МОДЕЛЬ ВОЗДЕЙСТВИЯ ЗЛОУМЫШЛЕННИКА НА ФРАГМЕНТ ТРАНСПОРТНОЙ СЕТИ СВЯЗИ НА ОСНОВЕ ТЕХНОЛОГИИ CARRIER ETHERNET

А.В. Ануфренко[1], **А.К. Канаев**[2], **Э.В. Логин**[2*]

[1]Военная академия связи имени Маршала Советского Союза С.М. Буденного,
Санкт-Петербург, 194064, Российская Федерация
[2]Петербургский государственный университет путей сообщения Императора Александра I,
Санкт-Петербург, 190031, Российская Федерация
*Адрес для переписки: elinabeneta@yandex.ru

Информация о статье
УДК 654.027
Язык статьи – русский

Ссылка для цитирования: Ануфренко А.В., Канаев А.К., Логин Э.В. Модель воздействия злоумышленника на фрагмент транспортной сети связи на основе технологии Carrier Ethernet // Труды учебных заведений связи. 2018. Т. 4. № 3. С. 17–25.

Аннотация: *Транспортная сеть связи играет ключевую роль в обеспечении переноса разнородного трафика между узлами доступа. При этом современная пакетная технология Carrier Ethernet, реализующая ряд механизмов для контроля и управления состоянием фрагментов транспортной сети связи, не имеет встроенных механизмов защиты от целенаправленного воздействия злоумышленника. Задача, связанная с оценкой вероятностно-временных характеристик воздействия злоумышленника на сеть, функционирующей на основе упомянутой технологии, является актуальной. В статье рассмотрено ее функционирование в условиях компьютерной атаки типа «Подмена доверенного объекта». Разработана и представлена блок-схема алгоритма функционирования варианта атаки данного типа, а также представлена ее математическая модель, разработанная с помощью метода топологического преобразования стохастических сетей и с учетом профильной модели атаки.*

Ключевые слова: *транспортная сеть связи, Carrier Ethernet, компьютерная атака, подмена доверенного объекта.*

Введение

Транспортная сеть связи (ТрС) является ключевым элементом телекоммуникационной сети, функционирование которой обеспечивает требуемую безопасность управления движением на железнодорожном транспорте. При этом стоит отметить, что современной технологией, которая представляет наибольший интерес относительно применения ее принципов в ТрС, является пакетная технология Carrier Ethernet (CE).

Посредством ТрС обеспечивается перенос трафика (в том числе и служебной информации) между сетями доступа. Структура ТрС имеет распределенный и протяженный характер и может включать в себя множество сетевых элементов. При этом ТрС на основе CE обладает мощными средствами контроля состояния отдельных элементов и сети в целом, а также средствами автоматического и автоматизированного управления. Однако указанные средства управления сетями связи операторского класса не имеют самостоятельных механизмов обеспечения безопасности от воздействия компьютерной атаки (КА). Все это говорит о возможной уязвимости ее отдельных фрагментов, поскольку задача, связанная с оценкой вероятностной характеристики воздействия злоумышленника на ТрС CE, остается нерешенной.

Carrier Ethernet как объект воздействия злоумышленником

Сетевая технология Ethernet долгое время полностью отвечала требованиям ведущих операторов связи по качеству и скорости передачи информации. Однако, несмотря на все достоинства Ethernet, ее использованию в сетях операторского класса препятствовал ряд недостатков. Развитие LAN-сетей потребовало усовершенствования технологии Ethernet, что привело к разработке Ethernet операторского класса или Carrier Ethernet. В рамках стандарта IEEE 802.3 международной организацией Metro Ethernet Forum (MEF) разработаны рекомендации для технологии CE и дано

ее определение как универсальной стандартизирующей службы и сети операторского класса.

Техническим комитетом MEF в рамках технологии Carrier Ethernet описаны подходы к реализации сетевого управления и взаимодействия через сеть связи. Процессы, затрагивающие эксплуатацию, управление и обслуживание (OAM, *от англ.* Operation, Administration, Maintenance) в CE позволяют осуществлять сквозное управление неисправностями (Fault Management), управление производительностью (Performance Management), управление конфигурациями (Configuration Management), а также мониторинг параметров работы (Performance Monitoring) в нескольких взаимосвязанных сетях.

На каждом уровне управления имеется свой набор функций, взаимодействие которых позволяет эффективно управлять сетевыми процессами и взаимодействием нескольких сетей.

Одной из целевых задач реализации OAM является Fault Management, которая обеспечивает возможность обнаружения, проверки, локализации неисправностей и оповещения о проблемах с доступностью сервисов. Выполнение перечисленных функций осуществляется в соответствии со стандартами IEEE 802.1ag и IEEE 802.3ah.

Стандарт IEEE 802.1ag ассоциируется как Connectivity Fault Management (CFM) для реализации OAM в сетях с поддержанием технологии пакетных технологий. Основные механизмы CFM включают в себя набор устройств, предоставляющих услугу под управлением определенного оператора, набор элементов для осуществления процесса мониторинга параметров работы сети.

Стандарт ITU-T Y.1731 также, как и стандарт CFM (IEEE 802.1ag) позволяет выполнять функции управления неисправностями. При этом имеются особенности относительно механизмов, оповещающих об отказе, и способов рассылки служебных сообщений. В данном случае оба стандарта дополняют друг друга.

Стандарт IEEE 802.3ah [1–2] определяет функции, связанные с предоставлением информации о соединениях для передачи сообщений OAM.

Управление конфигурациями осуществляется с помощью стандарта MEF E-LMI [1–2]. Здесь выполняются такие механизмы, как периодический опрос и оповещения о статусе удаленного пользовательского интерфейса, а также оповещения о добавлении, удалении и статусе виртуального соединения.

