УДК 004.49.5

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

*Кировоградский национальный технический университет, Кировоград*

# ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ МЕТОДА УПРАВЛЕНИЯ ДОСТУПОМ К ОБЛАЧНЫМ АНТИВИРУСНЫМ ТЕЛЕКОММУНИКАЦИОННЫМ РЕСУРСАМ

*В статье производится выбор показателя эффективности управления доступом к облачным антивирусным телекоммуникационным ресурсам. На основе результатов математического и имитационного моделирования проводится выбор показателя вероятности присвоения приоритета для определения «эталона» приоритета и оценка эффективности метода управления доступом к облачным телекоммуникационным ресурсам для обеспечения антивирусной защиты данных. Обосновывается достоверность результатов математического моделирования, и предлагаются практические рекомендации по использованию разработанного метода.*

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

## Постановка проблемы исследования

В работах [1-7] описано достаточно широкий спектр показателей качества обслуживания, которые в совокупности представляют собой некоторую функцию, отражающую свойство антивирусной безопасности системы с одной стороны, а с другой стороны характеризующую эффективность функционирования ТКС. К их числу относятся следующие показатели качества обслуживания, которые согласно рекомендации МСЭ-Т G.1010 рассматриваются как наиболее важные:

– производительность сети;

– потери пакетов;

– время передачи данных;

– вариация задержки (джиттер).

В работах [1-7] определена возможность каждого из приведенных показателей влияния на выбранную функцию характеризующую выполнение требований информационной и функциональной безопасности в случае воздействия на систему злоумышленного программного обеспечения – $B_i^{(TKC)}$.

В то же время в условиях использования облачных средств антивирусного программного обеспечения на приведенную функцию безопасности в большей степени влияют показатели производительности сети, время передачи данных и вероятность потери пакетов.

Под производительностью ТКС понимается свойство сети обеспечивать с заданными вероятностно-временными характеристиками качества обслуживания передачу от отправителей к получателям требуемого объёма данных [8].

Проведенные исследования показали, что к основным показателям производительности сети относят эффективную, пиковую, устойчивую и минимальную скорости передачи, измеряемые, как правило, в бит/с. Для упрощения исследований определим, что минимальное значение производительности обычно гарантируется поставщиком услуг, который, в свою очередь, должен иметь гарантии от сетевого провайдера. Параметры, связанные с эффективной скоростью передачи могут быть определены через дескриптор трафика IP-сети, который описан в рекомендации МСЭ-Т Y. 1221 [9].

В ходе исследования необходимо учитывать влияние потерь пакетов, которые, как правило, вызваны не столько ошибками передающей среды, сколько возможными перегрузками в сети по пути следования данных.

Значительный уровень потерь пакетов приводит к падению общей производительности сети и, как следствие, к неудовлетворительному качеству работы приложений. Количественно чувствительность к потерям и ошибкам оценивается через следующие показатели:

– коэффициент потерь пакетов IP (IP packet loss ratio, IPLR);

– коэффициент ошибок пакетов IP (IP packet error ratio, IPER).

Учет и оценка данного показателя наиболее наглядно демонстрируют преимущества того или иного метода управления телекоммуникационными ресурсами $r_2 = \overline{2,J}$ и $r_3 = \overline{J+1,R}$ уровней приоритетности. Но поскольку в рамках исследования большее внимание уделяется обслуживанию информационных пакетов $r_1$ уровня приоритетности оценивать эффективность разработанного метода целесообразнее по следующему показателю – показателю времени передачи информационных пакетов.

В соответствии с рекомендациями МСЭ-Т Y. 1540 [9] время передачи пакетов является основным параметром, характеризующим доставку пакетов IP-сети, и выражается через параметр задержки IPTD (IP packet transfer delay), который определяется как время доставки пакета между источником и получателем для всех пакетов – как успешно переданных, так и пакетов с ошибками.

Из ряда научных работ [10-14] известно, что одной из основных составляющих времени передачи информационных пакетов является время ожидания в очереди и время обслуживания информационных пакетов (далее оба показателя объединим в общее время обработки) в интеллектуальных узлах коммутации. В условиях использования облачных антивирусных систем данный показатель во многом определяет уровень информационной и функциональной безопасности как отдельных средств телекоммуникации так и ТКС в целом

Именно поэтому с целью оценки эффективности разработанных алгоритмов и метода было проведено их сравнение с ранее известным, наиболее эффективным решением (алгоритмом управления очередями в многопротокольных интеллектуальных маршрутизаторах $WF^2Q$), как с уже получившими протокольную реализацию. При этом количественный анализ адекватности разработанных моделей управления трафиком проводился путём сравнения результатов аналитического, имитационного моделирования и натурного эксперимента.

