УДК 004.49.5

А.А. Смирнов, А.К. Дидык, А.Н. Дреев, С.А. Смирнов

Кировоградский национальный технический университет, Кировоград

СПОСОБ КОНТРОЛЯ ЛИНИЙ СВЯЗИ ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ ОБЛАЧНОГО АНТИВИРУСА

Данная статья посвящена разработке и оценке способа контроля линий связи телекоммуникационной системы облачного антивируса. Новизна способа контроля линий связи ТКС заключается в учете «скомпрометированных» бит данных специальных сигнатур, передаваемых в облачные антивирусные системы. Это позволит снизить вероятность манипуляций метаданными, передаваемыми в узлы программного сервера.

Ключевые слова: *информационно-телекоммуникационные сети, облачные антивирусы.*

Введение

Постановка проблемы исследования. Авторами предложен метод безопасной маршрутизации метаданных в облачные антивирусные системы. Основными составляющими метода являются:

– алгоритмы формирования множества маршрутов передачи метаданных;

– способ контроля линий связи ТКС;

– модели системы нейросетевых экспертов безопасной маршрутизации.

Данная статья посвящена способу контроля линий связи телекоммуникационной системы облачного антивируса.

Новизна способа контроля линий связи ТКС заключается в учете «скомпрометированных» бит данных специальных сигнатур, передаваемых в облачные антивирусные системы. Это позволит снизить вероятность манипуляций метаданными, передаваемыми в узлы программного сервера.

Основная часть

Исследования процесса обслуживания информационных пакетов метаданных в многопротокольном маршрутизаторе ТКС показали, что основными его элементами, влияющими на вероятностно-временные показатели качества обслуживания являются: коммутатор, депакетизатор, блок управления маршрутизатором, запоминающее устройство буфер памяти) и анализатор линий связи (рис. 1.) [11 – 17].

Отличительной особенностью представленного маршрутизатора является включение в его состав анализатора линий связи и ассоциативного блока нейросетевых экспертов, построенного на основе нейронной сети АРТ-1. Указанные блоки выполняют задачи мониторинга канала связи и управления процессом маршрутизации в условиях возможных злоумышленных подключений. В предлагаемом алгоритме безопасной маршрутизации такие блоки предполагается использовать в каждом узле связи (УС) телекоммуникационной системы. Для того чтобы маршрутизатор мог функционировать, необходимо сформировать информацию о состоянии соединений, исходящих из данного узла.

Каждому соединению присваивается определённый вектор параметров, компоненты которого характеризуют определённую составляющую физического соединения. Одними из важнейших параметров, которые необходимо учитывать при выборе дальнейшего пути маршрутизации информации, является тип канала связи, его пропускная способность и функциональная безопасность.

Для некоторых каналов связи характеристики, используемые для выбора маршрутов при передаче метаданных в облачные антивирусные системы, приведены в табл. 1.

Параметры пропускной способности и функциональной безопасности представляются значениями в интервале от 0 до 1, которые характеризуют тип канала и кабеля связи по сравнению с параметрами, выбранными в качестве эталонных и имеющими максимальные значения пропускной способности и функциональной безопасности.

Формирование обучающей выборки для системы экспертов производится путём анализа линии связи, которая используется в рассматриваемой локальной сети. Вторжение может быть осуществлено путём прямого подсоединения к каналу связи и считывании информации с помощью технических средств. Вследствие этого должна быть возможность определения попыток подключения к каналу.

Следует заметить, что основная опасность подобного рода злоумышленных вторжений приходится на неконтролируемые участки ТКС, то есть участки глобальных и региональных сетей, в которых чаще всего используются каналы типа Е-1 и Е-2.

Проведенные исследования показали, что в настоящее время, несмотря на высокую стоимость и сложность, существует принципиальная возможность подсоединения к волоконнооптической линии связи (ВОЛС) и несанкционированного доступа к данным, передаваемым по указанным каналам связи. Способы несанкционированного доступа можно классифицировать по двум группам (рис. 2).

