УДК 004.49.5

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

*Кировоградский национальный технический университет, Кировоград*

# АНАЛИЗ И ИССЛЕДОВАНИЕ МЕТОДОВ УПРАВЛЕНИЯ СЕТЕВЫМИ РЕСУРСАМИ ДЛЯ ОБЕСПЕЧЕНИЯ АНТИВИРУСНОЙ ЗАЩИТЫ ДАННЫХ

*В данной статье анализируются перспективные методы и средства антивирусной защиты данных, требования обеспечения качества передачи данных в телекоммуникационных системах, основные направления и подходы математического моделирования, формулируется задача разработки метода управления доступом к облачным телекоммуникационным ресурсам для обеспечения антивирусной защиты данных.*

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

## Постановка проблемы исследования

В соответствии с законами Украины «Про телекомунікації», «Про інформацію», указом президента Украины «Про першочергові завдання щодо впровадження новітніх інформаційних технологій» одним из наиболее важных факторов развития социально-экономических взаимоотношений в Украине является обеспечение качественного доступа к публичной информации, оперативной обработки и безопасного хранения данных с использованием современных телекоммуникационных технологий [1, 2]. При этом анализ государственных стандартов Украины (ДСТУ 2941-94, ГОСТ 34.003-90 и др.), рекомендаций международного союза электросвязи (МСЭ) (МСЭ Е.430, Е.800, Х.134 –137 и др.) показал, что современная телекоммуникационная система должна обеспечивать заданные требования безопасности на всех этапах информационного обмена, включая процессы внутренней функциональности локальных телекоммуникационных и других систем автоматизированной обработки данных.

Анализ основных угроз информационной и функциональной безопасности телекоммуникационных систем показал явные тенденции к увеличению злоумышленного программного обеспечения, циркулирующего и внедряющегося в средства автоматизированной обработки данных телекоммуникационных систем. Это повышает спрос потребителей на различного рода средства антивирусной защиты данных.

Анализ литературы [3-7] и проведенные исследования показали, что в настоящее время существует ряд средств противодействия злоумышленному программному обеспечения (компьютерным вирусам). При этом среди них основное преимущество предоставляется антивирусному программному обеспечению. Анализ этих специализированных программ показал, что для их эффективного функционирования используется два основных метода сканирования и поиска вредоносных программ - сигнатурный и эвристический [6-8].

Проведенный анализ сигнатурного метода показал, что его отличительной особенностью является то, что каждому вирусу ставится в соответствие некоторая сигнатура или маска. Маска содержит набор вредоносных команд. В ряде случаев, в качестве сигнатуры, берется характерный для этого типа вируса фрагмент кода, например, фрагмент обработчика прерывания. Размер сигнатуры зависит от типа вирусов. Обычно используются маски длиной до 1 Кбит. Чем больше размер сигнатуры, тем меньше вероятность ложного срабатывания. Но при больших размерах сигнатур, база сигнатур вирусов становится очень большой. Если при сканировании подозрительного файла антивирус находил код, который отвечал маске, то исследуемый файл рассматривался как инфицированный.

Очевидно, что эффективность сигнатурного метода напрямую зависит от объема антивирусной базы и частоты ее пополнения. При этом с момента появления нового вируса до его идентификации проходит определенное время. За это время злоумышленное программное обеспечение может нанести значительный вред информационным ресурсам.

Анализ эвристических методов поиска вредоносных программ показал, что в их основу положены основные закономерности человеческого мышления. Применение эвристического анализа позволяет сделать вывод о возможном наличии в программе вируса. В результате работы эвристического метода анализируется не код подозрительного файла, а действия. Вирус может копировать свое тело в память, открывать другие файлы и записывать туда свое тело, записывать данные в сектора жесткого диска, записывать или удалять данные из реестра ключей. Программы, реализующие этот метод, проверяют загрузочные сектора дисков и файлы, пытаясь обнаружить в них код, характерный для вирусов.

Проведенные исследования показали, что в настоящее время существуют два основных метода работы эвристического анализатора – статический и динамический.