## Разработка имитационной модели системы управления доступом к облачным телекоммуникационным ресурсам

Одним из ключевых этапов исследования является синтез полученных знаний в единую систему антивирусной защиты данных и разработка имитационной модели данной системы. При этом их целью должно быть решение следующих частных задач:

– проверка адекватности разработанных моделей и метода управления доступом к облачным телекоммуникационным ресурсам;

– анализ достоверности полученных результатов в ходе решения поставленных оптимизационных задач;

– обоснованный выбор показателей, коэффициентов и характеристик функционирования системы, а также оценка по ним эффективности разработанного метода;

– выработка научно-практических рекомендаций по использованию моделей и метода управления доступом к облачным телекоммуникационным ресурсам в современных и перспективных информационных системах.

Для обоснования достоверности полученных результатов и оценки эффективности метода управления доступом к облачным телекоммуникационным ресурсам было проведено имитационное моделирование. В качестве инструментария имитационного моделирования использовано среду символьной математики MathCAD-14, специализированные программы распределения доступа в мультисервисных маршрутизаторах для передачи сигнатур и данных [8, 15, 16].

В состав программного комплекса имитационного моделирования входят две системы, выполняющие отдельные функции:

– выбора показателей, ограничений и критериев оптимизации процесса доставки метаданных в облачные антивирусные системы, а также выработки соответствующих управляющих сигналов (команд);

– определения допустимых вероятностно-временных характеристик передачи и обработки метаданных в облачных антивирусных системах

– выработки решений о способах защиты данных и оптимального управления коммутационными ресурсами в процессе передачи метаданных в облачные антивирусные системы.

Следует заметить, что для генерации злоумышленного программного обеспечения использовалось несколько известных генераторов: «Generator DAT Virusov», «Raptor Virus Generator», Nowhere Man «Virus Creation Laboratory» и др.

В процессе формирования требований к информационной безопасности ТКС и допустимых вероятностно-временных показателей передачи и обработки метаданных в облачных антивирусных системах эмулировались и рассматривались различные характеристики информационного обмена, типы системного программного обеспечения, различные способы архитектурного построения ТКС.

В частности, рассматривались следующие варианты:

– разнотиповость операционных систем;

– связность сети, количество функциональных узлов и связи между ними;

– интенсивность информационного обмена.

Сбор входной информации о загрузке сетевого устройства осуществлялся с помощью стандартного программного анализатора трафика («Wireshark»).

Система защиты от злоумышленного программного обеспечения основывается на следующих типах антивирусных программ:

– стационарные;

– облачные.

Разработка и исследование механизмов антивирусной защиты для стационарных систем не является содержанием работы. Для этого могут использоваться известные антивирусные программы (Ан-

тивирус Касперского, Vicrosoft Security Esentiale, Panda, Dr Web, Avira AntiVir и др.) [17-18].

Одной из наиболее важных составляющих подсистемы защиты на основе облачных антивирусных систем является подсистема управления доступом к облачным телекоммуникационным ресурсам. В ней реализованы основные алгоритмы управления интеллектуальным коммутаторами.

## Выбор показателя вероятности присвоения приоритета для определения «эталона» приоритета

Как было указано в [1-7] для решения задачи управления доступом к «облачным» телекоммуникационным ресурсам необходимо заранее задать показатель вероятности присвоения приоритета – $P_{присв}$.

Для решения данной задачи было проведено ряд экспериментов в условиях, когда N – число независимых потоков информационного трафика (может определяться количеством узлов в ТКС) равно 120, P – пропускная способность канала связи – 10 Гбит/с, RTT (Round Trip Time) – время прохождения сигнала от источника трафика до маршрутизатора и обратно равно 100 мс. Тогда B – объем буфера интеллектуального узла коммутации равен:

$$B \approx \frac{P \cdot RTT}{\sqrt{N}}, \qquad (1)$$

Путем несложных вычислений определим, что объем B равен 12,5 Мб.

Если размер одного информационного пакета 1024 байт [8], то объем буфера интеллектуального узла коммутации ~ 10000 пакетов.

На основе экспертных оценок определено, что вероятность $P_{присв}$ целесообразно выбирать в диапазоне $\{0{,}5\ldots0{,}9\}$ (в работе в качестве примера были выбраны значения 0,7 и 0,9.