В регламентирующих документах IEEE 802.1ag [1] и ITU-T Y.1731 [2] для управления соединениями на структуре сети определены границы ответственности (MD, *от англ.* Maintenance domain). Как показано на рисунок 1, границы могут проходить в одном месте, но не могут пересекаться. MD могут быть вложенными (до 8 уровней вложения). Например, такими MD могут быть Клиент/Оператор/Арендуемый сегмент сети. Для мониторинга доступности сервиса в MD определены Maintenance Association (MA). MA в свою очередь определяются как набор Maintenance End Points (MEP) на границах домена. Итак, MD – это группа устройств, предоставляющих услугу под управлением определенного оператора; MA – мониторинг экземпляра сервиса в пределах MD; MP – точка мониторинга, которая генерирует и отвечает на сообщения CFM. Точка MIP (*от англ.* Maintenance Domain Intermediate Point), определяет путь между MEP и место сбоя на этом пути.

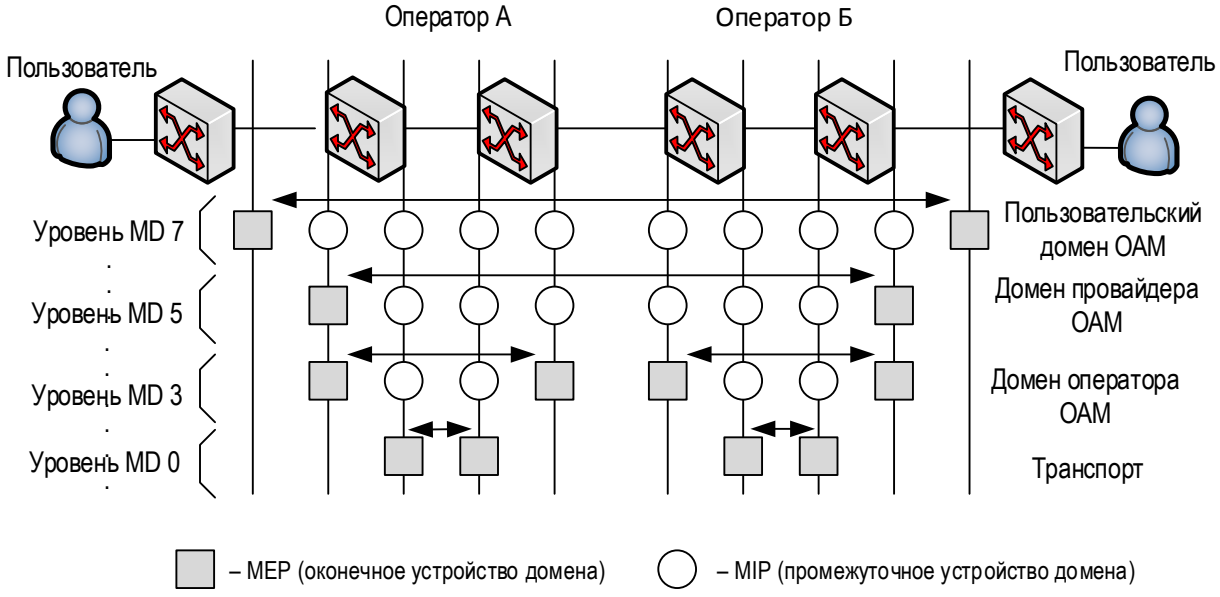

Рис. 1. Архитектура OAM Carrier Ethernet

Таким образом, указанные функции решают ряд подзадач, связанных с той или иной целевой задачей OAM (управление конфигурациями, управление отказами и управление производительностью).

Исследуемая модель системы управления СЕ, для которой существует риск реализации компьютерной атаки, содержит следующие механизмы OAM:

– механизм проверки целостности сети Ethernet (CCM, *от англ.* Continuity Check Message, – упреждающие действия OAM);

– механизм, оповещающий об отказе канала (ETH-AIS – сигнал индикации аварии), включающий сигнал аварии, который передается после обнаружения неисправности на (под)уровне сервера; проверка ширины полосы пропускания, потери кадров, битовые ошибки и т. д.;

– механизм, инициирующий сигнал, который отправляет предшествующий MEP в последующий в случае выполнения условия неисправности (ETH-RDI – индикация неисправностей на дальнем конце); таким образом, последующий MEP информируется о наличии ошибки в предшествующем MEP, при этом принимающий MEP не может определять место неисправности;

– механизм, который инициирует блокирующий сигнал ETH-LCK, который подавляет ошибки клиента и позволяет устройству данного клиента определить причину неисправности (преднаменное управление или сбор информации на серверном уровне).

Описание процесса функционирования транспортной сети связи СЕ в условиях целенаправленного воздействия

Процесс функционирования ТрС при целенаправленном воздействии программно-технических средств, реализующих компьютерную атаку (ПТС КА) представлен на рисунках 2 и 3.

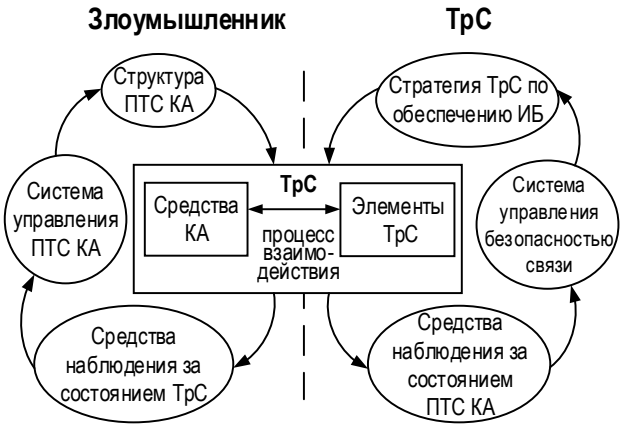

Рис. 2. Обобщенная модель функционирования ТрС в условиях целенаправленного воздействия ПТС КА