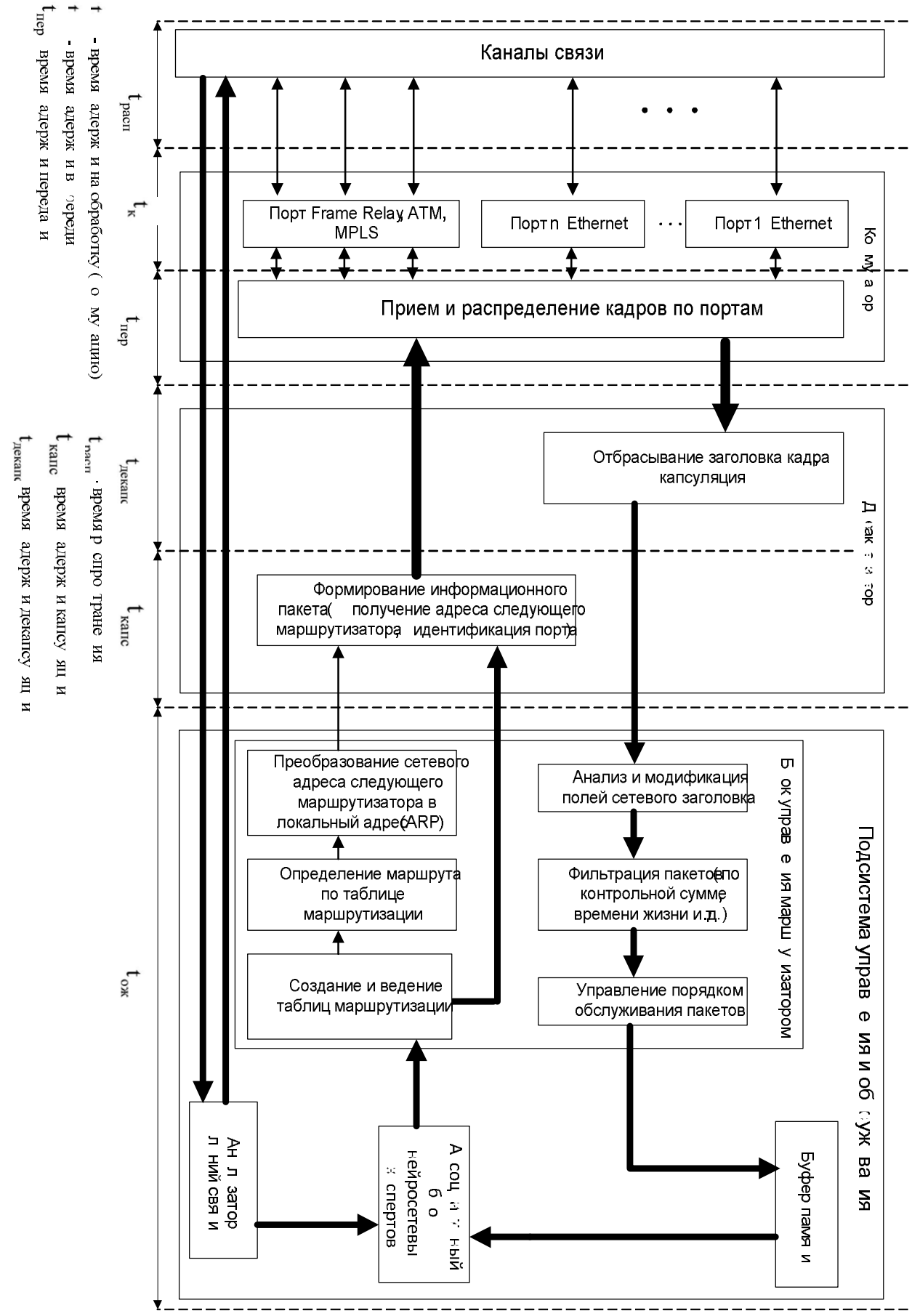

Рис. 1. Структурная схема многопротокольного маршрутизатора

Таблица 1

Характеристики, используемые для выбора маршрутов при передаче метаданных в облачные антивирусные системы