## Оценка эффективности метода управления доступом к облачным телекоммуникационным ресурсам для обеспечения антивирусной защиты данных

Построим графики среднего времени обработки информационного пакета. При этом для распределения информационных пакетов по приоритетам в соответствии с моделью $r_1 = 1$, $r_2 = \overline{2,J}$ и $r_3 = \overline{J+1,R}$, определим, что $J = 4$ а $R = 8$. В соответствии с указанными данными распределение информационных пакетов по их приоритетности представлено табл. 1.

Рассмотрим различные варианты распределения на примере использования разработанного алгоритма управления доступом к «облачным» телекоммуникационным ресурсам.

Таблица 1

Распределение информационных пакетов по их приоритетности

| Номер приоритета | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| Количество пакетов $(\times 1000)$ | 0,5 | 1,2 | 1,2 | 1,2 | 1,4 | 1,4 | 1,4 | 1,4 |

Анализ алгоритмов распределения ресурсов в интеллектуальных узлах коммутации показал, что императивный (статический) подход настройки сетевого оборудования является одним из самых распространенных.

Пример распределения телекоммуникационных ресурсов в соответствии с таким подходом администрирования представлен в табл. 2.

Таблица 2

Пример императивного администрирования и распределения телекоммуникационных ресурсов

| Номер приоритета: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| Весовой коэффициент: | 0,35 | 0,15 | 0,15 | 0,15 | 0,05 | 0,05 | 0,05 | 0,05 |

Результаты анализа показателя времени обработки информационных пакетов в интеллектуальном узле коммутации в условиях использования известного ($WF^2Q$) и усовершенствованного алгоритма управления доступом к «облачным» телекоммуникационным ресурсам представлены в виде гистограммы на рис. 1.

Как видно из рис. 1 использование разработанного алгоритма управления ( $P_{присв} = 0{,}9$ ) в условиях, приведенных в табл. 1 и табл. 2 до 3 раз уменьшит время обработки информационных пакетов первого уровня приоритетности. В то же время эффективность усовершенствованного алгоритма управления на всем выбранном диапазоне $P_{присв}$ незначительно уступает эффективности алгоритма $WF^2Q$. Поэтому можно сделать вывод о соизмеримости показателя времени обработки информационных пакетов $r_2 = \overline{2,J}$ и $r_3 = \overline{J+1,R}$ уровней приоритетности.

Таким образом, принцип несправедливого распределения вычислительных и телекоммуникационных ресурсов существенно уменьшает время обработки информационных пакетов выделенного (максимального) уровня приоритетности. Однако при этом наблюдается незначительное ухудшение качества обслуживания информационных пакетов других приоритетов.

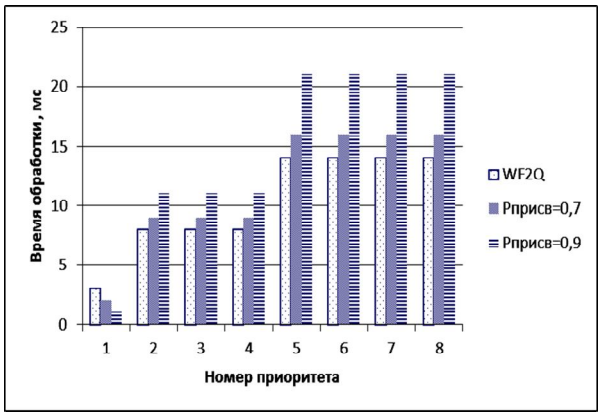



Рис. 1. Гистограммы времени обработки информационных пакетов в условиях императивного администрирования

В качестве еще одного примера решения задачи распределения телекоммуникационных ресурсов интеллектуальных узлов коммутации можно отметить принцип справедливого распределения. Анализ алгоритмов справедливого распределения показал наличие различных подходов определения весовых коэффициентов, определяющих долю обслуживаемого информационного потока. Так одним из примеров является подход, основанный на вычислении весового коэффициента $\omega_i$ с помощью выражения:

$$\omega_i = \frac{\sqrt{i}}{\sum_{j=1}^{N}\sqrt{j}}, N = 8, i = \overline{1..N} \qquad (2)$$

Значения весовых коэффициентов, полученных с помощью данного выражения представлены в табл. 3.

