УДК 004.49.5

Мохамад Абу Таам Гани, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов

Кировоградский национальный технический университет, Кировоград

УСОВЕРШЕНСТВОВАННЫЙ АЛГОРИТМ УПРАВЛЕНИЯ ДОСТУПОМ К «ОБЛАЧНЫМ» ТЕЛЕКОММУНИКАЦИОННЫМ РЕСУРСАМ

Предложен алгоритм управления доступом к «облачным» телекоммуникационным ресурсам, отличающийся от известных введением нестандартных условий принятия решения о присвоении «эталонного» приоритета информационному пакету на основе дополнительного показателя – вероятности присвоения приоритета. Это дает возможность решить задачу минимизации времени обработки информационных пакетов метаданных при их передаче в «облачные» антивирусные системы при обеспечении заданного качества обслуживания других информационно-телекоммуникационных услуг.

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

Постановка проблемы исследования

В настоящее время в современных информационно-телекоммуникационных системах (ИТС) в процессе их эксплуатации возникает множество нештатных ситуаций, обусловленных нестационарностью входной нагрузки, конечной надежностью и отказоустойчивостью ее элементов, внешними дестабилизирующими воздействиями, требующими автоматических или стационарных управляющих вмешательств в процесс функционирования системы.

Для решения прикладных задач сетевого управления и разработки соответствующих аппаратных или программных средств и приложений остаются актуальными вопросы математического моделирования технологий и процессов, сопровождающих информационный обмен (маршрутизации, коммутации, управления и др.).

Помимо этого, у пользователей ИТС все большим спросом пользуются услуги облачных антивирусных систем. Связано это во многом, с одной стороны, с динамическим развитием сетевых технологий, а с другой – ростом реальных угроз зловредного программного обеспечения, справиться с которым стационарные антивирусные системы не в состоянии [1 – 10]. Поэтому большое развитие получили в последнее время облачные антивирусы. Облачные антивирусы являются комплексами из клиентского приложения и веб-сервиса. Обе части антивируса работают совместно. Клиент – это небольшая программка, которая работает на компьютере пользователя и сканирует систему, проверяя, не заражена ли она вредоносным кодом. Известно, что традиционные антивирусные программы, устанавливаемые на компьютер, являются «пожирателями ресурсов», но клиентские программы облачных антивирусов требуют намного меньше вычислительной мощности [7 – 11].

Веб-сервис облачного антивируса располагается в Интернете, на одном или нескольких серверах. Большую часть задач по обработке данных выполняет именно он, поэтому компьютеру пользователя не приходится ни обрабатывать, ни хранить значительные объемы информации. Через определенные промежутки времени программа-клиент сканирует компьютер. Суть сканирования состоит в поиске вредоносного кода, информация о котором есть в базе данных веб-сервиса [7 – 11]. Теперь перечислим те преимущества, которыми обладает облачный антивирус в сравнении с традиционным [7 – 11]:

– программа-клиент имеет доступ к самым свежим данным о вредоносном коде спустя всего несколько минут после того, как о нем «узнал» веб-сервис. Нет необходимости постоянно обновлять антивирусное программное обеспечение;

– программа-клиент очень мала и довольствуется небольшой вычислительной мощностью. Следовательно, она не отвлекает компьютер от других выполняемых им задач;

– облачные антивирусы бесплатны. Впрочем, обновления, дополнительные утилиты и поддержка предлагаются за деньги.

Теперь, когда мы узнали о том, что представляет собою облачное антивирусное программное обеспечение, рассмотрим те функции, которые выполняет типичный облачный антивирус [7 – 11].

Интерфейс пользователя облачного антивируса не вызовет серьезных вопросов ни у кого из тех, кто имеет опыт использования традиционных антивирусных программ. И работу он выполняет ту же: сканирует компьютер, выявляет вредоносный код и чистит от него систему [7 – 11]. Перечислим основные функции, доступные в пользовательском интерфейсе облачного антивируса [7 – 11]:

– Сканирование всего компьютера или отдельных папок.