Анализируемая характеристика				
Пропускная способность			Функциональная безопасность	
Тип канала	Скорость передачи	Параметр пропускной способности	Тип кабеля	Параметр функциональной безопасности
Ethernet	10 Мбит/с	0,8	Коаксиальный кабель	
Ethernet	100 Мбит/с	0,9	«Толстый» коак. кабель	0,31
Ethernet	1000 Мбит/с	0,95	«Тонкий» коак. кабель	0,22
Канал Т-1	1,544 Мбит/с	0,45	Телевизионный кабель	0,15
Канал Т-2	6,312 Мбит/с	0,61	Витая пара	
Канал Т-3	44,736 Мбит/с	0,85	Экранированная	0,6
Канал Т-4	274 Мбит/с	0,93	Неэкранированная	0,5
Канал 56	56 Гбит/с	0,33	Волоконно-оптический	
Канал Е-2	8,488 Гбит/с	0,65	Многомодовый	0,8
Канал Е-1	2,048 Тбит/с	0,55	Одномодовый	1,0

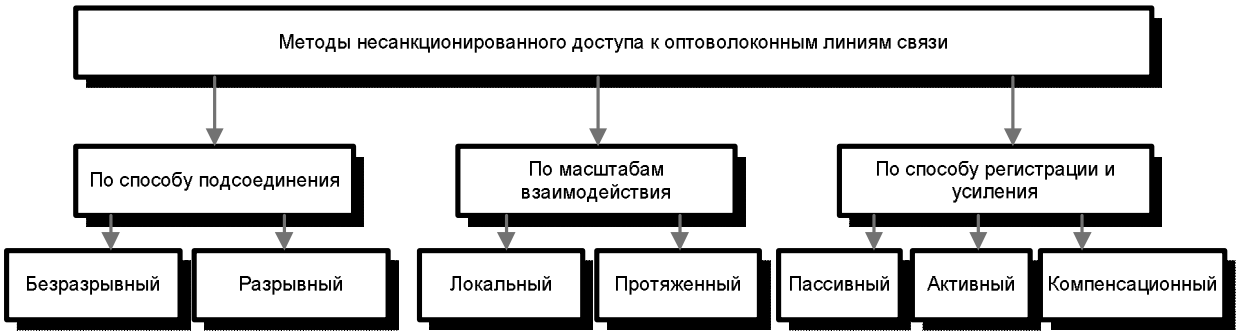

Рис. 2. Способы несанкционированного доступа к ВОЛС

Наиболее опасными, с точки зрения съема метаданных, передающихся на программные сервера (анализаторы метаданных) представляются разрывные способы несанкционированного доступа. Используя данный способ, злоумышленник имеет широкий спектр возможных воздействий на облачную антивирусную систему в целом, начиная от простого перехвата, заканчивая подменой метаданных. Устройства разрывного несанкционированного доступа позволяют осуществлять более надежный съем данных. Однако разрывное подключение требует временного отключения линий связи, что может послужить сигнализацией о наличии злоумышленного вторжения (несмотря на возможные попытки злоумышленников маскировки такой атаки).

Более незаметным по возможности обнаружения, конечно, является безразрывный способ подсоединения. В этом способе для съема сигнала используется излучение, возникающее естественным образом в результате рассеяния света на муфтах, соединителях, устройствах ввода и вывода оптической мощности, самом оптическом волокне. При этом возможно использование пассивных, активных и компенсационных способов регистрации данных.