Таблица 3

Экспериментальные значения весовых коэффициентов справедливого распределения

| Номер приоритета: | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| Весовой коэффициент: | 0,17 | 0,16 | 0,15 | 0,14 | 0,12 | 0,11 | 0,09 | 0,06 |

Результаты исследования показателя времени обработки информационных пакетов представлены на рис. 2.

Как видно из этого рисунка, использование в усовершенствованном алгоритме управления доступом к «облачным» телекоммуникационным ресурсам принципа справедливого распределения в соответствии с выражением (3) позволило до 2 раз при $P_{присв} = 0,9$, до 1,5 раз при $P_{присв} = 0,7$ снизить время обработки информационных пакетов по сравнению с алгоритмом WF2Q. В остальных случаях обработки информационных пакетов $r_2 = \overline{2,J}$ и $r_3 = \overline{J+1,R}$ уровней приоритетности эффективность разработанного алгоритма соизмерима с эффективностью известного $WF^2Q$.

Таким образом, приведенные результаты исследований позволили сделать вывод о эффективности разработанного метода управления доступом к облачным телекоммуникационным ресурсам и возможности уменьшения времени обработки информационных пакетов первого уровня приоритетности до 4 раз в случае императивного администрирования и до 2 раз в случае справедливого распределения.

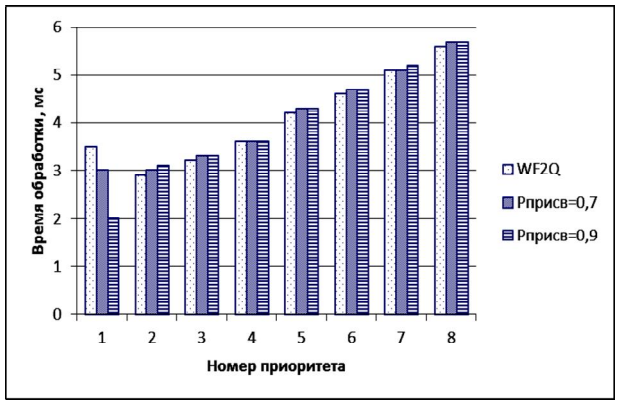



Рис. 2. Гистограммы исследования показателя времени обработки информационных пакетов различного уровня приоритетности в условиях справедливого распределения

## Обоснование достоверности результатов математического моделирования

Для обоснования достоверности полученных в [1-7] результатов проведено имитационное моделирование процесса обработки информационных пакетов в интеллектуальных узлах коммутации ТКС, в соответствии с условиями :

– все процессоры в подсистемы управления и обслуживания в узле связи однотипны и осуществляют обслуживание независимо друг от друга;

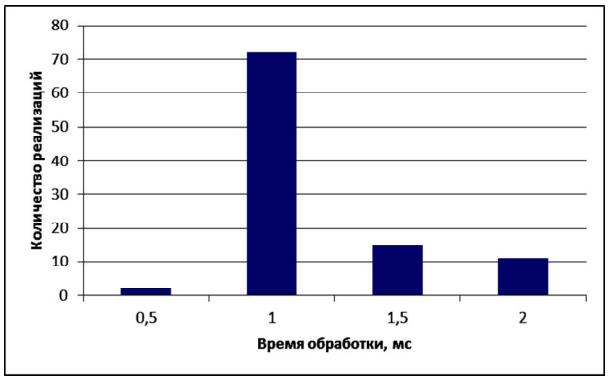
– один процессор может обслуживать в единицу времени такое количество пакетов, которое соответствует количеству пакетов, хранящихся в одной ячейке памяти буфера;

– длина информационного пакета $\ell_p = 1024$ бита;

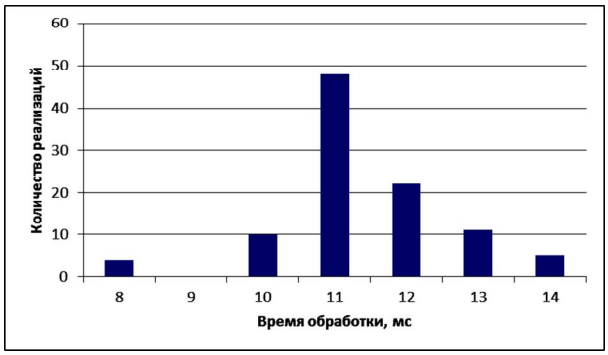
– число экспериментов N*=100.

По результатам имитационного моделирования для различного рода информации получены гистограммы времени обработки информационных пакетов в интеллектуальных узлах коммутации [19].