Статический метод, основанный на поиске коротких сигнатур. Такие сигнатуры содержат подозрительные команды, которые присутствуют в большинстве вирусов. Например, эвристический анализатор просматривает PE-структуру [5] подозрительного исполняющего файла. Затем происходит анализ найденных сигнатур, и если найдено некоторое количество необходимых и достаточных подозрительных команд, то принимается решение о том, что файл инфицирован. Преимуществом этого метода является простота реализации и высокая скорость работы, но уровень обнаружения новых вредоносных программ при этом достаточно низкий.

Динамический метод связан с эмуляцией команд процессора. Суть этого метода заключается в эмуляции выполнения программы и протоколировании всех подозрительных действий программы. На основе этого протокола принимается решение о возможном заражении программы вирусом. В отличие от статического, динамический метод является более требовательным к ресурсам компьютера, но и уровень обнаружения у него значительно выше.

В настоящее время в антивирусной индустрии наметилась тенденция перехода на новые, более совершенные, технологии защиты данных от злоумышленного программного обеспечения. Так на рис. 1 представлены основные направления развития и реализации средств антивирусной защиты данных.

Проведенные исследования показали, что одним из наиболее перспективных направлений совершенствования средств антивирусной защиты данных являются так называемые облачные вычисления (cloud computing), или облачные антивирусы. Это во многом связано с распространением и доступностью телекоммуникационных средств и ресурсов, увеличением числа компьютерных вирусов и повышением стоимости антивирусных средств (обновлений баз данных).

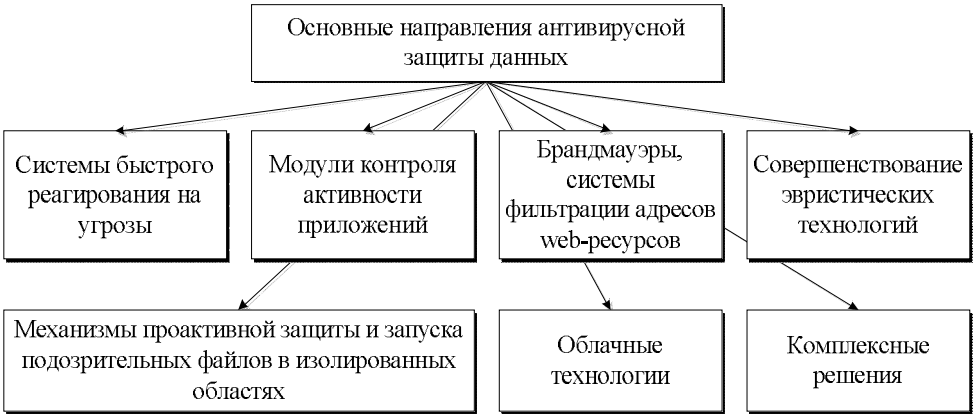


Рис. 1. Основные направления развития и реализации средств антивирусной защиты данных

В то же время использование подобного рода антивирусных программных ресурсов требует от разработчиков новых технических решений обеспечивающих заданное качество информационного обмена метаданными (специальными сигнатурами файлов) с удаленными облачными системами поддержки и принятия решений. Наиболее сложными, при этом, остаются системы управления телекоммуникационными ресурсами, в которых реализуются методы и процедуры распределения доступа с обеспечением качества передачи телекоммуникационного трафика различного уровня приоритетности.

Рассмотрим основные методы обеспечения качества обслуживания информационного трафика в телекоммуникационных системах.

## Анализ требований обеспечения качества передачи данных в телекоммуникационных системах

Проведенные исследования показали, что современные факторы развития сетевых и телекоммуникационных технологий требуют разработки адекватных (с необходимой точностью и подробностью) данным способам математических моделей, а также адекватного развития методов теоретического исследования процессов функционирования и проектирования (синтеза) телекоммуникационных систем, которое должно осуществляться на основе систематизации уже известных подходов в предметной области систем будущего поколения и разработки новых методов их анализа и синтеза, включая обеспечение:

– качества обслуживания при совместной передаче разнородного трафика с отличающимися требованиями к рабочим характеристикам сети;

– информационной и функциональной безопасности систем обработки и хранения данных.

В соответствии с рекомендациями E.430, E.800, X.134 и др. международного союза электросвязи под качеством обслуживания (Quality of Service, QoS) понимается обобщенный (интегральный) полезный эффект от обслуживания, который определяется степенью удовлетворения пользователя как от полученной услуги, так и от самой системы обслуживания [1, 2, 9, 10].