Пассивные способы обладают высокой скрытностью, так как практически не меняют параметров распространения излучаемого сигнала в ВОЛС. Однако этот способ имеет недостатки, связанные с низкой чувствительностью. Поэтому для перехвата метаданных злоумышленники могут использовать участки, на которых уровень бокового излучения повышен. Даже после формирования стационарного распределения поля в волокне небольшая часть рассеянного излучения все же проникает за пределы

оболочки и может быть каналом утечки передаваемых метаданных.

Возможные причины излучения и рассеивания в ВОЛС и, соответственно, атак несанкционированного доступа к ВОЛС представлены на рис. 3.

Как показали исследования, активные способы позволяют получить сигнал большей мощности и, соответственно повысить эффективность атаки несанкционированного доступа к ВОЛС. Однако при этом происходит изменение параметров (мощности) распространяющегося по ВОЛС сигнала, что также облегчает возможность обнаружения атаки.

Анализ способов съема данных с ВОЛС показал, что для выполнения данной операции на физическом уровне какого-либо участка, можно использовать локальное воздействие на его волоконные световоды. При таком воздействии изменяются их оптические свойства, что и приводит к «вытеканию» сигнала. Методов воздействия на волокно можно перечислить несколько:

– изгиб волокна;
– изменение диаметра волокна (например, путем давления)
– микроизгибы волокна;
– акустическое воздействие на волокно;
– воздействие химическими реактивами.

Проведенные исследования показали, что из этих методов одним из наиболее эффективных для злоумышленников является метод изгиба волокна (позволяет организовать направленный вывод излучения). Изменяя радиус изгиба волокна, злоумышленник может добиться снятия таких величин оптической мощности, которой ему будет вполне достаточно для перехвата метаданных

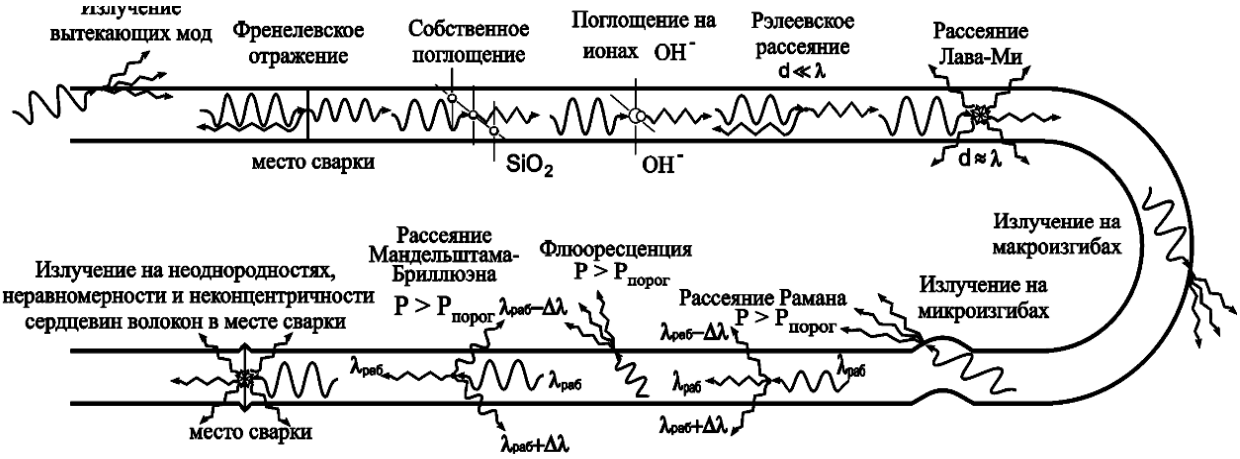

Рис. 3. Причины несанкционированного доступа к ВОЛС

Однако, следует заметить, абсолютно незаметным этот метод не является. Поскольку мощность отводится принудительно, то подключение вызовет снижение уровня мощности на приемной стороне линии. Поэтому основным методом обнаружения этого способа несанкционированного доступа является контроль над уровнем мощности на приемной стороне. Если устройство контроля обнаруживает ее снижение, то оно делает вывод о наличии несанкционированного доступа к ВОЛС и может принять решение о перенаправлении метаданных на программные сервера по другому маршруту.