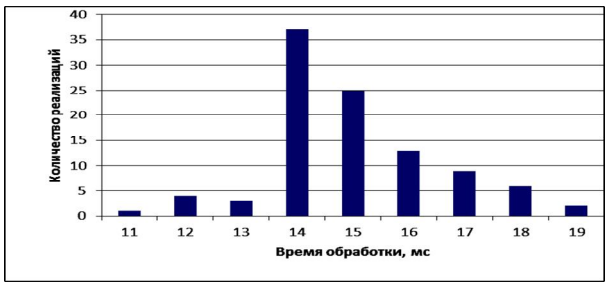
На рис. 3 представлены гистограммы времени обработки информационных пакетов метаданных $r_1$ уровня приоритетности (рис. 3, а), информационных пакетов протокола SKYPE $r_2$ – уровня приоритетности (рис. 3, б) и информационных пакетов FTP (HTTP)-трафика $r_3$ уровня приоритетности (рис. 3, в).




а




б




в

Рис. 3. Гистограммы времени обработки информационных пакетов в интеллектуальном узле коммутации

Выдвинутая гипотеза о нормальном распределении этой случайной величины была проверена по критерию согласия $\chi^2$ Пирсона [20]:

$$\chi^2 = N^* \sum_{i=1}^{k} (P_i^* - P_i)^2 / P_i ,$$

где k – число разрядов (интервалов) статистического ряда; $P_i^*$ и $P_i$ – «статистическая» и теоретическая вероятности «попадания» заданного показателя в і-й разряд.

Проведенная проверка доказала правдоподобность гипотезы о том, что величина времени обработки информационных пакетов в интеллектуальном узле коммутации распределена по нормальному закону.

Получены оценки $\hat{t}_{обр}^{(i)}$ математического ожидания и $\hat{D}_{t_{обр}^{(i)}}$ дисперсии ($\hat{\sigma}_{t_{обр}^{(i)}}$ среднеквадратического отклонения) случайной величины $t_{обр}^{(i)}$ времени обработки информационных пакетов в интеллектуальном узле коммутации [19]:

$$\hat{t}_{обр}^{(i)} = \frac{\sum_{i=1}^{k} \hat{t}_{обр}^{(i)}}{N^*};$$

$$\hat{D}_{t_{обр}^{(i)}} = \frac{\sum_{i=1}^{k} \left( \hat{t}_{обр}^{(i)} - t_{обр}^{(i)} \right)^2}{N^* - 1};$$

$$\hat{\sigma}_{t_{обр}^{(i)}} = \sqrt{\hat{D}_{\hat{t}_{обр}^{(i)}}} .$$

Воспользовавшись известным выражением для расчета доверительной вероятности отклонения относительной частоты от постоянной вероятности в независимых испытаниях [20] определим доверительную вероятность того, что полученное в результате эксперимента значение времени обработки информационных пакетов «не отклониться» от математического ожидания $\hat{t}_{обр}^{(i)}$ более чем на 1:

$$P\left( \left| \hat{t}_{обр}^{(i)} - t_{обр}^{(i)} \right| < 1 \right) = 2\Phi\left( 1 / \hat{t}_{обр}^{(i)} \right),$$

где Ф – функция Лапласа вида

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-t^2/2} dt \quad [20].$$

Проведенное имитационное моделирование показало, что для всех исследуемых видов данных доверительная вероятность того, что значение статистической величины $t_{обр}^{(i)}$ «не отклониться» от математического ожидания $\hat{t}_{обр}^{(i)}$ более чем на 1 равно: $P \approx 0,97$.

В условиях императивного администрирования интеллектуального узла коммутации проведено сравнительное исследование результатов математического и имитационного моделирования. Результаты сравнения представлены на рис. 4 в виде графика плотности распределения времени $t_{обр}$ обработки информационных пакетов метаданных, при их передаче в «облачные» антивирусные системы, соответствующих им границ доверительного интервала:

$$I_\beta = \left[ \hat{\bar{J}} - \varepsilon_\beta, \hat{\bar{J}} + \varepsilon_\beta \right],$$

в которой истинное значение $\bar{J}$ попадает с доверительной вероятностью $\beta = 0,95$ и оценок его $\hat{t}_{обр}^{(i)}$ математического ожидания.