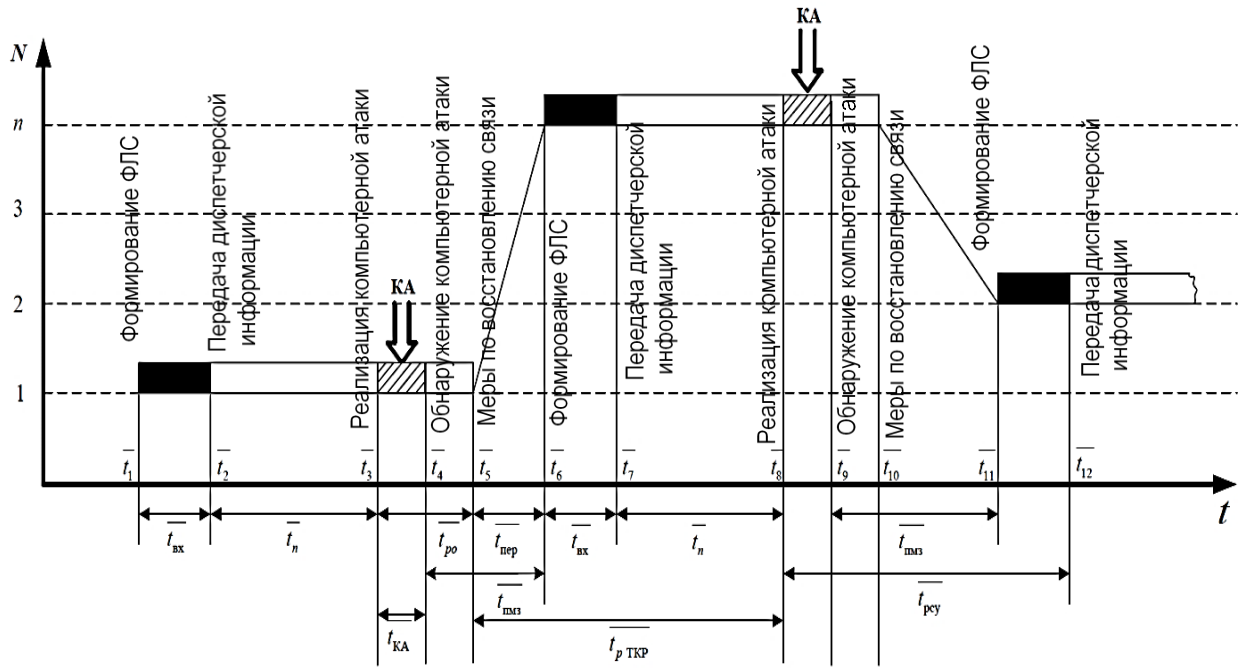

Рис. 3. Диаграмма процесса функционирования ТрС в условиях воздействия ПТС КА

В условиях так называемого информационного противоборства происходит процесс взаимодействия между ПТС КА и элементами ТрС. Злоумышленник реализует цикл воздействия на элементы ТрС, который включает непосредственное воздействие на основе определенной структуры ПТС КА, мониторинг с помощью средств наблюдения за состоянием ТрС и работу системы управления ПТС КА, обеспечивающей настройку оптимальных параметров ПТС КА с учетом данных, поступающих от средств наблюдения за состоянием ТрС. В то же время система обнаружения вторжений (СОВ) ТрС реализует цикл по обеспечению информационной безопасности (ИБ) на основе эффективной стратегии по обеспечению ИБ, мониторинг

DOI:10.31854/1813-324X-2018-4-3-17-25

с помощью средств наблюдения за состоянием ПТС КА и работу системы управления безопасностью связи (СУ), обеспечивающей настройку оптимальных параметров СОВ ТрС с учетом данных, поступающих от средств наблюдения за состоянием ПТС КА.

В этом случае эффективность функционирования ТрС в условиях воздействия на нее ПТС КА обеспечивается более оперативной реализацией цикла по обеспечению ИБ транспортной сети связи по отношению к реализации цикла воздействия программно-технических средств, реализующих компьютерную атаку.

Обобщенно работу ТрС в условиях воздействия системы КА можно представить следующим образом. Реализуется передача диспетчерской информации ($\overline{t_2}$, $\overline{t_7}$, $\overline{t_{12}}$ и т.д.), для чего сначала осуществляются процедуры формирования физического или логического соединения (ФЛС) – $\overline{t_1}$, на что затрачивается среднее время $\overline{t_{\text{вх}}}$.

Затем ($\overline{t_3}$, $\overline{t_8}$ и т.д.) ПТС КА реализует компьютерную атаку за среднее время $\overline{t_{\text{КА}}}$, которую СОВ ТрС сможет обнаружить ($\overline{t_4}$, $\overline{t_9}$ и т.д.) за среднее время $\overline{t_{\text{ро}}}$, определяемое временем реакции системы мониторинга ТрС. Обнаружив воздействие КА, система обнаружения вторжения ТрС будет принимать меры по восстановлению связи ($\overline{t_5}$, $\overline{t_{10}}$ и т.д.) за среднее время $\overline{t_{\text{пер}}}$. После этого СОВ транспортной сети связи обеспечивает формирование ФЛС ($\overline{t_6}$, $\overline{t_{11}}$ и т.д.), на что затрачивается некоторое среднее время $\overline{t_{\text{вх}}}$ и передача диспетчерской информации возобновляется.

Среднее время, затрачиваемое на принятие мер защиты формирования ФЛС ($t_{\text{пмз}}$), характеризует реакцию СУ на воздействие компьютерной атаки, то есть $\overline{t_{\text{рсу}}} = \overline{t_{\text{пмз}}} + \overline{t_{\text{вх}}} = \overline{t_{\text{пер}}} + \overline{t_{\text{ро}}} + \overline{t_{\text{вх}}}$. Среднее время от момента передачи диспетчерской информации до момента воздействия КА является временем реакции ПТС КА ($\overline{t_{\text{р ТКР}}}$) [7–10]. Реакция ПТС КА определяется временем, необходимым для обнаружения безопасного маршрута передачи диспетчерской информации после принятия мер защиты, и временем, необходимым ПТС КА для реализации повторного воздействия на идентифицированный маршрут передачи диспетчерской информации.