Проведенные исследования показали, что аппаратура, расположенная на стороне программного сервера контроля и анализа метаданных в облачных антивирусных системах, кроме основных своих функций должна включать в себя систему контроля и обнаружения несанкционированного доступа. В задачу этой системы должны входить: наблюдение за состоянием ВОЛС, контроль принимаемого сигнала и передача его в интеллектуальный ассоциативный блок нейросетевых решений, в котором и принимается решение о наличии несанкционированного доступа к ВОЛС.

Анализ литературы [6, 7] показал, что основными показателями эффективности, используемыми при решении поставленных задач являются:

– вероятность обнаружения – $P_{обн}$;
– вероятность ложного срабатывания – $P_д$;
– объем информации, перехватываемой нарушителем – k (бит).

Если значения этих показателей лежат в рамках допустимых порогов, то данная система является эффективной.

Проведем анализ функционирования рассматриваемой телекоммуникационной системы облачной антивирусной защиты и выясним факторы, влияющие на ее эффективность.

Обозначим через s_0 состояние ВОЛС в отсутствие несанкционированного доступа, а через s_1 – состояние ВОЛС при данном злоумышленном воздействии. Задачей анализатора линий связи (рис. 1) является определение момента изменения состояния ВОЛС.

Из работ [1 – 17] известно, что сигнал, поступающий на вход приемника облачной антивирусной системы, представляет собой последовательность бит, выраженных в виде импульсов света. Параметрами этих импульсов являются их длительность, уровень оптической мощности, а также функция распределения этой мощности. Подключение к линии внешних несанкционированных устройств, вызовет изменения в этих параметрах. Принимаемая оптическая мощность снизится, соответственно, изменится и ее распределение.

Аппаратура детектирования в приемнике облачной антивирусной системы работает с достаточно мощными оптическими сигналами, и потому соотношение «сигнал/шум» для нее будет большим. Эмпирически, в тестовом режиме несложно провести анализ его работы в условиях обмена метаданными и команд передачи управления программному клиенту, и найти зависимость между изменением принимаемой оптической мощности и вероятностями обнаружения и ложного срабатывания.

Следует заметить, что системы анализа (анализаторы) передаваемого сигнала являются одними из простых диагностических систем. На приемной стороне (серверной части) облачного антивируса анализируется прошедший сигнал. В случае проведения кибератаки (несанкционированного доступа) происходит фиксация изменений мощности сигнала.

Одним из основных недостатков подобного рода систем является отсутствие данных о координате (временной характеристике) появившейся аномалии. Это повышает вероятность ложных срабатываний в системе. На рис. 4 наглядно иллюстрируется данная ситуация.

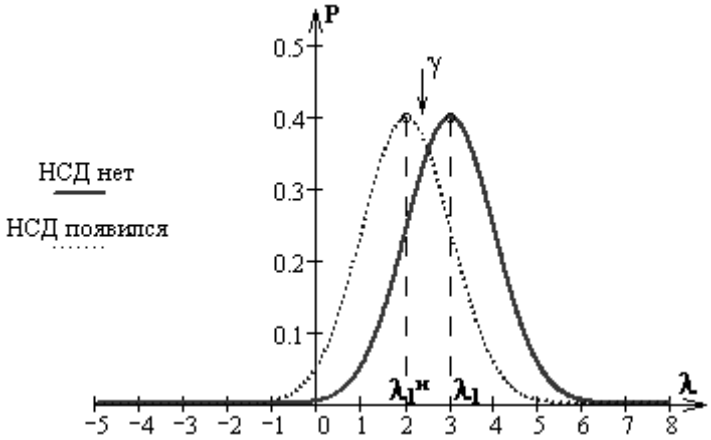

Рис. 4. График распределения вероятности для оптической мощности на легальном приемнике при наличии и отсутствии аномалии

При появлении аномалии оптическая мощность снижается, и математическое ожидание величины Z становится равным $\lambda_1^{(y)}$, а ее дисперсия – $\dfrac{\sigma_1 y^2}{N}$.

