УДК 621.395

Модель функционирования комплексов управления программно-конфигурируемыми компонентами защищенной NGN сети ведомственной системы связи в условиях таргетированных кибератак

Model of operation of control complexes of software configurable components of a protected NGN network of a departmental communication system under targeted cyber attacks

Буренин / Burenin A.
Андрей Николаевич
(direct-2011@mail.ru)
доктор технических наук, доцент.
АО «Научно-исследовательский институт «Рубин»,
ведущий научный сотрудник.
г. Санкт-Петербург

Чуйков / Chujkov V.
Владимир Борисович
(v.b.chujkov@rubin-spb.ru)
кандидат технических наук, доцент.
АО «Научно-исследовательский институт «Рубин»,
первый заместитель генерального директора.
г. Санкт-Петербург

Аванесов / Avanesov M.
Михаил Юрьевич
(avanesov@itain.ru)
кандидат технических наук.
ЗАО «Институт телекоммуникаций»,
научный секретарь.
г. Санкт-Петербург

Ключевые слова: система – system; автоматизированная система управления – the automated control system; сеть следующего поколения – next generation network (NGN); комплексы управления – control complexes; программно-конфигурируемые сетевые компоненты сети следующего поколения – software-configurable network components (SCNC) of the next generation network (NGN); уровень управления сетью – network control plane; таргетированные атаки – targeted attacks; потоки информации о состоянии – status information streams.

Рассматривается модель безопасного функционирования комплексов управления программно-конфигурируемыми компонентами защищенных сетей следующего поколения ведомственных (корпоративных) систем связи в условиях воздействия на них интенсивных таргетированных кибератак. Рассматриваются задачи получения в основном вероятностных моделей с учетом характеристик системы защиты от таргетированных кибератак при условии, что система защиты состоит из комплексов обеспечения безопасности.

A model of the safe functioning of control complexes for software-configurable components of secure networks of the next generation of departmental (corporate) communication systems under the influence of intensive targeted cyber attacks is considered. The problems of obtaining mainly probabilistic models are considered, taking into account the characteristics of the protection system against targeted cyber attacks, provided that the protection system consists of security systems.

Введение

В современных условиях резко возрастает вероятность существенного изменения характера функционирования корпоративных и ведомственных систем связи (СС) [1–4] под воздействием высокоинтенсивных таргетированных или целевых атак, представляющих собой вид кибератак, которые направлены на компрометацию системы управления СС, могут иметь различные векторы развития и проводиться в несколько этапов. Как правило, таргетированная атака состоит из нескольких стадий, и обнаружение такого типа угроз чрезвычайно затруднено из-за направленного характера действий злоумышленников и их воздействия на автоматизированные системы управления (АСУ) системами связи в целом или на их наиболее критически важные подсистемы. В результате может произойти срыв процессов управления.

Требуемое противодействие разного рода таргетированным кибератакам на АСУ СС и на подсистемы управления сетями не может быть обеспечено только созданием эффективной системы комплексной безопасности, поэтому обычно также создаются специальные подсистемы управления безопасностью, которые в совокупности образуют систему защиты АСУ от таргетированных кибератак [1, 4].

При создании такой комплексной системы защиты от таргетированных кибератак необходимо оперировать определенными параметрами и характеристи-

ками функционирования АСУ СС для того, чтобы быть уверенным в достаточности (или недостаточности) выделяемых средств для обеспечения устойчивого функционирования АСУ и устойчивого процесса управления базовой сетью следующего поколения (NGN), составляющей телекоммуникационное ядро ведомственных или корпоративных систем связи, строящейся в соответствии с концепцией защищенных мультисервисных сетей и компонентами этой сети. Последние все чаще реализуются на принципах программно-конфигурируемых (программно-определяемых) сетевых компонентов (ПКСК). Это связано с тем, что в сфере информационных технологий происходит кардинальная смена подходов к построению сетей на основе конвергенции двух основных технологий: SDN (программно-конфигурируемые сети) и NFV (виртуализация сетевых функций). Эта конвергенция достигается за счет более глубокого проникновения принципа программного управления в реализацию сервисов и развитие техники виртуализации, при этом основной упор делается на использование программных методов с возложением вспомогательной роли на аппаратную составляющую.