Для количественной характеристики большинства определённых в рекомендации TL 9000 и E.800 свойств качества телекоммуникационных услуг вводятся соответствующие показатели, определяемые на основе рабочих характеристик (параметров) сети.

Анализ рекомендаций I.350 показал, что качество предоставляемых телекоммуникационных услуг обеспечивается на трех стадиях:

– доступ к передаче информации (установление соединения);

– передача информации пользователя;

– завершение сеанса передачи информации (разъединение соединения).

Каждая из частей услуги в свою очередь характеризуется тремя основными показателями, образуя матрицу 3x3:

– оперативность (время установления соединения, время (эффективная скорость) передачи информации пользователя, вероятность своевременной доставки информации пользователя и время разъединения соединения);

– безопасность – это свойство, характеризующее способность системы противостоять случайным или преднамеренным, внутренним или внешним воздействиям, следствием которых могут быть ее нежелательное состояние или поведение (вероятность навязывания ложных соединений, вероятность ввода ложных данных, вероятность ложного завершения работы и др.);

– достоверность (гарантированность установления соединения, передачи данных и разъединения соединения, характеризуемые вероятностью отказа в установлении соединения, вероятностью потери информации пользователя, вероятностью отказа в разъединении соединения и др.).

Следует заметить, что в перечисленных показателях не нашлось места показателям, характеризующим способность системы противостоять различного рода злоумышленным воздействиям, в том числе воздействиям злоумышленного программного обеспечения (компьютерным вирусам).

Анализ ряда работ [11-13] в области защиты данных в телекоммуникационных системах, а так же «Оранжевой книги» американского военного ведомства [14] показал, что описанные в них требования носят более качественный, чем количественный характер, что в значительной степени сужает возможности их практического использования.

В работах [1, 14] представлен такой показатель как безопасное время $T_б$ [Security time] – математическое ожидание времени раскрытия системы защиты статистическим апробированием возможных вариантов доступа к данным. Его можно отнести к перечню ресурсных возможностей телекоммуникационных сетей, задействованных оператором (Resources and Facilities), и использовать при анализе ряда злоумышленных атак на ресурсы телекоммуникационных систем (ТКС). В то же время данный показатель не в полном объеме описывает защищенность системы от атак компьютерных вирусов. Поэтому возникает необходимость введения показателей, характеризующих способность системы противостоять атакам с помощью злоумышленного программного обеспечения.

Данный показатель является комплексным, и может быть представлен в виде произведения матриц:

$$B_i^{(ТКС)} = (X_{ik} \cdot Y_k) \cdot A, \qquad (1)$$

где $B_i^{(ТКС)}$ – показатель, характеризующий выполнение требований информационной и функциональной безопасности в случае воздействия на систему злоумышленного программного обеспечения,

$X_{ik} = \left[ x_{\psi}^{(\xi)} \right]$ – матрица усредненных коэффициентов влияния атак компьютерных вирусов и другого злоумышленного программного обеспечения на отдельные показатели качества обслуживания,

i – количество возможных воздействий злоумышленного программного обеспечения, влияющих на функционирование системы,

k – количество подсистем ТКС,

$x_{\xi}^{(\psi)} = \frac{1}{N} \sum_{j=1}^{N} x_{\ell_j}^{(\psi)}$ – усредненный коэффициент влияния атак компьютерных вирусов и другого злоумышленного программного обеспечения ($\psi$) на показатели качества функционирования отдельных подсистем ТКС ($\xi$),

$\ell$ – наименование отдельного показателя качества функционирования подсистемы ТКС,

A – матрица усредненных коэффициентов взаимовлияния различных подсистем ТКС в процессе распространения компьютерных вирусов,

$Y_k$ – матрица показателей качества в подсистемах ТКС.

Проведенные исследования показали, что в настоящее время качество обслуживания в ТКС задаётся несколькими способами. Но только один из них, определенный рекомендациями Международного союза электросвязи (рек. МСЭ-Т G.1010) [15], носит количественный характер. Как видно из данных рекомендаций в них отсутствуют требования антивирусной безопасности ТКС.

В этой связи возникает необходимость моделирования жизненного цикла компьютерных вирусов в ТКС и определения критического времени их распространения.