– Возможность настройки автоматического режима сканирования с указанием тех файлов, которые следует включить в область сканирования.

– Просмотр подробного отчета о том, какой вредоносный код был обнаружен в процессе сканирования.

– Действия по удалению или восстановлению файлов, помещенных в карантин или файлов, которые были обезврежены тем или иным способом.

В этих основных функциях отличий от традиционного антивируса не наблюдается. Но есть те возможности, которые свойственны исключительно облачным антивирусным сервисам. Как уже говорили, облачный антивирус распределяет выполнение своих задач между компьютером пользователя (программа-клиент) и удаленным веб-сервером (или несколькими серверами), доступ к которому осуществляется через Интернет [7 – 11].

Таким образом, часть ресурсов является «общей» для всех пользователей. Это не только вычислительные мощности серверов, но и центральная база данных, содержащая данные о вредоносном коде. Эта база данных составляется различными способами. Для каждого продукта характерны свои методы ее пополнения.

Облачные базы данных отличаются не только методиками сбора информации. Реальным преимуществом облачных антивирусов является та скорость, с которой они способны обеспечить защиту от новых угроз [7 – 11]. В облачных антивирусах предусмотрена также возможность кеширования базы данных на компьютере для дальнейшего использования в офлайн-режиме. Разумеется, в этом случае база будет содержать данные по состоянию на момент ее сохранения. Этот кеш может обновляться во время выхода компьютера в Интернет. Но он не содержит полный перечень информации о вредоносном коде, только о наиболее распространенных угрозах [7 – 11].

Процесс информационного обмена оконечных рабочих станций с узлами, предоставляющими услуги облачной антивирусной защиты, представляет собой четко организованную функциональную структуру, являющуюся совокупностью алгоритмов формирования сигнатур, транспортировки, коммутации, маршрутизации и обработки специализированными анализаторами.

Таким образом, **актуальной научной задачей** является усовершенствование алгоритма управления доступом к соответствующим «облачным» телекоммуникационным ресурсам.

Алгоритм управления доступом к «облачным» телекоммуникационным ресурсам

Для решения поставленной в первом разделе оптимизационной задачи повышения оперативности обработки информационных пакетов в интеллектуальных узлах коммутации при их передаче в «облачные» антивирусные системы предлагается усовершенствовать алгоритм управления доступом к соответствующим «облачным» телекоммуникационным ресурсам. В основу рассматриваемого алгоритма положена процедура вычисления виртуального времени обработки информационных пакетов, отличающаяся от известных учетом фактора введения дополнительного уровня приоритезации для информационных пакетов метаданных [1 – 6]. При этом указанные информационные пакеты получают наивысший приоритет обработки в интеллектуальных узлах коммутации класса r_1.

В табл. 1 представлены допустимые значения среднего времени и джиттера времени обработки информационных пакетов различного уровня приоритетности в интеллектуальных узлах коммутации.

Таблица 1

Допустимые значения среднего времени и джиттера времени обработки информационных пакетов различного уровня приоритетности

Уровень приоритета	$r_3 = \overline{J+1,R}$	$r_2 = \overline{2,J}$	$r_1 = 1$
$T_{доп}^{[i]}$, мс	100-800	50-150	1-10
$J_{доп}^{[i]}$, мс	47-53	10-30	1-5

Структурная схема алгоритма управления доступом к «облачным» телекоммуникационным ресурсам представлена на рис. 1.

На первом шаге в рассматриваемой структурной схеме осуществляется проверка нахождения пакетов на входе интеллектуального узла коммутации. При их отсутствии – алгоритм переходит в режим ожидания поступающих пакетов.

