МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

TP-LINK UKRAINE

TP-LINK®
The Reliable Choice

ТЕЗИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

2 – 5 червня 2014 р.

м. Київ

ISBN: 978-617-696-239-7

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
NATIONAL AVIATION UNIVERSITY
STATE SERVICE OF SPECIAL COMMUNICATION
AND INFORMATION PROTECTION OF UKRAINE
TP-LINK UKRAINE

PROCEEDINGS

OF THE SCIENTIFIC AND PRACTICAL CONFERENCE

«OPERATIONAL AND SECURITY PROBLEMS OF INFORMATION AND COMMUNICATION SYSTEMS»

June, 2 – 5, 2014
Kyiv, Ukraine

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ
TP-LINK UKRAINE

ТЕЗИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

2 – 5 червня 2014 р.
м. Київ, Україна

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ
НАЦИОНАЛЬНЫЙ АВИАЦИОННЫЙ УНИВЕРСИТЕТ
ГОСУДАРСТВЕННАЯ СЛУЖБА СПЕЦИАЛЬНОЙ СВЯЗИ
И ЗАЩИТЫ ИНФОРМАЦИИ УКРАИНЫ
TP-LINK UKRAINE

ТЕЗИСЫ

НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ

«ПРОБЛЕМЫ ЭКСПЛУАТАЦИИ И ЗАЩИТЫ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ»

2 – 5 июня 2014 г.
г. Киев, Украина

УДК 621.39: 004.9 (082)

Вихідні дані офіційної друкованої версії тез:
Проблеми експлуатації та захисту інформаційно-комунікаційних систем: Тези науково-практичної конференції; м. Київ, 2 – 5 червня 2014 р., Національний авіаційний університет. – К.: Вид-во ТОВ «НВП»Інтерсервіс», 2014. – 120 с.

ISBN: 978-617-696-239-7

ОРГКОМІТЕТ КОНФЕРЕНЦІЇ

Голова:

Кулик М.С. — д.т.н., професор, ректор Національного авіаційного університету, заслужений діяч науки і техніки України, лауреат Державної премії України.

Члени оргкомітету:

Харченко В.П. — д.т.н., професор, проректор Національного авіаційного університету з наукової роботи, заслужений діяч науки і техніки України, лауреат Державної премії України в галузі науки і техніки, заступник голови конференції;

Конахович Г.Ф. — д.т.н., професор, завідувач кафедри телекомунікаційних систем Національного авіаційного університету, заслужений працівник транспорту України, заступник голови конференції, **головний редактор редколегії**;

Корнейко О.В. — к.т.н., доцент, заступник Голови Державної служби спеціального зв'язку та захисту інформації України, заступник голови конференції;

Лінник О.О. — голова технічного департаменту ТОВ «ТІПІ-ЛІНК ЮКРЕЙН», заступник голови конференції;

Корченко О.Г. — д.т.н., професор, завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету, лауреат Державної премії України в галузі науки і техніки;

Юдін О.К. — д.т.н., професор, директор Інституту комп'ютерних інформаційних технологій Національного авіаційного університету, член-кореспондент Академії зв'язку України, лауреат Державної премії України в галузі науки і техніки;

Швець В.А. — к.т.н., доцент, завідувач кафедри засобів захисту інформації Національного авіаційного університету.

Секретар:

Голубничий О.Г. — к.т.н., доцент, докторант Національного авіаційного університету.

© Національний авіаційний університет, 2014

УДК 621.396 (043.2)

А.С. Кот, Д.А. Миночкин
НТУУ «Киевский политехнический институт», г. Киев

АДАПТИВНЫЙ АЛГОРИТМ ПЕРЕДАЧИ ОБСЛУЖИВАНИЯ НА ОСНОВЕ ОЦЕНКИ ПОДВИЖНОСТИ ТЕРМИНАЛОВ В СОТОВЫХ СИСТЕМАХ СВЯЗИ

Передача обслуживания – одна из основных особенностей сотовых систем мобильной связи. При передвижении пользователя в системе мобильной связи (СМС) предполагается, что сеть обеспечивает возможности для предоставления абоненту услуг на определенном уровне даже в случае его перемещения из одного района в другой. Это достигается с помощью процедуры изменения точки доступа (хэндовера) абонента с одного сетевого узла на другой. Чрезмерно длительное решение о хэндовере может привести к росту интерференции и повышению вероятности вынужденного прекращения текущего вызова; кроме того, из-за краткого прерывания обслуживания, его качество может ухудшиться ниже допустимого уровня. И напротив – слишком рано принятые решения имеют тенденцию повышать частоту хэндовера, что иногда приводит к выполнению нескольких бесполезных последовательных передач. Такой эффект в сотовых системах связи в современной литературе называют термином «пинг-понг» [1].