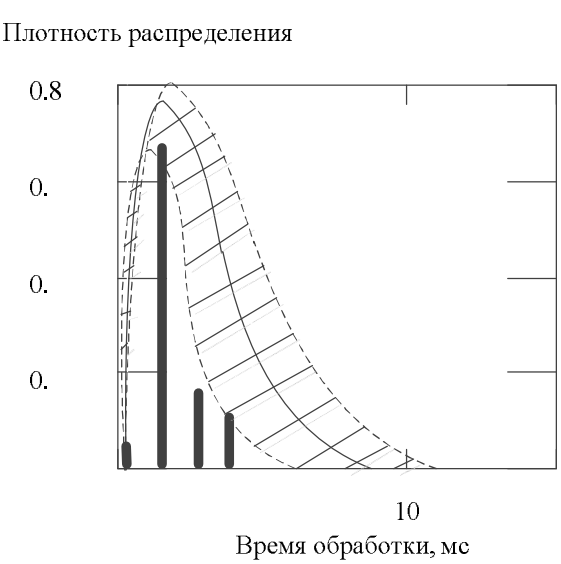



Рис. 4. График плотности распределения времени $t_{обр}$ обработки информационных пакетов, соответствующих им границ доверительного интервала и оценок его $\hat{t}_{обр}^{(i)}$ математического ожидания

Из графиков видно, что в ключевой тестовой ситуации (время обработки $t_{обр} \approx 1$ мс) «расчетная» кривая J (сплошная кривая), полученная в соответствии с разработанной в работах [1-7] математической моделью, в большинстве практических случаев попадают в «усредненный» доверительный интервал (заштрихованная область).

Это подтверждает достоверность разработанной математической модели узла коммутации с относительными приоритетами, резервированием ресурсов и учётом реальной надёжности обслуживающих приборов [1-7] и полученного в результате математического моделирования аналитического выражения для расчета времени обработки информационных пакетов в интеллектуальном узле коммутации.

## Обоснование практических рекомендаций по использованию метода управления доступом к облачным телекоммуникационным ресурсам для обеспечения антивирусной защиты данных

Проведенный анализ современных интеллектуальных узлов коммутации (маршрутизаторов), поддерживающих усовершенствованные алгоритмы QoS, позволил выделить их основные функции:

– перераспределение информационных пакетов;

– подстройка параметров подключенной телекоммуникационной среды.

Практическая реализация этих функций возможна как на однопроцессорных узлах коммутации, так и на многопроцессорных. При этом важную роль играет операционная система, установленная на узлах коммутации.

Так перераспределение информационных пакетов может осуществлять как отдельный интерфейсный процессор.

Проведенный анализ показал, что интеллектуальные узлы коммутации должны поддерживать различные алгоритмы управления – CAR, WFQ, RRP, RSVP, DiffServ и др.

Для выполнения этих требования современные маршрутизаторы (например, Cisco 3800 Series, Cisco 2800 Series, Cisco 7200 Series, 2210 Multiprotocol Routers, Motorola 6435/6455, ASUS RT-AC66U и др.) добавляют протокол ресурсов, контрольный модуль и интерфейс к политике очередей уровня коммутации [19].

В работах [1 – 7] предлагается дополнительную реализацию и использование в интеллектуальных узлах коммутации блоков управления телекоммуникационными ресурсами с учетом возможности приоритезации информационных пакетов (метаданных) для передачи в облачные антивирусные системы.

Несмотря на введение дополнительных механизмов регуляции и управления информационными пакетами современные узлы коммутации должны обеспечить максимальную скорость обслуживания информационных пакетов и других (более низких) уровней приоритетности.

Сравнительный анализ современных телекоммуникационных технологий, методов управления сетевыми ресурсами, а также результаты проведенных исследований позволили разработать практические рекомендации по повышению оперативности передачи метаданных в облачные антивирусные системы и применению разработанных моделей и метода, которые заключаются в следующем:

– для обеспечения качества обслуживания при передаче информационных пакетов $r_2 = \overline{2,J}$ уровня приоритета (в первую очередь мультимедийной информации) целесообразно объединение различных интерактивных служб и услуг в рамках единой многофункциональной информационной подсистемы;

– в процессе управления ТКС в целом и отдельными ее ресурсами необходимо проводить антивирусный мониторинг и оценку состояния узлов с помощью аппаратных или программных средств предотвращения и обнаружения вторжений (например, Snort);

– в процессе информационного обмена для повышения оперативности передачи метаданных в облачные антивирусные системы необходимо осу-

ществлять целый комплекс мероприятий (адаптивное кодирование, статистическое мультиплексирование, адаптивная маршрутизация и др.) [13];

– в системе управления очередями интеллектуального узла коммутации целесообразно использовать алгоритмы равномерного обслуживания очередей (WFQ, $WF^2Q$) с дополнительным внесением разработанных моделей, алгоритмов и методов, а также элементов первоочередного обслуживания информационных пакетов;

– в облачных антивирусных системах целесообразно использовать референсную архитектуру, основное назначение которой – адаптация оборудования к современным требованиям безопасности и повышение надежности используемых ресурсов [12].