Интервал времени $\overline{t_{\text{КА}}}$ назовем циклом воздействия ПТС КА. В реальных условиях один цикл работы программно-технического средства, реализующего компьютерную атаку, отличается по длительности от другого. Это обусловлено тем, что составляющие циклов – время подготовки ПТС КА к работе, принятие мер защиты маршрута от компьютерной атаки, время формирования ФЛС и т.д. – имеют в общем случае различную длительность в каждом цикле.

Среднее время, затрачиваемое на принятие и реализацию мер защиты от КА (время цикла по обеспечению информационной безопасности ТрС), характеризуется реакцией СУ на воздействие КА, то есть $\overline{t_{\text{рсу}}} = \overline{t_{\text{пмз}}} + \overline{t_{\text{вх}}} = \overline{t_{\text{пер}}} + \overline{t_{\text{ро}}} + \overline{t_{\text{вх}}}$ [7–10].

Исследуемая модель функционирования ТрС в условиях целенаправленного воздействия ПТС КА рассматривается с точки зрения функционирования системы управления СЕ в условиях дестабилизирующего воздействия на нее КА. В основе цикла воздействия ПТС КА лежит компьютерная атака типа «Подмена доверенного объекта», которая представляет собой ряд подпроцессов, направленных на передачу кадров Ethernet, предназначенных для реализации некоторых функций OAM (кадр Eth-AIS, кадр CCM с информацией Eth-RDI, кадр Eth-LCK) и обеспечения успешной идентификации этих кадров системой управления СЕ, как поступивших из доверенного источника. Цикл по обеспечению ИБ транспортной сети связи включает в себя задачи по обнаружения ложных Ethernet-кадров и меры по восстановлению безопасной передачи информации по ТрС путем переключения с подвергнувшегося атаке на защищенный от КА резервный маршрут передачи.

Описание компьютерной атаки на ТрС типа «Подмена доверенного объекта»

Реализация компьютерной атаки типа «Подмена доверенного объекта» описывается с применением метода топологического преобразования стохастических сетей (ТПСС), в котором сложный процесс реализации КА декомпозируется на элементарные подпроцессы, каждый из которых характеризуется функцией распределения или средним временем выполнения процесса [10]. Этапы создания математической модели процессов реализации КА с применением ТПСС подробно изложены в [9, 10].

Определение вероятностно-временных характеристик (ВВХ) стохастической сети (СС) процесса реализации КА будем осуществлять при помощи метода двухмоментной аппроксимации.

Тогда среднее время реализации КА, определяемое как начальный момент первого порядка, описывается при помощи выражения [10]:

$$\overline{t_{\text{П}}} = -\frac{d}{ds}\left[\frac{Q(s)}{Q(0)}\right]_{s=0}, \qquad (1)$$

где $Q(s)$ – эквивалентная функция СС, которая определяется топологическим уравнением Мейсона.

Дисперсия времени реализации КА $D[t_{\text{П}}]$, определяемая как второй центральный момент, описывается выражением [8–10]:

$$D[t_{\text{П}}] = \frac{d^2}{ds^2}\left[\frac{Q(s)}{Q(0)}\right]_{s=0} - \left\{-\frac{d}{ds}\left[\frac{Q(s)}{Q(0)}\right]_{s=0}\right\}^2. \qquad (2)$$

Вычисление математического ожидания и дисперсии позволяет приближенно определить функцию распределения времени реализации КА как неполную гамма-функцию [8–10]:

$$F(t) = \begin{cases} 0, t < 0; \\ \int_0^t \frac{\mu^\alpha}{\Gamma(\alpha)} x^{\alpha-1} \exp[-\mu x] dx, t \geq 0, \end{cases} \quad (3)$$

где $\alpha = \frac{\overline{t_П}^2}{D[t_П]}$, $\mu = \frac{\overline{t_П}}{D[t_П]}$ – параметры формы и масштаба, соответственно.

Для формирования математической модели процесса функционирования КА с применением ТПСС введем следующие ограничения и допущения [7–10]:

– функция распределения случайных величин относятся к классу экспоненциальных;

– вероятности, соответствующие ветвям СС, определяются статистическими методами;

– времена реализации отдельных подпроцессов искомого процесса имеют экспоненциальное распределение;

– модель предполагает отсутствие новых заявок до окончания обработки предыдущей;

– потоки заявок являются неконкурирующими.

С целью сокращения времени реализации КА злоумышленник будет воздействовать несколькими способами. При этом одним из наиболее уязвимых мест, на которое противник будет воздействовать, является система мониторинга и система управления. Исходя из этого в процессе функционирования ТрС учитывается воздействие КА на канальном уровне СЕ.

Блок-схема алгоритма атаки показана на рисунке 4. Злоумышленник реализует компьютерную атаку типа «Подмена доверенного объекта» в следующей последовательности:

– преодолевает систему идентификации и аутентификации сообщений OAM, циркулирующих в ТрС за среднее время $t_{преод}$ с функцией распределения времени $W(t)$;

– посылает кадр Ethernet об отключении сигнала аварии (кадр Eth-AIS) за среднее время $\overline{t_{1.2.1}}$ с функцией распределения времени $D(t)$, который с вероятностью P_1 воспринимается система управления ТрС, как кадр, поступивший из доверенного источника;

– посылает кадр Ethernet о состоянии неисправности (кадр CCM с информацией Eth-RDI) за среднее время $\overline{t_{1.2.2}}$ с функцией распределения времени $L(t)$, который с вероятностью P_2 воспринимается СУ транспортной сети связи, как кадр, поступивший из доверенного источника;

– посылает кадр Ethernet об административном блокировании (кадр Eth-LCK) за среднее время $\overline{t_{1.2.3}}$ с функцией распределения времени $M(t)$, который с вероятностью P_3 воспринимается СУ ТрС, как кадр, поступивший из доверенного источника;

– кроме того, в ходе реализации КА возникают потери и искажения информации или ее блокировка иными средствами защиты, что предполагает их повторного выполнения за среднее время $\overline{t_{повт}}$ с функцией распределения времени $Z(t)$.