Целью данной работы является рассмотрение адаптивного алгоритма передачи обслуживания, позволяющего эффективно бороться с указанными недостатками и повышать тем самым производительность хэндовера.

Стандартные алгоритмы принятия решения о надобности хэндовера строятся оперативно, полагаясь на мгновенную мощность сигнала и твердые пороговые правила. Предлагаемый алгоритм – напротив – заключается в принятии решения о хэндовере на основе неявной информации – оценки мобильности по измерениям мощности сигнала. Положим $S_i(t)$ – мощность сигнала, полученного от ячейки i в момент времени t и $S_i^e(t+\Delta t)$ – ориентировочный уровень по истечении Δt с момента t. В частности мы определяем фактор мобильности передачи θ_{i-j}, который выражен как: $\theta_{i-j} = E_k\left(\frac{dS_i(t)}{dt} - \frac{dS_j(t)}{dt}\right)$, где активная ячейка – i, а целевая – ячейка j. $E_k(\ldots)$ обозначает, что ус-

реднение проводится для любых значений k. Фактор мобильности увеличивается, если скорость или перемещение абонента относительно целевой ячейки j увеличиваются. В случае неизменного направления в течение короткого времени он может быть хорошим индикатором скорости абонента. Необходимо принимать порог измеряемых значений (H_{margin}) достаточно большим во избежание «пинг-понга». Однако, при увеличении H_{margin} до определенного уровня, производительность хэндовера уменьшится, ибо алгоритм, базирующийся на фиксированном пороге хэндовера не достаточно быстр, чтобы среагировать на изменения условий в канале передачи. В итоге, абонент не сможет соединиться с оптимальной БС из-за блокировки по причине ограниченной ёмкости ячейки [2]. Поскольку изменения скорости перемещения пользователя влияют на значение задержки инициации хэндовера (τ_p), время инициирования выполнения хэндовера выражается мгновенными факторами мобильности. Таким образом, предложенный алгоритм передачи состоит из следующих правил:

1) Быстрое решение добавления:

если $S_i^e(t+\Delta t) = S_i(t) + E_k\left(\frac{dS_i(t)}{dt}\right)\Delta t > T_{\text{add}}$, тогда ячейка i добавляется к набору кандидатов;

2) Быстрое решение отклонения:

если $S_j^e(t+\Delta t) = S_j(t) + E_k\left(\frac{dS_j(t)}{dt}\right)\Delta t < T_{\text{drop}}$, тогда ячейка j удаляется из набора кандидатов в соседний набор;

3) Адаптивная задержка для инициирования выполнения хэндовера: когда $S_i(t) - S_j(t) > H_{\text{margin}}$, τ_p задаётся следующим выражением (2): $\frac{\tau_0}{\min(\theta_{i-j}, \theta_{\min})}$; где τ_0 и $\theta_{\min}$ – константы; τ_p может быть обновлено периодом измерения (T_m).

Можно заметить, что когда абонент перемещается к краю ячейки с высокой скоростью, время принятия решений о добавлении в, или удалении из набора кандидатов уменьшается. Быстрое решение добавления обеспечивает выполнение быстрой передачи, в то время как быстрое отбрасывающее решение увеличит ёмкость БС. Данный ме-