При этом проведенные исследования показали, что одной из наиболее перспективных является облачная архитектура, базирующаяся на современных серверах семейства Z и в дополнение на нескольких серверах HP и Sun(Oracle):

– управляющая машина IBM z196 [8] (несколько CPU для поддержки z/OS и множество IFL (Integrated Facility for Linux) для поддержки z/VM и zLinux;

– zBX, управляемые из z196 (поддерживают операционные системы AIX, Linux, Windows);

– HP & SUN (для поддержки HP-UX и Solaris);

– СУБД – DB2 (все платформы), Oracle (все платформы), MSSQL, Sybase и другие системы управления базами данных;

– семейство программных продуктов IBM Tivoli [8].

Следует отметить, что постоянно растущий интерес к облачным технологиям требует от разработчиков новых конструктивных решений и практических рекомендаций.

Последний пример таких рекомендаций распространен журналом Infoworld в рамках специального отчета Cloud security, Deep Dive series, August 2011 под названием «Новая модель безопасности для новой эры» [21].

Авторы отчета настаивают на коренном пересмотре подхода к информационной безопасности при переходе к облачной среде. Это и повышенные требований к механизмам аутентификации, для которых необходимо усовершенствовать систему электронной цифровой подписи, и обеспечениие доступности к облачным антивирусным ресурсам вне зависимости от их территориального (адресного) размещения.

Кроме этого, в связи с появлением новых факторов, влияющих на состояние безопасности ТКС, возникает необходимость пересмотра подходов к оценке уязвимости виртуальных соединений с облачными системами.

Таким образом, использование разработанных моделей и методов управления доступом к облачным телекоммуникационным ресурсам в условиях модернизации сетевого телекоммуникационного оборудования позволит повысить уровень информационной и функциональной безопасности как отдельных секторов так и телекоммуникационной сети в целом, при этом обеспечив заданный уровень качества обслуживания в процессе информационного обмена.

## Выводы

В статье проведены исследования эффективности разработанного метода управления доступом к облачным телекоммуникационным ресурсам для обеспечения антивирусной защиты данных и обоснование практических рекомендаций по его использованию.

Определено, что в качестве показателя эффективности разработанного метода управления доступом к облачным телекоммуникационным ресурсам для обеспечения антивирусной защиты данных целесообразно выбрать время обслуживания информационных пакетов в интеллектуальных узлах коммутации.

Доказано, что использование разработанного метода до трех раз уменьшит время обслуживания информационных пакетов метаданных в интеллектуальных узлах коммутации при передаче их в облачные антивирусные системы. При этом будет обеспечен необходимый уровень качества обслуживания информационного обмена других телекоммуникационных услуг.

При оценке достоверности полученных в результате математического моделирования данных было проведено сравнение плотности распределения времени обработки информационных пакетов метаданных при их передаче в «облачные» антивирусные системы и оценок его математического ожидания. Истинное значение выбранного показателя попадает в доверительный интервал с доверительной вероятностью $\beta = 0,95$

В качестве практических рекомендаций предложены технические новшества и решения, которые позволят повысить эффективность информационного обмена в современной ТКС.

## Список литературы

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

*2. Мохамад Абу Таам Гани Структурно-логическая GERT-модель технологии распространения компьютерных вирусов / А.А.Смирнов, И.А.Березюк, Мохамад Абу*

*Таам Гани // Системи управління, навігації та зв'язку. – Випуск 1(29). – П.: ПНТУ. – 2014. – С. 120-125.*

*3. Мохамад Абу Таам Гани 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 // Збірник наукових праць "Системи обробки інформації". – Випуск 9(125). – Х.: ХУПС – 2014. – С. 105-110.*

*4. Мохамад Абу Таам Гани 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. Випуск 4 (41). – Харків: ХУПС. – 2014. – С. 48-52.*

*5. Мохамад Абу Таам Гани 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). – Харків: ХУПС. – 2014. – С.90-95.*