В случае, когда на вход интеллектуального узла коммутации информационные пакеты поступили (всех уровней приоритезации или только отдельных), необходимо выполнить выбор из каждой очереди буфера памяти интеллектуального узла коммутации по одному первому пакету $r_1 = 1$, $r_2 = \overline{2,J}$ и $r_3 = \overline{J+1,R}$ уровня приоритетности для определения «эталонного» информационного пакета с соответствующим уровнем приоритетности. Это позволит сократить время обработки информационных пакетов метаданных при обеспечении заданных показателей оперативности обработки информационных пакетов других уровней приоритетности.

На четвертом шаге рассматриваемом алгоритме определяется значение VST и VFT. Далее приступаем к выполнению процедур выявления информационного пакета для обработки в обслуживающем устройстве интеллектуального узла коммутации. При этом учитывается следующее: на вход буферного устройства может поступать N пакетов (N – количество очередей в системе) r_1, r_2 и r_3 уровней приоритетности.

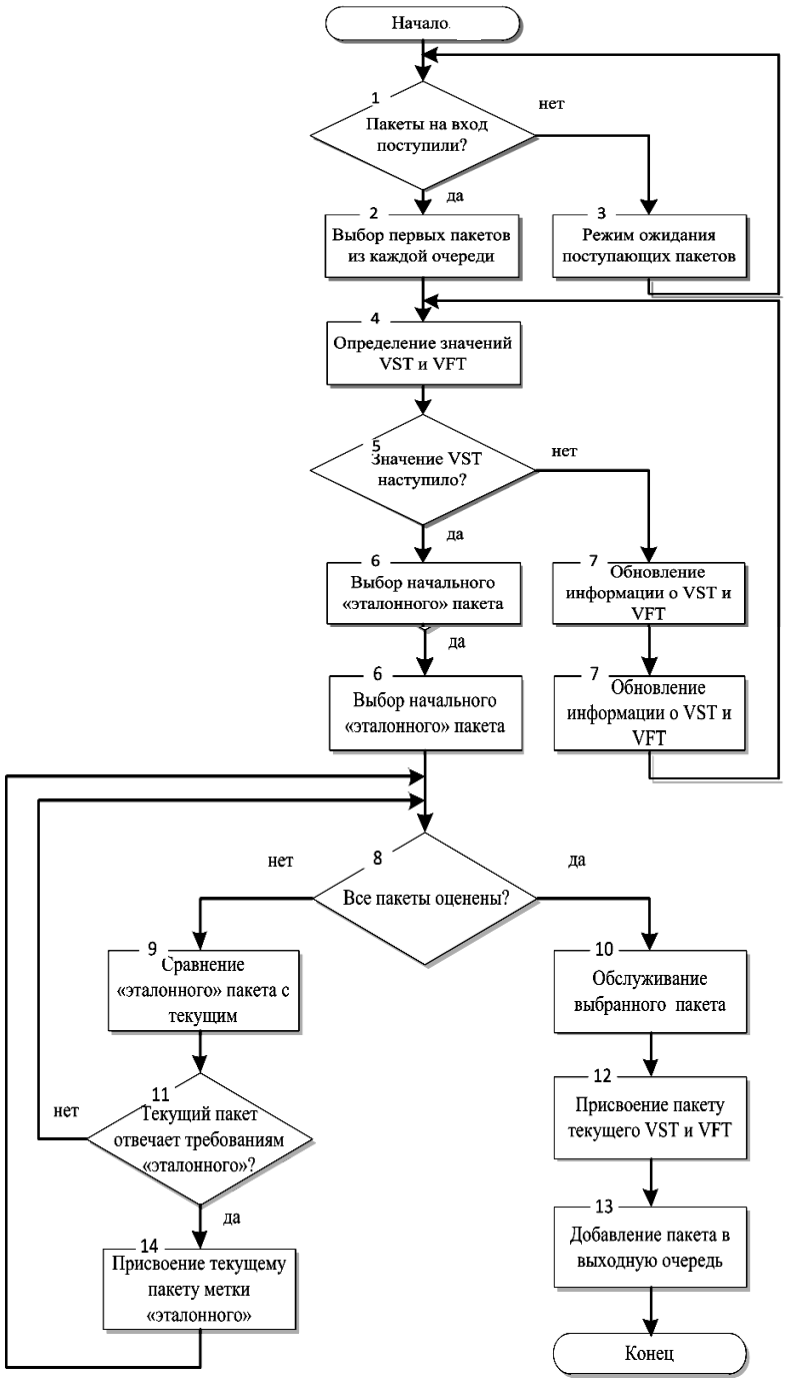

Рис. 1. Структурная схема алгоритма управления доступом к «облачным» телекоммуникационным ресурсам

Если значение VST наступило, то на шаге 6 из информационного потока выбирается первый («эталонный») пакет, с некоторым $N_{приор}$, а также значением виртуального времени обслуживания в очереди – VFT.

Далее на шаге 9 структурной схемы производится сравнение «эталонного» информационного пакета с другими поступившими на данный момент времени. При этом решение о присвоении «эталонного» приоритета информационному пакету принимается по следующим критериям:

1) минимальное значение виртуального времени обслуживания в очереди (VFT = min);

2) принадлежность информационного пакета к очереди с максимальным приоритетом ($r_1 > r_2 > r_3$).

Следует заметить, что условие присвоения «эталонного» приоритета на шаге 14 выполняется не в полном объеме, а с некоторыми исключениями, определяемыми заранее заданным показателем, например показателем $P_{присв}$ – вероятности присвоения приоритета [1 – 6]. Данный показатель может быть определен эмпирическим путем. При этом процедура управления с помощью данного показателя является отличительной особенностью рассматриваемого алгоритма управления доступом к «облачным» телекоммуникационным ресурсам.