Основные идеи SDN включают: разделение прохождения трафика (data plane) и сигнализацию/управление (control plane); существенное упрощение сетевых элементов уровня data plane; единый, унифицированный, не зависящий от поставщика интерфейс между уровнем управления и уровнем передачи данных; логически централизованное управление сетью, осуществляемое с помощью контроллеров с установленной сетевой операционной системой и реализованными поверх сетевыми приложениями с помощью программного интерфейса приложений (application programming interface или API).

Реализация управления отдельным ПКСК в рамках АСУ NGN осуществляется центрами управления (основным и резервными), реализующими два уровня программно-определяемого сетевого компонента: уровня приложений (application layer) и уровня сетевых контроллеров (control layer). Они для АСУ NGN являются функциональными агрегатами автоматизации управления (ААУ) ПКСК.

Особенности функционирования системы защиты АСУ NGN и агрегатов автоматизации управления ПКСК от таргетированных кибератак

Система защиты АСУ ведомственной (корпоративной) СС от таргетированных кибератак, как правило, носит распределенный по компонентам АСУ характер. Поэтому и система обеспечения комплексной безопасности будет содержать несколько серверов безопасности и управления безопасностью и будет также распределенной.

Из множества способов декомпозиции архитектур АСУ ведомственной (корпоративной) СС целесообразно выделить особый класс подсистем (агрегатов автоматизации управления), функционирование которых критически важно для АСУ и каждый из которых имеет специальные устройства защиты от кибератак, являющихся компонентами системы защиты. В каждом защищаемом ААУ ПКСК можно выделить вызванные таргетированными кибератаками временные отказы (сбои, зависания, приостановки работы) и длительные отказы или аварии. При этом к временным киберотказам или кибersбоям целесообразно относить отказы, при которых нормальное функционирование ААУ ПКСК прекращается, но это не сопровождается существенными его повреждениями (нарушением функционирования) и не требует больших затрат на его восстановление.

Длительные отказы или кибераварии характеризуются не только значительной величиной времени неработоспособности, но и значительными функциональными повреждениями самого ААУ ПКСК (особенно опасно повреждение программ application layer), а также связанного с ним другого ПО и оборудования АСУ, влекут за собой как большой ущерб работоспособности, так и большие (в основном временные) затраты на восстановление. Длительный отказ, как правило, возникает не мгновенно. Сначала в результате воздействий таргетированных кибератак на отдельные элементы самого ААУ ПКСК или изменения внешних условий его работы создается некоторая предаварийная ситуация, которая имеет объективные симптомы и может быть своевременно обнаружена. Эту задачу и выполняет тот компонент системы защиты, который выполняет функции обеспечения комплексной безопасности. При отсутствии в нем требуемых элементов каждая предаварийная ситуация переходит в длительный отказ или кибераварию ААУ ПКСК. Таким образом, цель системы защиты АСУ СС в целом и ее компонента для отдельного ПКСК состоит в переводе потенциальных длительных отказов (кибераварий) во временные отказы или кибersбои, при которых ААУ каждого ПКСК функционально восстанавливаются за конечное время.

Характеристики функционирования ААУ ПКСК и АСУ СС

Очевидно, что кратковременные отказы (кибersбои) и длительные отказы (кибераварии), вызванные кибератаками нарушителей, можно рассматривать как независимые случайные события. При этом безотказное функционирование каждого i-го ААУ ПКСК наиболее полно можно описать двумя функциями времени: $P_{isb}^{\text{ПССК}}(t)$ и $P_{iav}^{\text{ПССК}}(t)$ – соответственно вероятностями бессбойной и безаварийной работы в течение времени t, которые можно задать следующим образом [5–12]:

$$P_{isb}^{\text{ПССК}}(t)=1-F_{isb}^{\text{ПССК}}(t)$$
$$P_{iav}^{\text{ПССК}}(t)=1-F_{iav}^{\text{ПССК}}(t)\text{,} \quad (1)$$

где $F_{isb}^{\text{ПССК}}(t)$ и $F_{iav}^{\text{ПССК}}(t)$ – соответственно функции распределения времени возникновения сбойной или аварийной ситуации в *i*-м ААУ ПКСК, вызванной таргетированными кибератаками.

В целом система защиты от таргетированных кибератак может оказывать двоякое влияние на кибербезотказность функционирования каждого *i*-го ААУ ПКСК [1, 2, 4, 6–8].