*6. Мохамад Абу Таам Гани Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Збірник наукових праць "Системи обробки інформації". – Випуск 1(126). – Х.: ХУПС – 2015. – С. 150-153.*

*7. Mohamad Abou Taam 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.*

*8. 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.*

*9. ITU-T Recommendations [Электронний ресурс]. – Режим доступа к ресурсу: http://www.itu.int/ITU-T/recommendations/index.aspx?ser=Y*

*10. Арипов М.Н. Проектирование и техническая эксплуатация сетей передачи дискретных сообщений / М.Н. Арипов, Г.П. Захаров, С.Т. Малиновский, Г.Г. Яновский. М Радио и связь. 1988г. 360с*

*11. Бертсекас Д. Сети передачи данных: пер. с англ. / Д. Бертсекас, Р. Галлагер; под ред. Б.С. Цыбакова. – М.: Мир, 1989. – 544 с.*

*12. Галкин В.А. Телекоммуникации и сети / В.А. Галкин, Ю.А.Григорьев. – М.: МГТУ имени Н.Э. Баумана, 2003. – 608 с.*

*13. Королев А.В. Адаптивная маршрутизация в корпоративных сетях / А.В. Королев, Г.А. Кучук, А.А. Пашнев. – Х.: ХВУ, 2003. – 224 с.*

*14. Семенов С.Г. Оптимизация трафика на основе сбалансированной загрузки информационно-телекоммуникационной сети // Системи обробки інформації. – Х.: ХВУ, 2004. – № 8(36). – С.206-210*

*15. Semenov S.G. Mathematical Modelling of the Spreading of Software Threats in Computer Network / S.G. Semenov, V.V. Davydov, S.O. Engalichev // Proceedings of the XIth International Conference TCSET'2012 «Modern problems of radio engineering, telecommunications and computer science». – Lviv – Slavske, Ukraine 2012. – P. 329*

*16. Semenov S.G. A Mathematical Model for Technology for Spreading Malicious Software across Heterogeneous Networks based on Markov Chains / Semenov S., Davydov V.// European Researcher, 2014, Vol.(66), N1-1. - pp. 21-30.*

*17. Кингман Дж. Пуассоновские процессы / Дж. Кингман М.:МЦНМО, 2007. – 136 с.*

*18. Кормен Т. Алгоритмы: построение и анализ / Томас Кормен, Чарльз Лейзерсон, Рональд Ривест, Клиффорд Штайн. – М.:"Вильямс", 2005. –1296 с.*

*19. Одом Ш. Коммутаторы CISCO / Ш. Одом, Х. Ноттингем. – М.:"Кудиц-Образ", 2003. – 528 с.*

*20. Гмурман В.Е. Теория вероятностей и математическая статистика / Владимир Ефимович Гмурман. – М.: Высшая школа, 2003. – 479 с.*

*21. Cloud security, Deep Dive series, August 2011 [Электронный ресурс]. – Режим доступа к ресурсу: http://www.slideshare.net/kimrenejensen/cloud-security-deep-dive-2011#14375029197881&fbinitialized.*

*Поступила в редколлегию 3.08.2015*

**Рецензент***:* д-р техн. наук проф. Г.А. Кучук, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

## ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ МЕТОДУ УПРАВЛІННЯ ДОСТУПУ ДО ХМАРНИХ АНТИВІРУСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ РЕСУРСІВ

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

*У статті проводиться вибір показника ефективності управління доступом до хмарних антивірусних телекомунікаційних ресурсів. На основі результатів математичного та імітаційного моделювання проводиться вибір показника ймовірності присвоєння пріоритету для визначення «еталона» пріоритету та оцінка ефективності методу управління доступом до хмарних телекомунікаційних ресурсів для забезпечення антивірусного захисту даних. Обґрунтовується достовірність результатів математичного моделювання, і пропонуються практичні рекомендації з використання розробленого методу.*

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

## RESEARCH EFFECTIVE METHOD OF CONTROLLING ACCESS TO CLOUD ANTIVIRUS TELECOMMUNICATION RESOURCES

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

*The article selects the performance indicator control access to cloud antivirus telecommunication resources. Based on the results of mathematical modeling and simulation is performed for the probability range of prioritization to determine the "standard" priority and performance evaluation method of controlling access to cloud telecommunication resources for antivirus protection of data. Substantiates the validity of the results of mathematical modeling, and offers practical advice on the use of this method.*

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