тод позволяет осуществить динамичное управление пороговым уровнем отдельного пользователя согласно его мобильности. Для анализа его эффективности было проведено имитационное моделирование. Область моделирования состоит из семи ячеек, с одинаковым радиусом в тысячу метров. Средняя мощность сигнала имеет логарифмическую зависимость от расстояния d_i между БС i и абонентом, в то время как теневое исчезновение – нулевой средний Гауссов процесс u_i с экспоненциально затухающей автокорреляционной функцией [3]. Уровнем сигнала абонента принято $S_i(t)$, полученное от БС i: $S_i(t) = K_1 - K_2 \log(d_i) + u_i(t)$, где K_1 и K_2 зависят от мощности передатчика, функций антенны в БС и сред передачи. Мобильные терминалы в произвольном порядке распределены по всей поверхности (в две группы: первая сосредоточена внутри, вторая – на периферии ячейки). Затем они перемещаются по смоделированной области, независимо друг от друга, на определенном расстоянии. Их начальное направление сгенерировано равномерным распределением $U \in [0,360]$. Предположено, что у пользователей есть постоянная скорость, а их направления изменчивы. По истечении экспоненциально распределенного количества времени со средним значением, равным 10 с, новое направление генерируется Распределением Гаусса со средним значением, равным старому направлению, но с отклонением в 30°. Чтобы исследовать эффект «пинг-понга» согласно τ_p, тег времени используется для указания периода времени, прошедшего с момента последнего успешного хэндовера. Кроме того, предполагается, что все пользователи запрашивают одинаковый тип услуги (фиксированный канал базовой скорости). Вследствие ограниченного количества доступных в системе каналов трафика, важно использовать механизм контроля допустимости вызова, чтобы препятствовать перегрузке системы при процедуре хэндовера. Основным объектом исследования эффективности решения о хэндовере являются ситуации «пинг-понга», при которых наблюдаются повторные передачи обслуживания к предыдущей ячейке перед длительным периодом времени (например, 20 с). Уровень «пинг-понга» определяется отношением количества хэндоверов «пинг-понгом» к общему количеству хэндоверов.

Результаты моделирования приведены для следующих параметров системы: $K_1 = 112{,}7$, $K_2 = 36{,}7$, $T_{\text{add}} = 0$ дБ, $T_{\text{drop}} = -4$ дБ, $\tau_0 = 0{,}15$, период измерения – 20 мс; значения τ_p берутся в диапазо-

не [5,30]. На рис. 1 изображена зависимость количества передач «пинг-понгом» от задержки инициации хэндовера τ_p. Как и предполагалось, при увеличении τ_p возникновение «пинг-понга» уменьшается. Среднее число передач «пинг-понга» более чувствительно к изменению τ_p при уменьшении H_{margin}.

На рис. 2 эффективность адаптивного τ_p рассматривается с точки зрения качества обслуживания. Видно, что при увеличении H_{margin} существует его определённое оптимальное значение. Нагляден выигрыш производительности предложенной схемы у производительностей базируемых фиксированных.

Результаты моделирования показывают, что предложенная схема может значительно поспособствовать улучшению производительности хэндовера даже при недостаточной величине гистерезисного поля.

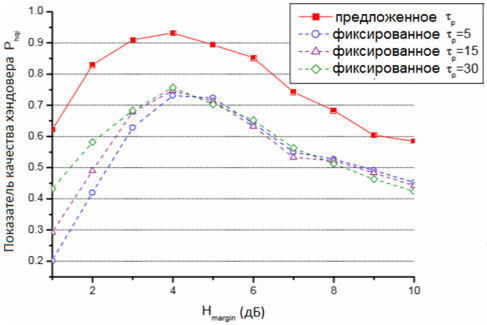

Рис. 1. Зависимость количества передач «пинг-понгом» от задержки инициации хэндовера τ_p

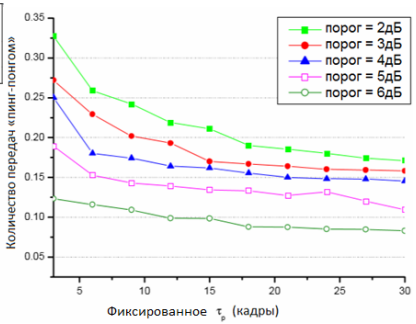

Рис. 2. Зависимость показателя качества хэндовера от H_{margin}

Список литературы

1. Qing-an Zeng and Dharma P. Agrawal. Handoff in Wireless Mobile Networks, Chapter 1, Section 1.3. Handbook of Wireless Networks and Mobile Computing, Edited by Ivan Stojmenovic'. ISBN 0-471-41902-8, 2002.

2. M. Peng, J. Zhang, C. Hu, and W. Wang, "Handover performance analysis in TDD-CDMA cellular network", IEEE Wireless Communications and Networking, vol. 2, pp. 806–811, 2003.