С одной стороны, снижается вероятность возникновения киберавариий при неизменной вероятности возникновения аварийной ситуации $P_{iav}^{\text{ПССК}}(t)$, т. к. аварийная ситуация может перейти в кибераварию только в том случае, если система защиты сама будет находиться в неработоспособном состоянии (состоянии «несрабатывания» по неработоспособности) или если она не содержит требуемые компоненты защиты (состояние «несрабатывания» по недостаточной функциональности системы защиты). В противном случае аварийная ситуация переходит в состояние киберсбоя и восстановления.

С другой стороны, увеличивается вероятность возникновения сбойных ситуаций: во-первых, киберавариии (по крайней мере, часть из них) переводятся в сбойные ситуации, а во-вторых, при возникновении отказов типа «ложное срабатывание» возможны необоснованные отключения *i*-го ААУ ПКСК. Поэтому показателями кибербезотказности системы защиты АСУ в целом от кибератак является совокупность функций распределения времени возникновения киберотказов каждого *i*-го ААУ ПКСК типа «несрабатывание» и «ложное срабатывание» или соответственно $F_{insr}^{\text{ПССК}}(t)$ и $F_{ilsr}^{\text{ПССК}}(t)$.

Показатели киберустойчивости АСУ с системой защиты, очевидно, должны быть аналогичны показателям для каждого *i*-го ААУ ПКСК. Поэтому по аналогии с *i*-м ААУ ПКСК для всей АСУ СС с системой защиты от кибератак при соответствующей трактовке состояний можно записать:

$$P_{ASCsb}^{\Sigma}(t)=1-F_{ASCsb}^{\Sigma}(t)$$
$$P_{ASCav}^{\Sigma}(t)=1-F_{ASCav}^{\Sigma}(t)\text{,} \quad (2)$$

где $F_{ASCsb}^{\Sigma}(t)$ и $F_{ASCav}^{\Sigma}(t)$ – соответственно функции распределения времени возникновения сбойной или аварийной ситуации в АСУ СС из-за воздействия таргетированных кибератак при наличии системы защиты от них.

Часто при наличии защиты от таргетированных кибератак трудно получить полное выражение для функций $F_{ASCsb}^{\Sigma}(t)$ и $F_{ASCav}^{\Sigma}(t)$. Тогда в качестве показателей киберустойчивости АСУ СС с системой защиты от таргетированных кибератак можно использовать некоторые числовые характеристики этих распределений или связанные с ними параметры (интенсивность λ_{ASCav}^{Σ} потока аварийных или интенсивность λ_{ASCsb}^{Σ} сбойных ситуаций, среднее время $t^{\Sigma}_{ASCbo\text{ср}}$ бессбойной или среднее время $T^{\Sigma}_{ASCba\text{ср}}$ безаварийной работы АСУ СС в условиях воздействия на нее таргетированных кибератак и т. п. Такие показатели киберустойчивости удобны в тех случаях, когда рассматриваемая АСУ является функционально восстанавливаемой и отрезок времени $\tau^{\Sigma}_{ASC\text{ср}}$, в расчете на который ведется оценка ее киберустойчивости, значительно превышает среднее время ее безотказной работы $T^{\Sigma}_{ASC\text{ср}}$, т. е. $\tau^{\Sigma}_{ASCsb} >> T^{\Sigma}_{ASC\text{ср}}$.

Для АСУ СС с системой защиты по-настоящему аварийная ситуация, вызванная таргетированными кибератаками нарушителей, явление достаточно редкое. Как правило, средняя наработка на одну кибераварию даже в условиях интенсивных таргетированных кибератак может достигать во время функционирования СС сотен часов [1, 4]. При этом расчетный отрезок времени зависит от условий, в которых функционирует СС. В нормальных условиях этот отрезок составляет от месяца до года, а в чрезвычайных в зависимости от выполняемых СС задач – от десятков часов до суток.

Поэтому в чрезвычайных условиях функционирования СС всегда выполняется неравенство $\tau^{\Sigma}_{ASCsb} >> T^{\Sigma}_{ASC\text{ср}}$ и можно пользоваться для описания функционирования параметрами λ^{Σ}_{ASCav}, λ^{Σ}_{ASCsb}, $t^{\Sigma}_{ASCbo\text{ср}}$ и $T^{\Sigma}_{ASCba\text{ср}}$, а также декомпозированными параметрами $\lambda^{\text{ПССК}}_{iASCav}$, $\lambda^{\text{ПССК}}_{iASCsb}$, $t^{\text{ПССК}}_{iASCbo\text{ср}}$ и $T^{\text{ПССК}}_{iASCba\text{ср}}$ для каждого *i*-го ААУ ПКСК.