Проведем анализ существующих подходов математического моделирования технологии распространения компьютерных вирусов в ТКС.

## Анализ и сравнительные исследования подходов математического моделирования технологии распространения злоумышленного программного обеспечения в телекоммуникационных системах

Анализ литературы [3, 16, 17] показал, что в настоящее время существует ряд подходов математического моделирования технологии распространения компьютерных вирусов в ТКС, основой которых являются теории связи, массового обслуживания, графов др. В то же время в основу большинства подобных математических моделей положены биологические знания [14-17].

В настоящее время известно несколько разновидностей математических моделей распространения компьютерных вирусов, отличающихся между собой областью ограничения и условиям применения в реальных технических системах. Среди них можно выделить следующие модели:

SI (Suspected-Infected),

SIR (Suspected-Infected-Recovered),

SEIQR (Suspected-Exposed-Infected-Quarantined-Recovered),

PSIDR (Progressive Suspected-Infected-Detected-Recovered).

Разработка и описание указанных моделей возможно с использованием различного математического аппарата. Так в работах [16, 17] для описания процесса распространения компьютерных вирусов использовался математический аппарат дифференциальных уравнений. Это позволило расширить спектр оцениваемых факторов влияния злоумышленного программного обеспечения на процесс функционирования ТКС.

Например, учесть множественность связей между узлами коммутации ТКС. Кроме этого данный подход, известный в распространенной терминологии как «хищник-жертва» достаточно хорошо изучен. Поэтому адекватность и достоверность полученных, в результате математического моделирования, оценок не вызывает сомнений.

Очень похожим по своей сути с предыдущим математическим направлением описания процесса распространения злоумышленного программного обеспечения является использование знаний и аналогий об иммунной системе. Данный подход несколько уточняет основное математическое направление приведенных выше биологических систем с учетом возможных факторов иммунизации и лечения аппаратных и программных средств ТКС.

Еще одним из направлений описания технологии распространения злоумышленного программного обеспечения, описанным в работах [3, 14], является подход на основе цепей Маркова. Отличительной особенностью данного направления является возможность учета гетерогенности структурного и функционального построения ТКС и влияния данного фактора на процесс распространения злоумышленного программного обеспечения.

Кроме указанных математических подходов существуют и нестандартные, например, в работе [14] предлагается для математического моделирования распространения злоумышленного программного обеспечения использовать каноническую катастрофу складки. В то же время сложность ряда частных задач, связанных с определением уровней детализации оценки угроз и последствий не позволяет на данном этапе использовать результаты моделирования на практике.

Таким образом, наряду с достоинствами существующих математических моделей технологии распространения злоумышленного программного обеспечения, в настоящее время существую и недостатки. В частности модели, описанные в работах [3, 4], не учитывают связность ТКС, а, например, математическая формализации, представленная в [14, 16, 17], не учитывает временные задержки как внутри каждой подсети, так и на «мостах». В работе [14] на наш взгляд наиболее полно раскрыты особенности жизненного цикла злоумышленного программного обеспечения, однако и в ней присутствует ряд ограничений, связанных с невозможностью выбранного математического аппарата описать структурно-функциональные особенности конкретных разновидностей злоумышленного программного обеспечения. Это позволяет сделать вывод о необходимости усовершенствования существующих математических моделей с целью учета особенности конкретных разновидностей злоумышленного программного обеспечения.

Основной задачей разработанных математических моделей на этапе проектирования является определение и нормирование требований к безопасности телекоммуникационных систем в условиях воздействия злоумышленного программного обеспечения. Учет данных требований позволит повысить эффективность технологий и средств обеспечения заданного уровня качества обработки и передачи данных.

Кроме этого результаты математического моделирования технологии распространения злоумышленного программного обеспечения должны стать входными ограничениями для исследования процесса обработки, передачи и управления доступом в телекоммуникационном оборудовании. Подобного рода исследования возможно с использованием различных средств и подходов, в том числе математического моделирования. Рассмотрим наиболее часто используемые подходы.