Данные исключения необходимы для обеспечения качества обслуживания информационных пакетов других (низших) приоритетов. Информационные пакеты можно сравнивать попарно, при этом в начальный момент времени первый выбранный информационный пакет условно обладает высшим уровнем приоритетности. Если условие, определяемое на шаге 5, не наступило, то на шаге 7 алгоритма происходит обновление информации о VST и VFT.

На шаге 10 происходит переход непосредственно к процедурам обработки информационных пакетов. На шаге 12 информационному пакету присваиваются текущие значения VST и VFT с целью дальнейшего сопровождения информационного пакета к пункту назначения. Далее на шаге 13 информационный пакет добавляется в выходную очередь и заканчивается процесс его обработки в интеллектуальном узле коммутации.

Выводы

Таким образом, разработан алгоритм управления доступом к «облачным» телекоммуникационным ресурсам, отличающийся от известных введением нестандартных условий принятия решения о присвоении «эталонного» приоритета информационному пакету на основе дополнительного показателя – вероятности присвоения приоритета. Это дает возможность решить задачу минимизации времени обработки информационных пакетов метаданных при их передаче в «облачные» антивирусные системы при обеспечении заданного качества обслуживания других информационно-телекоммуникационных услуг.

Список литературы

1. Давыдов В.В. Сравнительный анализ моделей распространения компьютерных вирусов в автоматизированных системах управления технологическим процессом [Текст] / В.В. Давыдов // Системи обробки інформації. – Х.: ХУПС, 2012. – Вип. 3(101), т. 2. – С. 147-151.

2. Семенов С.Г. Математическая модель распространения компьютерных вирусов в гетерогенных компьютерных сетях автоматизированных систем управления технологическим процессом [Текст] / С.Г. Семенов, В.В. Давыдов // Вісник НТУ «ХПІ». Інформатика та моделювання. – Х.: НТУ «ХПІ», 2012. – Вип. 38. – С. 163-171.

3. Математическая GERT-модель технологии передачи метаданных в облачные антивирусные системы / В.В. Босько, А.А. Смирнов, И.А. Березюк, Мохамад Абу Таам Гани // Системи обробки інформації. – Х.: ХУПС, 2014. – Вип. 1(117). – С. 137-141.