Как видно из графика рис. 4., наряду с правильным обнаружением злоумышленных вторжений в линии связи, использование одного анализатора без дополнительных «интеллектуальных» средств обнаружения допускает ситуацию ложного обнаружения или пропуска аномалий. Это может произойти, если уровень мощности сигнала станет меньше (либо больше) порогового значения γ под влиянием каких либо объективных факторов (например, старение оборудования).

В работах [6, 7] для расчета вероятностей ложного обнаружения или пропуска аномалий предлагается использовать выражения:

$$P_{ло} = \frac{1}{\sqrt{2\pi}\dfrac{\sigma_1}{\sqrt{N}}} \int_{-\infty}^{\gamma} e^{\frac{-(z-\lambda_1)^2}{2\sigma_1^2/N}} dz; \qquad (1)$$

$$P_{проп} = \frac{1}{\sqrt{2\pi}\dfrac{\sigma_1^н}{\sqrt{N}}} \int_{-\infty}^{\gamma} e^{\frac{-(z-\lambda_1^н)^2}{2(\sigma_1^н)^2/N}} dz, \qquad (2)$$

где $\lambda_1^н$ и $\left(\sigma_1^н\right)^2$ – математическое ожидание и дисперсия случайных величин y_i при наличии несанкционированного доступа.

Для устранения указанного недостатка разобьем передаваемые данные на множество участков одинаковой длительности N бит. При этом исследуем величину y_i – параметр уровня сигнала в i-й момент времени. Пусть данная случайная характеристика отвечает нормальному закону распределения:

$$P(y_i) = \frac{1}{\sqrt{2\pi}\sigma_i} e^{\frac{-(y-\lambda_i)^2}{2\sigma_i}}, \qquad (3)$$

где λ_i, σ_i – математическое ожидание и дисперсия случайной величины y_i соответственно.

Сумму величин y_i, определяемых в анализаторе линий связи для всех y_i, соответствующих положи-

тельным импульсам, обозначим как Z и сравним с порогом γ::

$$Z = \frac{1}{N}\sum_{j=1}^{N} y_j , \qquad (4)$$

где N – интервал анализа.

По результатам такого сравнения в системе нейросетевых экспертов принимается решение о наличии несанкционированного доступа. Если атаки не обнаруживается, то этот процесс повторяется для следующего интервала N.

Statechart-диаграмма, иллюстрирующая данный процесс, представлена на рис. 5.

На этой диаграмме определяется состояние анализатора ВОЛС в процессе передачи метаданных.

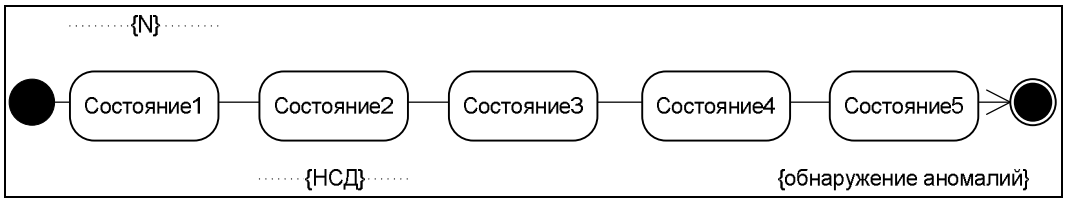

Рис. 5. Statechart-диаграмма, иллюстрирующая процесс обнаружения аномалий в процессе передачи метаданных

Из диаграммы видно, что последовательность передающихся бит данных разбивается на участки одинаковой длительности N бит ($N_1 \ldots N_5$). В некоторый момент времени (состояние 2) проходит атака несанкционированного доступа к ВОЛС. Этот момент приходится на некоторый бит участка N_2. Система должна принять решение, что начиная с этого бита, все остальные себя скомпрометировали (изменили параметры).