## Анализ методов и средств обеспечения заданного уровня качества обработки и передачи данных

В настоящее время качество обслуживания в телекоммуникационных системах нового поколения нормируется в основном рекомендациями ITU-T (серия Y.2xxx), ETSI (NGN R.l, R.2), 3GPP/IETF (концепция IMS, R.5-R.7) [19] и частично руководящими документами и стандартами Украины [1, 2]. Основным механизмом, регулирующим качество предоставляемых услуг, в том числе и в сетях связи следующего поколения, является соглашение об уровне обслуживания (Service Level Agreement, SLA) между поставщиком (оператором) и пользователем услуг. В общем случае соглашение об уровне обслуживания включает организационно-экономические параметры, а также параметры производительности сети (скорости передачи данных пользователя), надёжности связи и качества обслуживания передаваемого трафика и др., которые измеряются путём активного и пассивного тестирования системами поддержки эксплуатации рабочих характеристик сети [9, 14].

Сети связи следующего поколения (NGN) характеризуются открытой архитектурой, что определяет наличие в их составе различных компонентов (уровней, плоскостей) и технологий (IP, MPLS, и др.) с адаптивными к требованиям клиентов метриками параметров качества. В данных условиях качество предоставляемых услуг предлагается обеспечивать с использованием интегрированной системы управления ресурсами NGN, реализующей концепцию обеспечения гарантированного качества услуг (Service Assurance). Это с одной стороны предполагает обеспечение требований пользователей на всех уровнях обслуживания для всех приложений и их трансляцию в параметры, определяющие требуемый уровень качества услуг, а с другой стороны обеспечение наиболее важных (обеспечивающих работоспособное состояние) показателей и характеристик по умолчанию [18]. К таковым можно отнести и показатель, характеризующий выполнение требований информационной и функциональной безопасности в случае воздействия на систему злоумышленного программного обеспечения $B_i^{(TKC)}$.

Рассмотрим телекоммуникационные технологии IP, MPLS, а также составные методы и средства, предназначенные для построения транспортных сетей NGN, и их возможности по обеспечению качества обслуживания при передаче разнородного трафика.

Проведенные исследования технологии и используемых в ней протоколов показали, что ее основными особенностями, определяющими область применения являются следующие [10, 14, 18].

1. Алгоритмы функционирования и управления технологии IP не требуют предварительного установления соединения, что уменьшает накладные расходы на сетевом уровне. При этом данная технология изначально проектировалась для передачи пакетов в гетерогенных сетях. В соответствии с этим IP эффективно функционирует в сетях связи со сложной топологией и оборудованием различных производителей, рационально используя адресное пространство.

2. Технология IP не обеспечивает гарантированной доставки информации и качества обслуживания при передаче в сети, при этом пакеты одного сообщения могут доставляться в сети по различным маршрутам с различной задержкой (джиттером задержки), теряться и изменять порядок следования, что также снижает уровень качества обслуживания и увеличивает вероятность успешного проведения различного рода злоумышленных атак.

3. В данной технологии отсутствуют механизмы управления потоком данных (контроль перегрузок), исправления ошибок и восстановления пропущенных пакетов. Отсутствие данных механизмов требует для обеспечения надёжной доставки данных использования протоколов канального и транспортного уровней.

4. Технология IP не предусматривает каких-либо определённых протоколов уровня доступа к среде передаче и физическим средам передачи данных. Требования к канальному уровню ограничиваются наличием интерфейса с модулем IP и обеспечением преобразования IP-адреса узла получателя в MAC-адрес. В качестве уровня доступа к среде передачи используются технологии ATM, IPX, X.25 и др.

Перечисленные ограничения технологии IP требуют применения дополнительных решений для предоставления услуг реального времени. С этой целью для обеспечения качества обслуживания при передаче разнородного трафика разработаны две взаимодополняющие модели управления трафиком — модели интегрированных (Integrated Service, RFC 1633) и дифференцированных (Differentiated Service, RFC 2475) услуг, а также внедрены соответствующие протоколы RSVP, RTCP, RTP, обеспечивающие управление задержками [16, 19]. В свою очередь для обеспечения безопасности информационного обмена разработан протокол IPSec.