4. Смирнов А.А. Структурно-логическая GERT-модель технологии распространения компьютерных вирусов / А.А. Смирнов, И.А. Березюк, Мохамад Абу Таам Гани // Системи управління, навігації та зв'язку. – Полтава: ПНТУ, 2014. – Вип.1(29). – С. 120-125.

5. Smirnov A.A. Experimental studies of the statistical properties of network traffic based on the BDS-statistics / A.A. Smirnov, D.A. Danilenko // International Journal of Computational Engineering Research (IJCER). – India. Delhi. – 2014. – Volume 4, Issue 5. P. 41-51.

6. Кузнецов А.А. Дисперсионный анализ сетевого трафика для обнаружения и предотвращения вторжений в телекоммуникационных системах и сетях / А.А. Кузнецов, А.А. Смирнов, Д.А. Даниленко // Системи обробки інформації". – Х.: ХУПС, 2014. – Вип. 2(118). – С. 124-133.

7. Matrosov A. Stuxnet under microscope. [Электронный ресурс] / A. Matrosov, E. Rodionov, D. Harley. – Режим доступа к ресурсу: http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.

8. Zesheng Chen. Modeling the spread of active worms. INFOCOM 2003. [Электронный ресурс] / Zesheng Chen, Lixin Gao, Kevin Kwait. – Режим доступа к ресурсу: http://www.ieee-infocom.org/2003/papers/46_03.PDF.

9. Rohloff K. Stochastic Behavior of Random Constant Scanning Worms [Text] / K. Rohloff, T. Basar // Computer Communications and Networks, 2005. ICCCN 2005. Proceedings. 14th International Conference on 17-19 Oct. 2005. – P. 339-344.

10. Williamson M.M. Epidemiological model of virus spread and cleanup. HPL-2003-39. [Электронный ресурс] / M.M. Williamson, J. Leveille. – Режим доступа к ресурсу: http://www.hpl.hp.com/techreports/2003/HPL-2003-39.pdf.

11. Добвня О. Как работают облачные антивирусы. [Электронный ресурс] / О. Добвня. − Режим доступа к ресурсу: http://hi-news.ru/software/fakty-kak-rabotayut-oblachnye-antivirusy.html.

Поступила в редколлегию 13.11.2014

Рецензент: д-р техн. наук, проф. А.А. Можаев, Национальный технический университет «ХПИ», Харьков.

УДОСКОНАЛЕНИЙ АЛГОРИТМ УПРАВЛІННЯ ДОСТУПОМ ДО «ХМАРНИХ» ТЕЛЕКОМУНІКАЦІЙНИХ РЕСУРСІВ

Мохамад Абу Таам Гані, О.А. Смірнов, М.С. Якименко, С.А. Смірнов

Запропоновано алгоритм управління доступом до «хмарних» телекомунікаційних ресурсів, що відрізняється від відомих введенням нестандартних умов прийняття рішення про присвоєння «еталонного» пріоритету інформаційного пакету на основі додаткового показника – ймовірності присвоєння пріоритету. Це дає можливість вирішити задачу мінімізації часу обробки інформаційних пакетів метаданих при їх передачі в «хмарні» антивірусні системи при забезпеченні заданої якості обслуговування інших інформаційно-телекомунікаційних послуг.

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

ADVANCED ALGORITHM CONTROL ACCESS TO THE "CLOUD" OF TELECOMMUNICATION RESOURCES

Mohamad Abou Taam, A.A. Smirnov , M.S. Yakimenko, S.A. Smirnov

An algorithm is proposed to control access to the "cloud" of telecommunications resources, characterized by the introduction of non-standard conditions known to a decision on awarding a "standard" priority information package on the basis of an additional parameter - the probability of assigning priority. This makes it possible to solve the problem of minimizing the processing time of data packets during transmission of metadata in the "cloud" antivirus systems while providing a specified quality of service information and other telecommunication services.

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