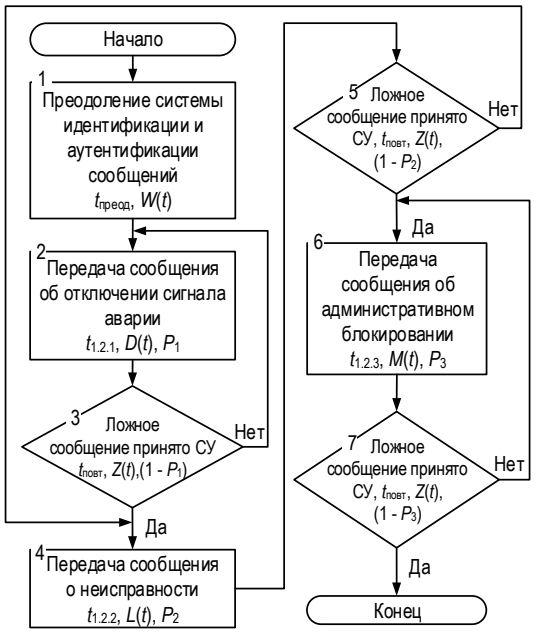

Рис. 4. Блок-схема алгоритма компьютерной атаки типа «Подмена доверенного объекта»

Разработанная математическая модель КА типа «Подмена доверенного объекта» [7, 8] в виде стохастической сети представлена на рисунке 5. Представим подпроцесс, характеризующийся функцией распределения $Q(t)$ и средним временем выполнения процесса функционирования КА, используя преобразование Лапласа [7–10].

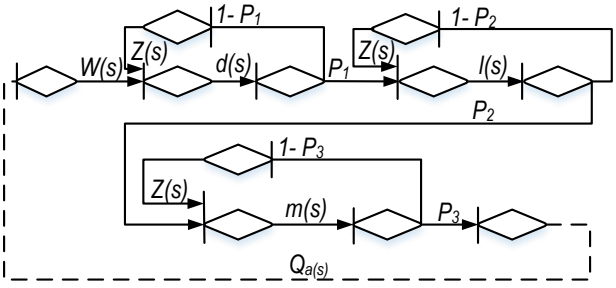

Рис. 5. Стохастическая сеть процесса реализации компьютерной атаки на ТрС через подсистему OAM

Ветви разработанной стохастической сети ($W(s)$, $m(s)$, $l(s)$, $d(s)$, $Z(s)$) описывают процессы КА в соответствии с блок-схемой алгоритма компьютерной атаки, отображенной на рисунке 4 [7–10]. На основе данной сети при использовании топологического уравнения Мейсона получена эквивалентная функция $Q(s)$, которая имеет следующий вид [8–10]:

$$F(s):=\frac{\frac{w}{w+s}\cdot\frac{d}{d+s}\cdot\frac{1}{1+s}\cdot\frac{m}{m+s}\cdot P1\cdot P2\cdot P3}{1-\frac{z}{z+s}\cdot\left[(1-P1)\cdot\frac{d}{d+s}+(1-P2)\cdot\frac{1}{1+s}+(1-P3)\cdot\frac{m}{m+s}\right]+}$$
$$+\left(\frac{z}{z+s}\right)^2\cdot\left[\begin{array}{c}(1-P1)\cdot(1-P2)\cdot\frac{d}{d+s}\cdot\frac{1}{1+s}+(1-P1)\cdot(1-P3)\\ \cdot\frac{1}{1+s}\cdot\frac{m}{m+s}+(1-P2)\cdot(1-P3)\cdot\frac{d}{d+s}\cdot\frac{m}{m+s}\end{array}\right]- \quad (4)$$
$$-\left(\frac{z}{z+s}\right)^3\cdot(1-P1)\cdot(1-P2)\cdot(1-P3)\cdot\frac{d}{d+s}\cdot\frac{1}{1+s}\cdot\frac{m}{m+s}.$$

Результаты расчетов $F(t)$, $\overline{t_{KA}}$, полученные с помощью выражений (1–3) представлены на рисунках 6–8. В качестве исходных данных используются значения параметров времени реализации КА, приведенных в [8]: $\overline{t_{\text{преод}}}$ = 5 мин; $\overline{t_{1.2.1}}$ = 5 мин; $\overline{t_{1.2.2}}$ = 5 мин; $\overline{t_{1.2.3}}$ = 5 мин; $P1$ = 0,9; $P2$ = 0,9, $P3$= 0,9.

На рисунке 6а представлены результаты моделирования в виде функции распределения времени реализации КА для разных значений вероятности $P1$ восприятия СУ транспортной сети связи кадра Eth-AIS, посланного ПТС КА, как кадра, поступившего из доверенного источника. На рисунке 6а показано, что с увеличением значения вероятности $P1$ значительно возрастает вероятность успешной реализации КА за то же время.

На рисунке 6 представлены функции распределения времени реализации КА для разных значений вероятности $P1$ при изменении вероятности $P2$ восприятия системы управления ТрС кадра ССМ с информацией Eth-RDI, посланного ПТС КА, как кадра, поступившего из доверенного источника.

Из графиков (рисунок 6) видно, что при осуществлении КА несколькими способами, реализуемыми последовательной цепочкой, рост вероятности успешной реализации каждого из способов компьютерной атаки ведет к значительному росту вероятности принятия СУ ложной информации.

На рисунке 7а представлены результаты моделирования в виде функции распределения времени реализации КА для разных значений времени $\overline{t_{1.2.1}}$ посылки кадра Eth-AIS. Из рисунка видно, что вероятность принятия СУ ложной информации зависит от времени передачи ПТС компьютеной атаки кадра Eth-AIS. С увеличением времени $\overline{t_{1.2.1}}$вероятность успешной реализации КА уменьшается.