Учет этого факта позволяет на участке N_5, отстоящем от участка N_2 в общем случаем на Т участков, анализатору обнаружить аномалию в принятом сигнале.

Пусть х – число бит, переданных в ВОЛС после проведенной кибератаки («скомпрометированных») на интервале N_2.

Тогда общее число «скомпрометированных» бит данных будет равно:

$$X_i = x_i + N \cdot T + T_{ра}, \qquad (5)$$

где $T_{ра}$ – время, распространения данных о сигнале аномалий.

Данные о числе скомпрометированных бит необходимо использовать при пересчете количества метаданные, перенаправляемых по новому нескомпрометированному маршруту.

Таким образом, разработан способ контроля линий связи телекоммуникационной системы, отличающийся от известных введением процедуры учета «скомпрометированных» бит данных специальных сигнатур, передаваемых в облачные антивирусные системы.

Использование данного способа позволит выявлять изменение характеристик ВОЛС в процессе функционирования ТКС, (получить необходимые данные для начала процедуры обучения нейронных экспертов) и выдавать необходимые сигналы аномалий (возможных кибератак) в линиях связи в систему нейросетевых экспертов безопасной маршрутизации.

Это позволит снизить вероятность манипуляций метаданными, передаваемыми в узлы программного сервера.

Выводы

Для постоянного мониторинга и решения задачи переформатирования маршрутов связи с узлом программного сервера разработан способ контроля линий связи ТКС.

Использование данного способа позволит выявлять изменение характеристик ВОЛС в процессе функционирования ТКС, (получить необходимые данные для начала процедуры обучения нейронных экспертов) и выдавать необходимые сигналы аномалий (возможных кибератак) в линиях связи в систему нейросетевых экспертов безопасной маршрутизации.

Отличительной особенностью предложенного способа является введение процедуры учета «скомпрометированных» бит данных специальных сигнатур, передаваемых в облачные антивирусные системы.

Это позволит снизить вероятность манипуляций метаданными, передаваемыми в узлы программного сервера.

Список литературы

1. Narvfiez P. New Dynamic Algorithms for Shortest Path Tree Computation / Paolo Narvfiez, Kai-Yeung Siu, Hong-Yi Tzeng // IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 8, NO. 6, DECEMBER 2000 / Электронный вариант Режим доступа: http://akira.ruc.dk/~keld/ teaching/ algoritmedesign_ f08/Artikler/07/Narvaez00.pdf.

2. Партыка С.А. Метод ускоренной коррекции spt с использованием динамических алгоритмов / С.А. Партыка // Электронный вариант Режим доступа: .http:// openarchive.nure.ua/bitstream/123456789/936/1/ASU_158_2 012%20%2842-47%29.pdf.

3. Гмурман В.Е. Теория вероятностей и математическая статистика / В.Е. Гмурман. – М.: Высшая школа, 200 – 479 с.

4. Семенов С.Г. Защита данных в компьютеризированных управляющих системах / С.Г. Семенов, В.В. Давыдов, С.Ю. Гавриленко. – LAP Lambert Academic Publishing GmbH & Co. KG (Саарбрюккен, Германия), 2014. – 236 с.

5. Семенов С.Г. Разработка распределенного метода многопутевой маршрутизации, основанного на потоковой модели с предвычислением путей (маршрутов) / С.Г. Семенов, А.Г. Беленков, А.А. Можаев // Моделювання та інформаційні технології. – К.: ІПМЕ ім. Г.Є. Пухова. – 2005. – Вип. 32. – С. 189-192.