В нормальных условиях функционирования СС целесообразно оценить киберустойчивость АСУ СС с системой защиты на переходном участке, т. е. определить вероятность безаварийной работы до первой киберавариии. В общем случае основными показателями бессбойного и безаварийного функционирования АСУ СС с системой защиты от таргетированных кибератак следует считать функции распределения времени безаварийной и бессбойной работы за некоторое время τ, а также среднее время восстановления компонентов системы защиты, которое при наличии отказов типа «несрабатывание» соответствует среднему времени профилактики. С учетом критической важности каждого *i*-го ААУ ПКСК для функционирования всей АСУ СС важно рассматривать характеристики функционирования отдельного агрегата автоматизированного управления ПКСК при различных вариантах построения системы защиты.

Функционирование ААУ ПКСК и АСУ СС при различных вариантах организации системы защиты от таргетированных кибератак

При организации системы защиты АСУ СС от таргетированных кибератак возможны три способа

включения элементов системы защиты в защищаемый *i*-й ААУ ПКСК (*i*-му ААУ ПКСК приписан *i*-й компонент системы защиты):

– последовательное включение, когда все элементы *i*-го агрегатного компонента системы защиты включены последовательно с компонентами защищаемого *i*-го ААУ ПКСК;

– параллельное включение, когда все элементы *i*-го агрегатного компонента системы защиты включены параллельно компонентам защищаемого *i*-го ААУ ПКСК и не влияют на их функционирование;

– мешанное включение, представляющее собой комбинацию из двух способов включения элементов *i*-го агрегатного компонента системы защиты.

При последовательном включении компонентов подсистемы защиты вероятность безотказной работы защищаемого *i*-го ААУ ПКСК составит:

$$P_{ibos}^{\text{ПССК}}(t) = P_{ibo}^{\text{ПССК}}(t) P_{boisz}^{\text{ПССК}}(t), \qquad (3)$$

где $P_{ibo}^{\text{ПССК}}(t)$ и $P_{boisz}^{\text{ПССК}}(t)$ – вероятности безотказной работы за время соответственно *i*-го защищаемого ААУ ПКСК и *i*-го компонента системы защиты.

Ясно, что такое включение компонентов системы защиты от таргетированных кибератак имеет ряд недостатков. Во-первых, отказ *i*-го компонента системы защиты (например, типа «обрыв логической цепи») ведет к отказу всего защищаемого *i*-го ААУ ПКСК. Таким образом, АСУ СС теряет работоспособность *i*-го ААУ ПКСК за счет отказов как самого незащищенного *i*-го ААУ, так и *i*-го компонента системы защиты от кибератак, что приводит к ряду ложных остановок *i*-го агрегата по вине системы защиты, что является недостатком последовательно включенных устройств защиты.

Вместе с тем вероятность безаварийной работы при последовательном включении *i*-го компонента системы защиты в цепь функционирования незащищенного *i*-го ААУ ПКСК повышается, так как ситуация, при которой компонент защиты отказал, а сам *i*-й ААУ ПКСК продолжает работать незащищенным, просто невозможна. Примером подобной защиты являются локальные анализаторы трафика. Они включены последовательно как с точки зрения телекоммуникационных цепей *i*-го ААУ ПКСК, так и с точки зрения кибербезопасности. Выход из строя такого компонента системы защиты (обрыв цепи передачи информации) приведет к отключению защищаемого *i*-го ААУ ПКСК. Ситуация же, при которой компонент защиты отказал, а защищаемый *i*-й ААУ ПКСК продолжает функционировать, исключена.

При параллельном включении *i*-го ААУ ПКСК и соответствующего компонента системы защиты, его отказ не сопровождается кибераварией данного *i*-го ААУ ПКСК и АСУ в целом. Защита может отказать, а *i*-й агрегат автоматизации будет продолжать работать. В этом случае возникновение аварийной ситуации в *i*-м ААУ ПКСК неизбежно приводит к кибераварии.