На рисунке 7б представлены результаты моделирования, из которых видно, что рост времени $\overline{t_{\text{повт}}}$ повторного выполнения рассматриваемой КА уменьшает вероятность ее успешной реализации, когда атака продолжается более 20 мин и увеличивает, когд атака продолжается менее 20 мин.

На рисунке 7в показаны результаты моделирования в виде функции распределения времени реализации КА для разных значений времени $t_{\text{преод}}$ преодоления системы идентификации и аутентификации сообщений, циркулирующих в ТрС. Вероятность успешной реализиации КА увеличивает уменьшение времени $t_{\text{преод}}$.

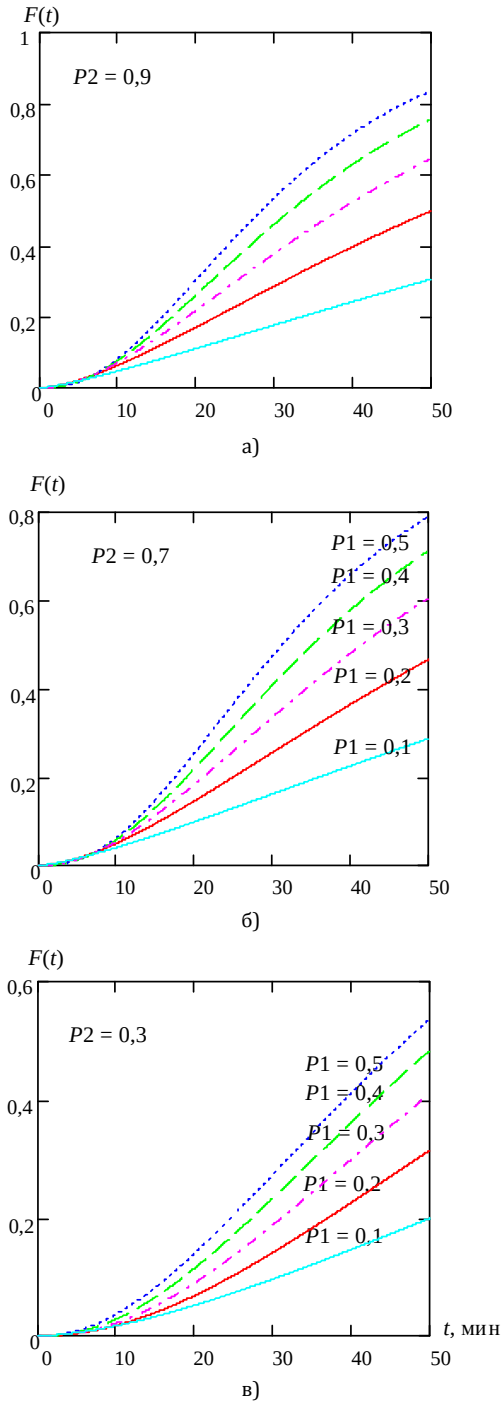

Рис. 6. Зависимость интегральной функции распределения вероятности принятия СУ ложной информации от времени реализации компьютерной атаки при вероятности восприятия СУ ТрС кадра ССМ, как кадра, поступившего из доверенного источника, равна: а) 0,9; б) 0,7; в) 0,3

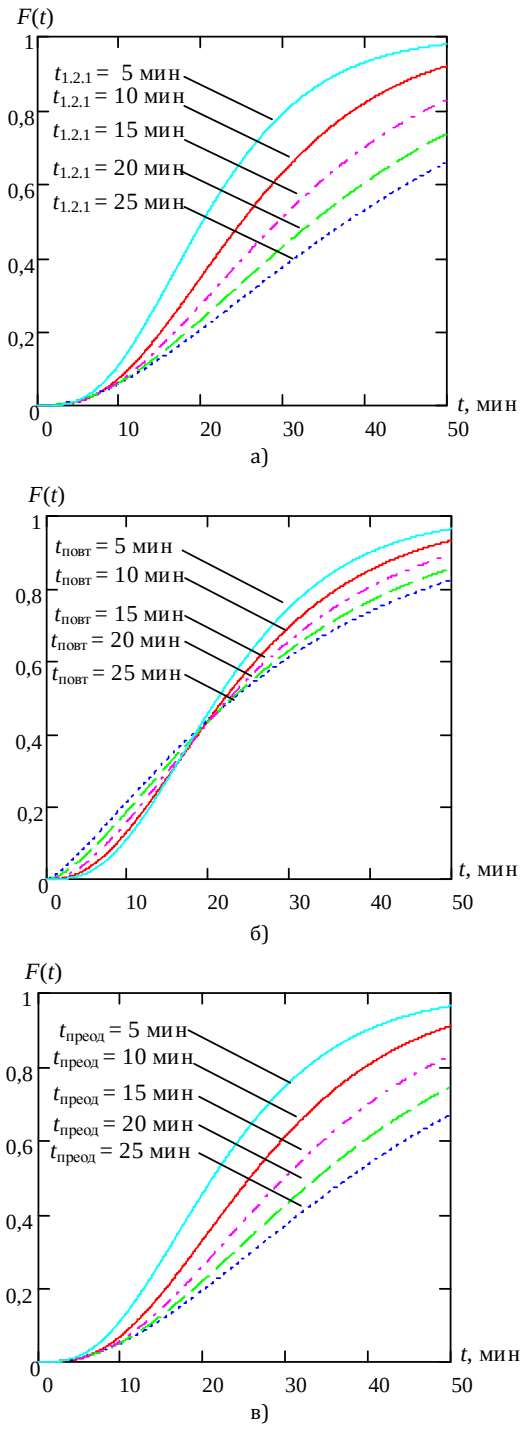

Рис. 7. Зависимость интегральной функции распределения вероятности принятия СУ ложной информации от времени реализации компьютерной атаки при различных значениях времени: а) посылки кадра Eth-AIS; б) повторного выполнения КА; в) преодоления системы идентификации и аутентификации сообщений, циркулирующих в ТрС

Представленные на рисунках 6 и 7 графики иллюстрируют изменение длительности реализации КА на транспортной сети связи СЕ для различных вероятностей установления данного воздействия при изменении интегральной функции (комплексная оценка всех этапов компьютерной атаки), давая возможность определить вероятность $P_n(t \le T_з)$ решения задачи по подмене доверенного объекта за время не более заданного $T_з$. Это позволяет оценивать эффективность функционирования ТрС СЕ в условиях воздействия КА и обоснованно задавать требуемые временные характеристики реализации КА с целью перспективного моделирования механизмов защиты ТрС СЕ.