Исследования модели интегрированных услуг показали ряд ее механизмов предназначенных для поддержания различных уровней качества обслуживания в объединённых IP-сетях. Это в первую очередь такие механизмы:

– классификация трафика по требованиям к качеству обслуживания;

– маршрутизация, основанная на параметрах качества обслуживания (балансировка нагрузки в сети);

– контроль допуска, обеспечивающий посредством протокола RSVP для каждого нового соединения;

– управление очередями в маршрутизаторах с учетом требований качества обслуживания и длин пакетов, включая: справедливую организацию очередей, взвешенную справедливую организацию очередей и др.;

– политику отбрасывания пакетов на основе алгоритма случайного раннего обнаружения (Random Early Detection, RED).

Перечисленные механизмы и средства в ряде практических случаев позволяют решить задачу обеспечения качества обслуживания отдельных видов телекоммуникационных услуг.

Вместе с тем, практическое применение модели интегрированных услуг обнаружило и её недостатки: жесткая регламентация уровней приоритетности пакетов и соответственно связанные только с данным уровнем гарантии качества обслуживания (это в значительной степени снижает возможности современных протоколов управления ресурсами в обеспечении качества новых услуг связи, в том числе связи с облачными антивирусными системами), низкий уровень масштабирования, а также высокий уровень служебной (сигнальной) информации для контроля состояния соединений и требований к производительности оборудования. Это обуславливает использование данной модели (протоколов) управления трафиком на границах IP сети.

Проведенные исследования модели дифференцированных услуг показали, что данная модель является логическим продолжением работ с целью обеспечения динамического качества обслуживания. Основная идея данной модели состоит в предоставлении дифференцированных услуг для набора классов трафика, отличающихся требованиями к показателям качества обслуживания, определёнными в соглашении об уровне обслуживания (SLA).

Следует заметить, что в модели дифференцированных услуг определены два класса (приоритета) услуг: срочное (Expedited Forwarding, EF, RFC 2598) [19] и гарантированное продвижение данных (Assured Forwarding, AF, RFC 2597) [19], характеризуемые скоростью передачи, задержкой (джиттером) и коэффициентом потери пакетов. С одной стороны данное разбиение в совокупности с относительной простотой классификации трафика, а также отсутствие механизмов сквозного резервирования ресурсов определяют широкое применение модели дифференцированных услуг для обработки интегрированного трафика в мультисервисных сетях связи, но с другой стороны и данная технология не лишена недостатков. В частности модель дифференцированных услуг не позволяет маршрутизировать пакеты, просто игнорируя DSCP в их заголовках, и обрабатывать пакеты в соответствии с рядом используемых в ТКС алгоритмов (например, алгоритмом BE). Этот факт также может снизить эффективность информационного обмена с облачными антивирусными системами, поскольку удаленное их расположение затрудняет процесс информационного обмена.

Указанные ограничения могут быть устранены путем разработки и применения специальных статических и динамических комбинированных механизмов управления трафиком, позволяющих эффективно распределять ресурсы ТКС. Классификация исследуемых в работе приоритетных механизмов управления трафиком, приведена на рис. 2.


Рис. 2. Классификация приоритетных механизмов управления

Проведенные исследования механизмов обеспечения качества технологии ATM показали, общую направленность решения задачи в установлении виртуального соединения для каждого информационного потока пользователя.

В ATM-сетях контролируемые параметры трафика измеряются с помощью специального алгоритма буферизации и формирования очередей, называемого Leaky Bucket (метод «дырявого» ведра).

С помощью этого алгоритма контролируемые параметры трафика могут быть определены и заданы либо управляющим воздействием при установлении виртуального соединения, либо по умолчанию.

Анализ данного свойства технологии ATM позволил сделать вывод о ее недостатках связанных с отбрасыванием (потерей) низкоприоритетных пакетов при возникновении перегрузок в сети, необходимостью использования высокоскоростного телекоммуникационного оборудования и соответственно высокой стоимостью ее эксплуатации.

Проведенный анализ используемых технологий сетевого и канального уровней показали как их достоинства, так и недостатки.

Для объединения достоинств рассмотренных технологий передачи данных разработаны следующие механизмы:

– протоколы передачи IP трафика поверх ATM: Classical IP over ATM (RFC 2225), обеспечивающие инкапсуляцию IP трафика в ячейки ATM на уровне AAL5 и преобразование адресов для постоянных и коммутируемых виртуальных соединений;

– Multiprotocol over ATM (MPOA), обеспечивающий инкапсуляцию IP трафика в ячейки ATM на уровне AAL5, маршрутизацию для коммутируемых виртуальных соединений, поддержание параметров трафика и качества обслуживания;

– технология быстрой коммутации пакетов в многопротокольных сетях MPLS (Multiprotocol Label Switching), позволяющая выбирать маршрут передачи на основе идентификационной метки, сопровождающей передачу пакета по сети.