Следует отметить, что для большинства АСУ NGN ведомственных (корпоративных) СС имеет место (или используется наиболее часто) параллельное включение компонентов системы защиты от таргетированных кибератак со всеми защищаемыми ААУ. При этом характеристики безаварийности и безотказности таких АСУ существенно зависят от режима обслуживания каждого *i*-го ААУ ПКСК при возникновении сбойной или аварийной ситуации. При этом возможно применение двух моделей обслуживания каждого *i*-го ААУ ПКСК при использовании системы защиты от таргетированных кибератак:

– аварийный *i*-й ААУ ПКСК до истечения расчетного времени τ не восстанавливается и вновь в работу не запускается;

– аварийный ААУ мгновенно восстанавливается (заменяется резервным, ранее не подключенным к сети, с некоторыми базовыми начальными сетевыми установками) и вновь включается в работу, в результате чего за время τ он может восстанавливаться многократно (определяется числом резервных *i*-х ААУ ПКСК, с учетом программно восстановленных), а время восстановления (подключения резервного *i*-го ААУ ПКСК) после таргетированных кибератак обычно невелико по сравнению с расчетным временем и его влиянием на безаварийность каждого *i*-го ААУ ПКСК можно пренебречь.

Различие приведенных двух моделей защиты проявляется в том, что в первой модели к концу отрезка времени τ каждый *i*-й ААУ ПКСК может находиться в одном из трех состояний в контексте безопасности – работоспособности, сбойной ситуации и аварийной ситуации, а во второй модели таких состояний только два – работоспособность и аварийная ситуация. Рассмотрим данные модели раздельно.

Если *i*-й аварийный ААУ ПКСК не восстанавливается, то в качестве исходных данных для анализа будем считать заданными функции распределения $F_{isb}^{\text{ПССК}}(t), F_{iav}^{\text{ПССК}}(t), F_{insr}^{\text{ПССК}}(t), F_{ilsr}^{\text{ПССК}}(t)$ и их производные (плотности распределения) $f_{isb}^{\text{ПССК}}(t), f_{iav}^{\text{ПССК}}(t), f_{insr}^{\text{ПССК}}(t), f_{ilsr}^{\text{ПССК}}(t)$.

Время работы *i*-го ААУ ПКСК с компонентом защиты до возникновения кибераварии $T_{iav}^{\text{ПССК}}$ представляет собой функцию «отставания» от случайных аргументов $T_{iavsb}^{\text{ПССК}}$ и $T_{insr}^{\text{ПССК}}$:

$$T_{iav}^{\text{ПССК}} = \begin{cases} T_{iav}^{\text{ПССК}} \to t_{iavsb}^{\text{ПССК}} \geq t_{insr}^{\text{ПССК}}; \\ 0 \to t_{iavsb}^{\text{ПССК}} < t_{insr}^{\text{ПССК}} \end{cases}. \qquad (4)$$

При такой постановке функция распределения времени работы *i*-го ААУ ПКСК с компонентом системы защиты до кибераварии будет определяться следующим выражением:

$$F_{iav}^{\text{ПССК}}(\tau)=\int_0^{\tau} F_{insr}^{\text{ПССК}}(t)\,f_{iav}^{\text{ПССК}}(t)\,dt\,. \qquad (5)$$

Естественно предположить, что:

– вероятность одновременного возникновения аварийной ситуации и отказа *i*-го компонента системы защиты от таргетированных кибератак равна нулю;

– отказ *i*-го компонента системы защиты от таргетированных кибератак как следствие развития аварийной ситуации исключается (в противном случае следовало бы признать, что принципы защиты выбраны неудачно, а сама система защиты просто неправильно спроектирована, так как не может работать в условиях, для которых предназначена). Тогда вероятность безаварийной работы *i*-го ААУ ПКСК составит:

$$P_{iav}^{\text{ПССК}}(\tau)=1-F_{iav}^{\text{ПССК}}(\tau)=1-\int_0^{\tau} F_{insr}^{\text{ПССК}}(t)\,f_{iav}^{\text{ПССК}}(t)\,dt\,. \qquad (6)$$

Выражение (6) является достаточно общим, позволяющим определить функцию распределения времени безаварийной (в контексте безопасности) работы *i*-го ААУ ПКСК с компонентом системы защиты при любых известных законах распределения аварийных ситуаций и отказов типа «несрабатывание» в нем.