Разработанная математическая модель дает возможность определения различных функциональных зависимостей времени реализации КА от изменения ее параметров. Так, например, с помощью модели можно определить среднее время $t(P1)$ реализации КА (рисунки 8 и 9).

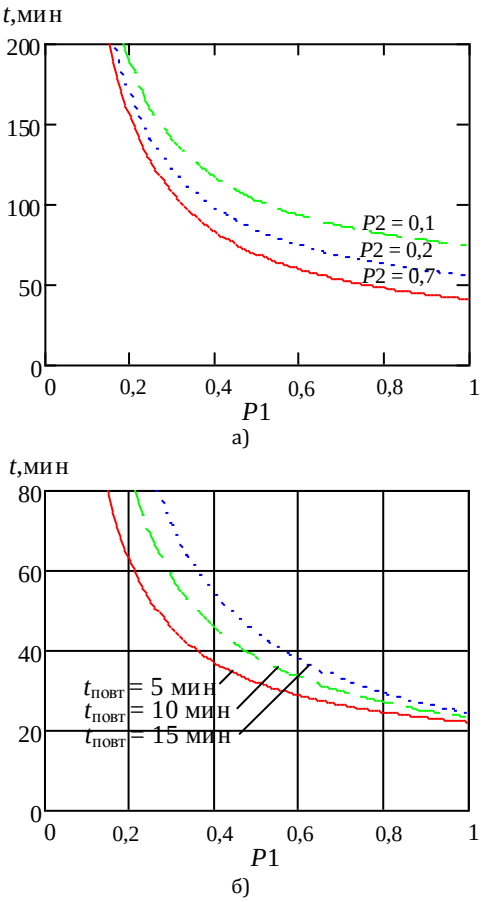

Рис. 8. Зависимость среднего времени реализации компьютерной атаки от вероятности восприятия СУ ТрС кадра Eth-RDI, как кадра, поступившего из доверенного источника: а) при различной вероятности восприятия СУ ТрС кадра ССМ, как кадра, поступившего из доверенного источника; б) при различных значениях времени повторного выполнения КА

Графики на рисунке 8а демонстрируют зависимость среднего времени реализации КА от вероятности восприятия системы управления ТрС кадра Eth-RDI, как кадра, поступившего из доверенного источника при разной вероятности выполнения процесса передачи кадра ССМ системой ПТС КА. Из графиков видно, что рост $P1$ и $P2$ ведет к снижению времени успешной реализации КА. Низкое значение $P1$ (0 – 0,2) снижает чувствительность разработанной модели КА к изменению $P2$ вероятности восприятия СУ ТрС кадра ССМ, как кадра, поступившего из доверенного источника.

DOI:10.31854/1813-324X-2018-4-3-17-25

Графики на рисунке 8б демонстрируют зависимость среднего времени реализации КА от вероятности восприятия СУ ТрС кадра Eth-RDI, как кадра, поступившего из доверенного источника при разных значениях времени повторного выполнения КА. Из графиков видно, что высокое значение $P1$ (0,8 – 1) ведет к снижению чувствительности разработанной модели КА к времени $\overline{t_{повт}}$ повторного выполнения рассматриваемой КА.

На рисунке 9а показаны результаты моделирования, демонстрирующие зависимость среднего времени реализации компьютерной атаки от вероятности восприятия СУ ТрС кадра Eth-RDI, как кадра, поступившего из доверенного источника при разных значениях времени преодоления системы идентификации и аутентификации сообщений, циркулирующих в ТрС. Низкое значение $P1$ (0 – 0,2) снижает чувствительность разработанной модели КА к изменению времени $t_{преод}$ преодоления системы идентификации и аутентификации сообщений.

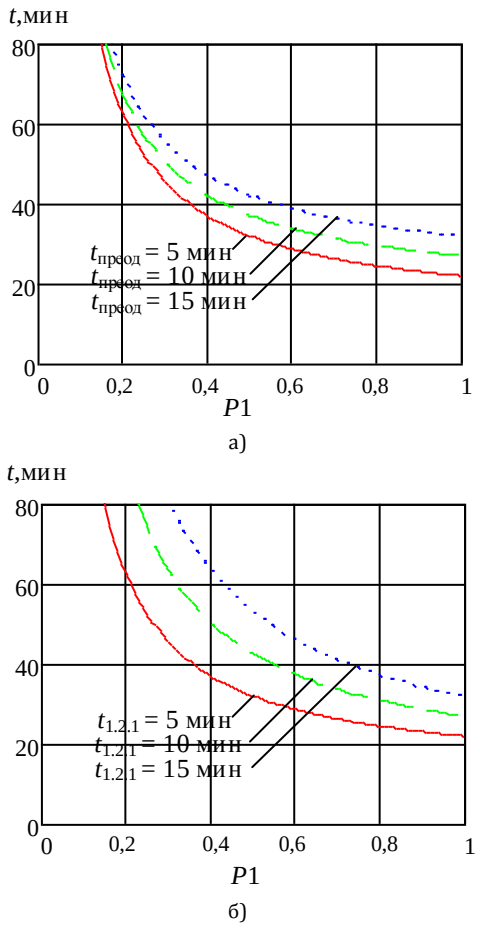

Рис. 9. Зависимость среднего времени реализации компьютерной атаки от вероятности восприятия СУ ТрС кадра Eth-RDI, как кадра, поступившего из доверенного источника при разных значениях времени: а) преодоления системы идентификации и аутентификации сообщений, циркулирующих в ТрС; б) посылки кадра Eth-AIS

На рисунке 9б показаны результаты моделирования, демонстрирующие зависимость среднего времени реализации компьютерной атаки от вероятности восприятия СУ ТрС кадра Eth-RDI, как кадра, поступившего из доверенного источника при разных значениях времени посылки кадра Eth-AIS. Разработанная модель КА остается чувствительна ко времени $\overline{t_{1.2.1}}$ посылки кадра Eth-AIS при любых значениях вероятности $P1$.