При этом технология MPLS предназначена для объединения нескольких сетевых технологий (ATM, IP) в рамках единой сети, конструирования трафика (формирования и управления трафиком), создания виртуальных частных сетей (VPN), построения высокоскоростных IP-магистралей, а также магистралей на основе любых других маршрутизируемых сетевых протоколов [18].

Общие рекомендации по применению технологии MPLS для решения задач конструирования трафика (Traffic Engineering, TE) и обеспечения качества услуг сформулированы в RFC 2702 "Requirements for Traffic Engineering over MPLS" [18, 19].

Управление трафиком в MPLS сети предполагает:

– автоматическую маршрутизацию в сети;

– оценку полосы пропускания канала и параметров трафика при определении маршрута в телекоммуникационной сети;

– механизмы динамической адаптации, которые позволяют сделать телекоммуникационную систему устойчивой к отказам.

Проведенные исследования показали, что концепция MPLS обладает рядом достоинств по сравнению с вышеописанными технологиями IP и ATM. Это, например, снижение требований к производительности маршрутизаторов, повышение эффективности утилизации каналов, информационной безопасности и биллинга операторов мультисервисной сети за счет децентрализации служб сбора информации о трафике и др.

В то же время и данная технология имеет недостатки, которые могут снизить эффективность функционирования телекоммуникационной системы в условиях воздействия злоумышленного программного обеспечения. Это, например, необходимость контроля параметров QoS абонентскими портами совместно с операторами, использование высокопроизводительных, а значит и дорогих, коммутаторов на границе мультисервисной сети, отсутствие детерминированных алгоритмов, с помощью которых определяются значения контролируемых параметров в узлах ТКС и др.

Таким образом, проведенные исследования показали объективно существующее противоречие, заключающееся в том, что применяемый математический аппарат, методы управления телекоммуникационными ресурсами, а также средства защиты данных не позволяют учесть тенденции развития облачных телекоммуникационных технологий, новых, зачастую технически и социально опасных факторов внешнего воздействия злоумышленного программного обеспечения, обеспечить выполнение повышенных вероятностно-временных требований к оперативности, достоверности и безопасности данных в телекоммуникационных системах и сетях.

Следовательно, можно сделать вывод о необходимости разработки и практического использования новых механизмов, методов и средств управления информационным трафиком с облачными системами для обеспечения антивирусной защиты данных.

## Выводы

Проведенный анализ и сравнительное исследование перспективных методов и средств антивирусной защиты данных показали целесообразность активизации и интенсификации использования «облачных» антивирусных телекоммуникационных ресурсов, позволяющих повысить эффективность антивирусной защиты и обеспечить требования информационной и функциональной безопасности.

Показано, что одним из определяющих показателей может быть комплексный показатель, характеризующий выполнение требований информационной и функциональной безопасности в случае воздействия на систему злоумышленного программного обеспечения, обеспечение которого возможно путем разработка и применение новых методов управления ресурсами сетевого оборудования в процессе обмена специальными сигнатурами с облачными антивирусными системами.

Показано, что существующие методы управления доступом к облачным телекоммуникационным

ресурсам не обеспечивают оперативности передачи данных в рассматриваемых условиях.

Таким образом, становится актуальной разработка метода управления доступом к облачным телекоммуникационным ресурсам для обеспечения антивирусной защиты данных.