При эксплуатации ведомственных (корпоративных) СС нередки ситуации, когда на *i*-й ААУ ПКСК воздействуют таргетированные кибератаки, для которых характерным является, что приведенные функции распределения имеют экспоненциальный вид: $F_{insr}^{\text{ПССК}}(t)=1-e^{-\lambda_{insr}^{\text{ПССК}}t}$ и $F_{iav}^{\text{ПССК}}(t)=1-e^{-\lambda_{iav}^{\text{ПССК}}t}$. При этом выражение (6) принимает следующий вид:

$$P_{iav}^{\text{ПССК}}(\tau)=e^{-\lambda_{iav}^{\text{ПССК}}\tau}+\frac{\lambda_{iav}^{\text{ПССК}}}{\lambda_{iav}^{\text{ПССК}}+\lambda_{insr}^{\text{ПССК}}}[1-e^{-(\lambda_{iav}^{\text{ПССК}}+\lambda_{insr}^{\text{ПССК}})\tau}]. \qquad (7)$$

Если учесть, что к АСУ NGN ведомственной (корпоративной) СС, оснащенной системой защиты от таргетированных кибератак, как правило, предъявляются достаточно высокие требования по кибер безаварийности (вероятность безаварийной работы должна быть выше 0,99), то значения $\lambda_{iav}^{\text{ПССК}}$ и $\lambda_{insr}^{\text{ПССК}}$ достаточно малы. Тогда допустимы следующие приближения:

$$e^{-\lambda_{iav}^{\text{ПССК}}\tau}\approx 1-\lambda_{iav}^{\text{ПССК}}\tau+0{,}5(\lambda_{iav}^{\text{ПССК}}\tau)^2\,. \qquad (8)$$

$$e^{-(\lambda_{iav}^{\text{ПССК}}+\lambda_{insr}^{\text{ПССК}})\tau}\approx 1-(\lambda_{iav}^{\text{ПССК}}+\lambda_{insr}^{\text{ПССК}})\tau+0{,}5(\lambda_{iav}^{\text{ПССК}}+\lambda_{insr}^{\text{ПССК}})^2\tau^2\,. \qquad (9)$$

Подставив выражения (8) и (9) в уравнение (7), можно получить выражение для вероятности безаварийного (в контексте безопасности) функционирования *i*-го ААУ ПКСК, достаточно простое и удобное для практических расчетов:

$$P_{iav}^{\text{ПССК}}(\tau)=e^{-\lambda_{iav}^{\text{ПССК}}\tau}+\frac{\lambda_{iav}^{\text{ПССК}}}{\lambda_{iav}^{\text{ПССК}}+\lambda_{insr}^{\text{ПССК}}}[1-e^{-(\lambda_{iav}^{\text{ПССК}}+\lambda_{insr}^{\text{ПССК}})\tau}]=$$

$$=1-0{,}5\lambda_{iav}^{\text{ПССК}}\lambda_{insr}^{\text{ПССК}}\tau^2 \qquad (10)$$

Из (10) следует, что при $\tau\to 0$ значение вероятности $P_{iav}^{\text{ПССК}}(\tau)\to 1$, а при $\tau\to\infty$ значение вероятности $P_{iav}^{\text{ПССК}}(\tau)\to\frac{\lambda_{iav}^{\text{ПССК}}}{\lambda_{iav}^{\text{ПССК}}+\lambda_{insr}^{\text{ПССК}}}$. Несомненно, это совершенно естественный результат для принятой модели защиты каждого *i*-го ААУ ПКСК. Если *i*-й ААУ ПКСК в случае сбойной ситуации не восстанавливается, то это значит, что при достаточно длительном наблюдении он придет либо в состояние кибераварии (с вероятностью $P_{iav}^{\text{ПССК}}(\tau)=\frac{\lambda_{insr}^{\text{ПССК}}}{\lambda_{iav}^{\text{ПССК}}+\lambda_{insr}^{\text{ПССК}}}$), либо в состояние сбойного состояния (киберсбой с вероятностью $P_{isb}^{\text{ПССК}}(\tau)=\frac{\lambda_{iav}^{\text{ПССК}}}{\lambda_{iav}^{\text{ПССК}}+\lambda_{insr}^{\text{ПССК}}}$).

Если же отказавший из-за таргетированной кибератаки *i*-й ААУ ПКСК мгновенно восстанавливается (заменяется резервным), то выражение для вероятности возникновения аварийной ситуации в интервале (t, τ) примет следующий вид:

$$P_{iav}^{\text{ПССК}}(t,\tau)=F_{iav}^{\text{ПССК}}(\tau-\theta)-F_{iav}^{\text{ПССК}}(t-\theta), \qquad (12)$$

где θ – момент возникновения последнего (перед отказом компонента системы защиты типа «несрабатывание») сбойной ситуации *i*-го ААУ ПКСК.

