленника, так и для систем СОИБ. Данную зависимость можно оценить как задачу оптимизации как для действий злоумышленника, так и для систем СОИБ.

2. интервал интенсивности попыток действий организованного злоумышленника и действий систем СОИБ можно разделить на два диапазона. В первом диапазоне незначительное изменение интенсивности действий злоумышленника или действий систем СОИБ приводит к значительному изменению коэффициента исправного действия $К_и$. Во втором диапазоне изменение интенсивности противоборствующих сторон не приводит к значительному изменению коэффициента исправного действия $К_и$. Оценив данные диапазоны, злоумышленник может оптимально управлять своими ресурсами по организации атаки на СУ сетью ТСС, а администраторы безопасности соответственно управлять средствами защиты.

3. по результатам моделирования можно также оценить среднее время реализации атаки и среднее время восстановления сети ТСС от последствий реализации атаки в зависимости от ресурсов самого злоумышленника так и ресурсов систем СОИБ.

Заключение

Сеть ТСС является важной подсистемой ТКС, непосредственно влияющей на качество предоставления услуг связи. В связи с чем в данной статье представлен анализ основных угроз для сети ТСС и пути их реализации организованным злоумышленником. В особый класс угроз выделены угрозы при реализации атак на СУ ТСС. Приведены результаты по оценке стационарных характеристик защищенности и уязвимости СУ сети ТСС от действий организованного злоумышленника при атаке, которая реализует угрозу перестроения структуры сети ТСС. Полученные результаты позволят на основе анализа отдельных средств защиты СУ сети ТСС и всей сети ТСС, статистики архива отраженных и завершенных атак, а также различных методов тестирования оценить показатели защищенности и уязвимости СУ сети ТСС, а следовательно, сделать вывод о целесообразности использования или внедрения отдельного вида средств защиты.

Предполагается, что функции распределения условных случайных времен пребывания в каждом из состояний будут определяться из практики и анализа результатов контрольных тестирований, что позволит получить модель действий злоумышленника с реальными свойствами. Данная модель универсальна, отличается полнотой учёта состояний и может быть применена к любой СУ сети ТСС, а также позволяет определять стационарные характеристики процесса действий злоумышленника для каждого состояния, что позволяет при наложении нормативных требований на стационарные характеристики формировать множество стратегий защиты от действий организованного злоумышленника.

Литература

1. 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.

2. Давыдкин, П. Н. Тактовая сетевая синхронизация / П.Н. Давыдкин, М.Н. Колтунов, А.В. Рыжков. – М.: Эко-Трендз, 2004. – 205 с.

3. Буренин, А. Н. Теоретические основы управления современными телекоммуникационными сетями: Монография / А.Н. Буренин, В.И. Курносов. – М.: Наука, 2011. – 464 с.

4. Канаев, А. К. Предложения по построению интеллектуальной системы поддержки принятия решений по управлению сетью тактовой сетевой синхронизацией / А.К. Канаев, Е.В. Опарин // Труды учебных заведений связи. – 2017. – № 4. – С. 43–53.

5. Романов, В. Н. Системный анализ для инженеров / В.Н. Романов. – СПб.: СЗГЗТУ, 2006. – 186 с.

6. Лукацкий, А. В. Обнаружение атак / Алексей Лукацкий. – СПб.: БХВ-Санкт-Петербург, 2003. – 596 с.

7. Скудис, Э. Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите: Пер. с англ. / Эд. Скудис. – М.: ДМК Пресс, 2003. – 512 с.

8. Шубинский, И. Б. Структурная надёжность информационных систем. Методы анализа / И. Б. Шубинский. – Ульяновск: Областная типография «Печатный двор», 2012. – 216 с.

9. Обеспечение устойчивости информационно-телекоммуникационных сетей в условиях информационного противоборства / М.А. Коцыняк [и др.]. – СПб.: ЛО ЦНИИС, 2014. – 126 с.

4-2020.indd 56 24.12.2020 16:48:52