6. Манько А. Защита информации в волоконно-оптических линиях связи от несанкционированного доступа / А. Манько, В. Котюк, М. Задорожний // науково-технічний збірник НТУУ "КПІ" "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні". – 2001. –Вип. 2.– С. 249-255.

7. Все об оптоволокне (подборка из статей) / Электронный вариант Режим доступа: http://pst-proekt. ru/tech/vse_ob_optovolokne.pdf.

8. Лавренков Ю.Н. Разработка алгоритма адаптивной маршрутизации на основе нейронечеткого иммунного подхода / Л.Г. Комарцова, Ю.Н Лавренков // Сборник трудов десятого международного симпозиума «Интеллектуальные системы». – М., 2012. – С. 272 -276.

9. Лавренков, Ю.Н. Нейронечеткнй иммунный алгоритм для оптимизации параметров радиальнобазисной нейронной сети / Ю.Н. Лавренков // Сб. матлов Всероссийской научн.-технич. конф.: Наукоемкие технологии в приборо- и машиностроении и развитии инновационной деятельности в ВУЗЕ. – М.: Издательство МГТУ им. Н.Э. Баумана. –Том 2. – 2011. – С. 217-221.

10. Обзор научно-технической литературы по АРТ-методам. Электронный ресурс. – Режим доступа: http:// fullref.ru/job_7d20c5db5ea838ce3ad648ed743a4630.html.

11. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А.А. Смирнов, А.В. Коваленко, С.А. Смирнов // Системи обробки інформації. – Х.: ХУПС, 2014. – Вип. 9(125). – С. 105-110.

12. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Абу Таам Гани, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. – Х.: ХУПС, 2014. – Вип. 4 (41). – С. 48-52.

13. Смирнов С.А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Абу Таам Гани, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України. – Випуск 4(17). – Х.: ХУПС. – 2014. – С.90-95.

14. Смирнов С.А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Системи обробки інформації. – Х.: ХУПС, 2015. – Вип. 1(126). – С. 150-15.

15. Smirnov S.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – Volume 5, Issue 5. – India. Delhi. – 2015. – P. 1-7.

16. Смирнов С.А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты данных / Мохамад Абу Таам Гани, А.А. Смирнов, С.А. Смирнов // Системи озброєння і військова техніка. – – Х.: ХУПС, 2015. – Вип. 3(43). – С. 100-107.

17. Смирнов С.А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А.А. Смирнов, С.А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України. – Х.: ХУПС, 2015. – Вип. 3(20). – С. 134-141.

Поступила в редколлегию 8.02.2016

Рецензент: д-р техн. наук, проф. И.В. Рубан, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

СПОСІБ КОНТРОЛЮ ЛІНІЙ ЗВ'ЯЗКУ ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ХМАРНОГО АНТИВІРУСУ

О.А. Смірнов, А.К. Дідик, А.М. Дрєєв, С.А. Смірнов

Дана стаття присвячена розробці та оцінці способу контролю ліній зв'язку телекомунікаційної системи хмарного антивірусу. Новизна способу контролю ліній зв'язку ТКС полягає в обліку «скомпрометованих» біт даних спеціальних сигнатур, переданих в хмарні антивірусні системи. Це дозволить знизити ймовірність маніпуляцій метаданими, переданими в вузли програмного сервера.

Ключові слова: *інформаційно-телекомунікаційні мережі, хмарні антивіруси.*

METHOD FOR CONTROL LINE COMMUNICATION SYSTEM TELECOMMUNICATION CLOUD ANTIVIRUS

A.A. Smirnov, A.K. Didyk, A.N. Dreyev, S.A. Smirnov

This article focuses on the development and evaluation of a method of controlling communication lines telecommunication system of the cloud antivirus. The novelty of the method of controlling the communication lines TKS is taken into account "compromised" bit special signature data transmitted in the cloud antivirus system. This will reduce the possibility of manipulation of metadata transmitted in the application server nodes.

Keywords: *information and communication networks, cloud antivirus.*