Учитывая, что θ есть величина случайная, в общем случае с произвольным законом распределения, расчет $P_{iav}^{\text{ПССК}}(t,\tau)$ сопряжен со значительными трудностями.

Почему же в практических исследованиях рассматривается весьма распространенное экспоненциальное распределение времени аварийных ситуаций?

Потому, что в этом случае момент времени проведения последнего восстановления *i*-го ААУ ПКСК безразличен, а имеет значение лишь сам факт нахождения его в работоспособном состоянии в момент отказа компонента системы защиты. Тогда вероятность возникновения аварийной ситуации в интервале (t, τ), т. е. после отказа компонента системы защиты от таргетированных кибератак, составит:

$$P_{iav}^{\text{ПССК}}(t,\tau)=F_{iav}^{\text{ПССК}}(0,\tau-t). \qquad (13)$$

Соответствующие функция и плотность распределения (при экспоненциальном распределении времени возникновения аварийных ситуаций и отказов компонентов системы защиты от кибератак) будут иметь следующий вид:

$$F_{iav}^{\text{ПССК}}(0,\tau-t)=\int_0^{\tau-t}\lambda_{iav}^{\text{ПССК}}e^{-\lambda_{iav}^{\text{ПССК}}\tau}dt=1-e^{-\lambda_{iav}^{\text{ПССК}}\tau}e^{-\lambda_{iav}^{\text{ПССК}}t}. \qquad (14)$$

$$f_{insr}^{\text{ПССК}}(t) = \lambda_{insr}^{\text{ПССК}} e^{-\lambda_{insr}^{\text{ПССК}} t}. \quad (15)$$

Тогда выражение для вероятности безаварийного функционирования *i*-го ААУ ПКСК примет следующий вид:

$$P_{iav}^{\text{ПССК}}(\tau) = \begin{cases} e^{-\lambda_{insr}^{\text{ПССК}}\tau} + \dfrac{\lambda_{insr}^{\text{ПССК}}}{\lambda_{insr}^{\text{ПССК}} - \lambda_{iav}^{\text{ПССК}}}\left(e^{-\lambda_{iav}^{\text{ПССК}}\tau} - e^{-\lambda_{insr}^{\text{ПССК}}\tau}\right) \\ \forall \lambda_{iav}^{\text{ПССК}} \neq \lambda_{insr}^{\text{ПССК}}; \\ e^{-\lambda_{insr}^{\text{ПССК}}\tau} + \lambda_{insr}^{\text{ПССК}}\tau e^{-\lambda_{iav}^{\text{ПССК}}\tau} \rightarrow \lambda_{iav}^{\text{ПССК}} = \lambda_{insr}^{\text{ПССК}} \end{cases}. \quad (16)$$

Если ведущие функции распределений $\lambda_{iav}^{\text{ПССК}}\tau << 1$, $\lambda_{insr}^{\text{ПССК}}\tau << 1$, то справедливо следующее выражение для вероятности $P_{iav}^{\text{ПССК}}(\tau)$:

$$P_{iav}^{\text{ПССК}}(\tau) \approx 1 - 0{,}5\lambda_{iav}^{\text{ПССК}}\lambda_{insr}^{\text{ПССК}}\tau^2. \quad (17)$$

Таким образом, если выполняются условия $\lambda_{iav}^{\text{ПССК}}\tau << 1$, $\lambda_{insr}^{\text{ПССК}}\tau << 1$, то выражение для вероятности безаварийного функционирования *i*-го ААУ ПКСК за время τ в условиях применения нарушителем широкого класса таргетированных кибератак (для модели с мгновенным восстановлением каждого *i*-го ААУ) идентично выражению (10) для модели с невосстанавливаемым агрегатом автоматизации управления. Это объясняется тем, что при высокоустойчивых к таргетированным кибератакам ААУ ПКСК (выполнение условия $\lambda_{iav}^{\text{ПССК}}\tau << 1$) маловероятно наличие больше одного киберотказа (от удачно проведенной таргетированной кибератаки) за время τ и расчетные формулы для обеих моделей совпадают.