Таким образом, можно сделать общий вывод: при возникновении условий, позволяющих увеличить вероятность подмены доверенного объекта, в разы уменьшается время реализации КА. Также это позволяет формировать исходные данные по реализации КА типа «Подмена доверенного объекта» в ТрС СЕ для перспективных исследований в области разработки механизмов защиты транспортной сети связи СЕ от целенаправленных воздействий злоумышленника. Анализ полученных результатов показывает, что математическая модель типа «Подмена доверенного объекта» работоспособна, чувствительна к изменению входных данных.

Выводы

ТрС является ключевым элементом телекоммуникационной сети с точки зрения управления и обеспечения безопасности функционирования железнодорожного транспорта. При этом технология СЕ представляет наибольший интерес относительно применения ее принципов в ТрС.

Важным местом относительно воздействия злоумышленника на ТрС является система мониторинга и управления, на которые злоумышленник будет воздействовать сразу несколькими способами. Причем одним из основных видов воздействия является КА типа «Подмена доверенного объекта».

Составляющие каждого цикла функционирования ПТС КА имеют различную длительность, что требует разработки математических моделей КА для их учета при анализе реакции ПТС КА и затрат времени для реализации мер защиты ТрС от КА. Таким образом для разработки модели КА типа «Подмена доверенного объекта» используются профильные модели атак и метод ТПСС.

Разработанные модели КА помогают обоснованно задавать требуемые временные характеристики реализации КА с целью перспективного моделирования механизмов защиты ТрС СЕ, а также позволяют формировать исходные данные по реализации КА типа «Подмена доверенного объекта» в ТрС СЕ для перспективных исследований в области разработки механизмов защиты ТрС СЕ от целенаправленных воздействий злоумышленника.

Учитывая тот факт, что рассмотренный тип компьютерной атаки является лишь одним из основных вариантов воздействия злоумышленника на ТрС, задачи разработки моделей КА представляют дальнейший интерес.

DOI:10.31854/1813-324X-2018-4-3-17-25

Список используемых источников

1. IEEE 802.1ag Connectivity Fault Management.
2. ITU-T Y.1731 OAM functions and mechanisms for Ethernet based networks.
3. Ануфренко А.В., Волков Д.В., Канаев А.К. Принцип организации узла агрегации мультисервисной сети связи // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция: сборник научных статей в 2 томах. 2015. Т. 1. С. 203–206.
4. Степанов С.Н. Основы телетрафика мультисервисных сетей. М.: Эко-Трендз, 2010. 392 с.
5. Цыбаков В.И. Разработка и исследование метода расчета качества обслуживания пользователей широкополосной интегрированной мультисервисной корпоративной сети: дис. канд. техн. наук. М., 2005. 174 с.
6. Боев В.Д., Сыпченко Р.П. Компьютерное моделирование. Элементы теории и практики: учеб. пособие. СПб.: ВАС, 2009. 436 с.
7. Ануфренко А.В., Канаев А.К. Предложения по обоснованию требований к характеристикам оборудования узлов пакетной транспортной сети связи // T-COMM: Телекоммуникации и транспорт. 2018. Т. 12. № 2. С. 47–54.
8. 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: ЛО ЦНИИС, 2014. 126 с.
9. Привалов А.А. Метод топологического преобразования стохастических сетей и его использования для анализа систем связи ВМФ. СПб.: ВМА, 2001. 186 с.
10. Привалов А.А., Карабанов Ю.С., Королев А.И., Кириленко В.О. Разработка структуры программного комплекса моделирования информационного конфликта системы безопасности телекоммуникационного объекта РЖД с подсистемой нарушителя // Интеллектуальные системы на транспорте: материалы V Международной научно-практической конференции «ИнтеллектТранс-2015». 2015. С. 327–332.

* * *

MODEL OF THE ATTACKER'S INFLUENCE ON A FRAGMENT OF TRANSPORT COMMUNICATION NETWORK BASED ON THE CARRIER ETHERNET TECHNOLOGY

A. Anufrenko[1], A. Kanaev[2], E. Login[2]

[1]Telecommunications Military Academy,
St. Petersburg, 194064, Russian Federation
[2]PGUPS of the Emperor Alexander I,
St. Petersburg, 190031, Russian Federation

Article info
Article in Russian

For citation: Anufrenko A., Kanaev A., Login E. Model of the Attacker's Influence on a Fragment of a Transport Communication Network Based on the Carrier Ethernet Technology // Proceedings of Telecommunication Universities. 2018. Vol. 4. Iss. 3. PP. 17–25.

Abstract: *The transport communication network plays a key role in ensuring the transfer of traffic between access nodes. At the same time, modern Carrier Ethernet network technology, which implements a number of mechanisms for monitoring and managing the state of the transport communication network fragments, does not have built-in protection mechanisms against the targeted attack of the attacker on the communication network. In this regard, the task associated with the evaluation of the probability-time characteristics of the attacker's attack on the transport communication network, functioning on the basis of Carrier Ethernet technology, is actualized. The article examines the functioning of the Carrier Ethernet transport network in terms of the impact on the computer-style attack "Substitution of the trusted object." A block diagram of the algorithm of the computer attack of this type will be revealed, as well as its mathematical model developed taking into account the profile model of the attack and the method of topological transformation of stochastic networks.*

Keywords: *transport communication network, Carrier Ethernet, computer attack, substitution of the trusted object.*