## Список литературы


*1. ДСТУ 2481 – 94 Системи оброблення інформації інтелектуальні інформаційні технології. Терміни та визначення. – Х.: ДЕРЖСТАНДАРТ УКРАЇНИ, 1994. – 33 с.*

*2. ДСТУ ISO 9000:2007 Системи управління якістю. Основні положення та словник термінів [Електронний ресурс]. – Режим доступу до ресурсу: http://document.ua/docs/tdoc14237.php*

*3. Бабанин Д.В. Модели распространения компьютерных вирусов на основе цепей Маркова / Д.В. Бабанин // Математическое и программное обеспечение вычислительных систем: межвуз. сб. науч. тр. / под ред. А.Н. Пылькина – М.: Горячая линия - Телеком, 2009. 156 с. – С. 89-93.*

*4. Бабанин Д.В. Оценка структурной защищенности компьютерной сети от вирусных атак / Д.В. Бабанин // Математическое и программное обеспечение вычислительных систем: межвуз. сб. науч. тр. / Под ред. А.Н. Пылькина – Рязань: РГРТУ, 2011.224 с. – С. 133-138.*

*5. Касперский Е. Компьютерное зловредство / Е. Касперский. – СПб.: Питер, 2007. – 208 с.*

*6. Касперский К. Записки исследователя компьютерных вирусов. / К. Касперский. – СПб.: Питер, 2006. – 316 с.*

*7. Касперский К. Компьютерные вирусы изнутри и снаружи. / К. Касперский. – СПб.: Питер, 2006. – 526 с.*

*8. Gang Cheng. A New Heuristics For Finding The Delay Constrained Least Cost Path / Gang Cheng, Nirwan Ansari. // IEEE GLOBECOM – 2003, P. 3711-3715.*

*9. Современные телекоммуникации. Технологии и экономика / [В.Л. Банкет, О.В. Бондаренко, П.П. Воробьенко и др.]; под ред. С.А. Довгого. – М.: Эко-Трендз, 2003. – 320 с.*

*10. Телекоммуникационные системы и сети: учебное пособие. В 3 томах / [В.В. Величко, Е.А. Субботин, В.П. Шувалов, А.Ф. Ярославцев]; под ред. В.П. Шувалова. – М.: Горячая линия-Телеком, 2005, т. 3 – 592 с.*

*11. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология Методы и средства обеспечения безопасности Часть 1 Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий [Електронний ресурс]. – Режим доступу до ресурсу: http://www.rfcmd.ru/sphider/docs/InfoSec/GOST-R_ISO_IEC_13335-1-2006.htm*

*12. ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции [Електронний ресурс]. – Режим доступу до ресурсу: http://protect.gost.ru/document.aspx?control=7&id=179072*

*13. Семенов С.Г. Методика математического моделирования защищенной ИТС на основе многослойной GERT-сети / С.Г. Семенов // Вісник Національного технічного університету «Харківський політехнічний інститут». – Х.:НТУ «ХПІ». – 2012. –№62 (968). – С 173-181.*

*14. 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.*

*15. МСЭ-Т Рекомендация G.101. Международные телефонные соединения и цепи – Общие определения //11/2003. [Електронний ресурс]. – Режим доступу: http://www. telecom61.ru›SharedFiles/Download.aspx?...pageid=106*

*16. 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*

*17. 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. – P. 21-30.*

*18. A.B. Bagula Online Traffic Engineering: The Least Interference Optimization Algorithm / A.B. Bagula, M. Botha, and A.E Krzesinski. // IEEE Communications Society – 2004. – P. 1232-1236.*

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


*Поступила в редколлегию 20.08.2015*

**Рецензент:** д-р техн. наук, ст.научн.сотр. С.Г. Семенов, Национальный технический университет «ХПИ», Харьков.

### АНАЛІЗ ТА ДОСЛІДЖЕННЯ МЕТОДІВ УПРАВЛІННЯ МЕРЕЖЕВИХ РЕСУРСІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ АНТИВІРУСНОГО ЗАХИСТУ ДАНИХ

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

*У даній статті аналізуються перспективні методи і засоби антивірусного захисту даних, вимоги забезпечення якості передачі даних в телекомунікаційних системах, основні напрями та підходи математичного моделювання, формулюється завдання розробки методу управління доступом до хмарним телекомунікаційним ресурсам для забезпечення антивірусного захисту даних.*

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

### ANALYSIS AND STUDY METHODS NETWORK MANAGEMENT FOR ANTI-VIRUS PROTECTION OF DATA

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

*This article analyzes the promising techniques and anti-virus protection of data requirements to ensure the quality of data transmission in telecommunication systems, main directions and approaches of mathematical modeling, we formulate the problem of developing a method to control access to cloud-based telecommunication resources for antivirus protection of data.*

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