Выводы

Обеспечение безопасности функционирования АСУ NGN как телекоммуникационной основы ведомственной или корпоративной системы связи, гарантирующей предоставления требуемых услуг пользователям, предполагает осуществление процедур организации комплексной защиты информации, информационных ресурсов сетей, а также элементов АСУ, выполняющих активные функции по управлению компонентами NGN, которые все чаще реализуются на принципах программно-конфигурируемых (программно-определяемых) сетевых компонентов (ПКСК). ПКСК включают разделение прохождения трафика (data plane) и сигнализацию/управление (control plane); существенное упрощение сетевых элементов уровня data plane; единый, унифицированный, независящий от поставщика интерфейс между уровнем управления и уровнем передачи данных; логически централизованное управление сетью, осуществляемое с помощью контроллеров с установленной сетевой операционной системой и реализованными поверх сетевыми приложениями.

Задача обеспечения безопасного функционирования АСУ СС усложняется в условиях использования нарушителем разного рода высокоинтенсивных таргетированных кибератак на наиболее критически важные ее элементы (агрегаты автоматизации управления ПКСК), нарушение работы которых может привести к срыву процессов обмена информацией.

Для решения задачи обеспечения безопасного функционирования системы управления полезно иметь определенные вероятностно-временные характеристики, определяющие достаточность (или недостаточность) выделяемых средств для обеспечения устойчивого функционирования каждого ААУ ПКСК. При этом требуемые вероятностно-временные характеристики процесса функционирования каждого ААУ ПКСК в обстановке воздействующих на него широкого класса таргетированных кибератак и при условии реализованной системы защиты от них зависят при прочих равных условиях от вариантов построения этой системы защиты, от того, как подключены ее компоненты к каждому агрегату управления автоматизации.

В материалах статьи для возможных вариантов подключения компонентов системы защиты к каждому агрегату автоматизации управления программно-конфигурируемым сетевым компонентом, а также для различных моделей обслуживания каждого ААУ предложен и получен ряд таких характеристик функционирования, задав определенные значения которых можно быть уверенным, что создаваемая система защиты от таргетированных кибератак обеспечит устойчивое управление элементами базовой сети ведомственной (корпоративной) системы связи и, следовательно, в значительной степени устойчивое функционирование самой системы связи.

Литература

1. Буренин, А. Н. Инфокоммуникационные системы и сети специального назначения. Основы построения и управления / А.Н. Буренин, К.Е. Легков. – Москва : ИД Медиа Паблишер, 2015. – 348 с.

2. Буренин, А. Н. Методические подходы к формализации управления инфокоммуникационными системами и сетями специального назначения / А.Н. Буренин, К.Е. Легков // Наукоемкие технологии в космических исследованиях Земли. – 2015. – Т. 7, № 5. – С. 64–67.

3. Буренин, А. Н. Модели состояния современных инфокоммуникационных сетей при организации стохастического управления ими / А.Н. Буренин, К.Е. Легков // Наукоемкие технологии в космических исследованиях Земли. – 2019. – Т. 11, № 2. – С. 32–40.

4. Буренин, А. Н. Вопросы безопасности инфокоммуникационных систем и сетей специального назначения: основные угрозы, способы и средства обеспечения комплексной безопасности сетей / А.Н. Буренин, К.Е. Легков // Наукоемкие технологии в космических исследованиях Земли. – 2015. – Т. 7, № 3. – С. 46–61.

5. Ушаков, И. А. Вероятностные модели надежности информационно-вычислительных систем / И.А. Ушаков. – Москва : Радио и связь, 1991. – 132 с.

6. Феллер, В. Введение в теорию вероятностей и ее приложения. В 2 т. Т. 1 / В. Феллер. – Москва : Мир, 1984. – 567 с.

7. Шнепс, М. А. Системы распределения информации. Методы расчета / М.А. Шнепс. – Москва : Связь, 1979. – 344 с.

8. Математическая теория оптимальных процессов / Л.С. Понтрягин, В.Г. Болтянский, З.В. Гамкрелидзе, Е.Ф. Мищенко. – Москва : Наука, 1983. – 392 с.

9. Гихман, И. И. Введение в теорию случайных процессов / И.И. Гихман, А.В. Скороход. – Москва : Наука, 1965. – 606 с.

10. Prabhu, N. U. Stochastic Processes. Basic Theory and its Applications / N.U. Prabhu. – New York, 1965. – 347 p.

11. Карлин, С. Основы теории случайных процессов / С. Карлин ; перевод с английского В.В. Калашникова. – Москва : Мир, 1971. – 658 с.

12. Володин, И. Н. Лекции по теории вероятностей и математической статистике / И.Н. Володин. – Казань : Издательство Казанского университета, 2006. – 271 с.