3. F. Santucci, M. Pratesi, M. Ruggieri, and F. Graziosi, "A general analysis of signal strength handover algorithms with co-channel interference", IEEE Transactions on Communications, vol. 48, no. 2, pp. 231–241, 2000.

УДК 621.396.49 (043.2)

Д.А. Миночкин, И.А. Кушниренко
НТУУ «Киевский политехнический институт», г. Киев

МОДЕЛИРОВАНИЕ СПУТНИКОВЫХ MIMO КАНАЛОВ

В последнее время в беспроводных сетях широко применяется технология MIMO. В случае с использованием нескольких антенн для передачи-приёма в наземных системах, существуют хорошо описанные подходы моделирования каналов передачи данных. Применение MIMO технологии при построении спутниковых систем связи имеет ряд особенностей. Эти особенности делают невозможным оценку сигнала методами, описанными для наземных систем. Для оценки MIMO каналов спутниковых сетей не существует единого систематизированного метода и подхода к расчёту.

Целью данной работы является рассмотрение существующих методик расчёта спутниковых каналов, и определение систематизированного подхода к оценке параметров системы связи. Рассмотрим следующие модели MIMO каналов для спутниковых систем.

Физическо-статистическое моделирование предполагает использование L-диапазона (1–2 ГГц) или S-диапазона (2–4 ГГц) излучения. Модель строится на основе кластеров. Кластеры – это группы препятствий, которые имеют сферическую форму. Центр кластера позиционируется случайным образом. Высоты зданий нормируют по логарифмическому закону, двадцать предполагаемых рассеивателей расположены случайным образом вокруг центра кластера, коэффициент рассеивания подчиняется закону Лапласа. Плотность зданий достигает 90% процентов кластеров, имитирующих городские условия. Если же кластер моделирует пересечённую местность – то 90% кластера занимают деревья. Сигналы переотражаются от кластеров и могут блокироваться между построек в отдельном кластере. Каждому рассеивателю в кластере случайным образом определён равномерный коэффициент отражения. В этой модели описывается три случая распространения сигнала – распространение в свободном (космическом) пространстве, распространение при отсутствии прямой видимости, распространение при прямой видимости. При расчёте, такие параметры, как неравномерность при измерениях, коэффициент ослабления, коэффициент отражения, определены в спецификациях, полученных при проведении измерений в г. Мюнхен, Германия, при излучении на частоте 1,54 ГГц.

Суть увеличения выигрыша при использования MIMO – уменьшение взаимной корреляции между каналами передачи данных, что достигается с помощью значительного пространственного разделения антенн, как один из возможных вариантов. Однако, такой подход делает невозможным использование в качестве наземного терминала небольшого подвижного объекта.

Альтернативным решением является использование 2x2 MIMO системы, в которой обе передающие антенны находятся на одном спутнике, и при этом одна из них излучает с правой круговой поляризацией, а другая – с левой. На приёмной стороне размещают обе антенны рядом друг с другом с использованием соответствующей конфигураций [1, 2]. Такая архитектура позволяет использовать 4-ре канала передачи данных – между антеннами с одинаковой поляризацией, и 2 кросс-поляризационных канала. Физическо-статистическая модель с использованием разных поляризаций предполагает, что в случае с отсутствием помех на пути распространения сигнала все каналы взаимокоррелированы, а в случае многолучевого распространения (переотражений), взаимокорреляция каналов пропадает. Параметры излучения антенн описываются теоремой Стокса, и полностью представлены в работе [3]. Данный вариант модели позволяет достаточно точно описать широкополосный канал передачи данных.

При физизическо–статистическом моделировании модель использует частоты L-диапазона (1–2 ГГц) или S-диапазона (2–4 ГГц). Если же необходимо провести оценку в диапазоне Ku (12–18 ГГц) и выше, можно использовать аналитическое моделирование. Аналитическая модель базируется на использовании двух передающих антенн от двух разных спутников, терминальная станция оборудована двумя соотнесёнными антеннами. Также в описании этой модели представлены пространственное мультиплексирование для двух передающих и двух приёмных антенн, и аналитические выражения для оценки потерь в канале. Модель даёт возможность оценить не только ёмкость канала, но и уровень мощности сигнала на приёмной стороне, учитывая потери в свободном пространстве, а также и потери, вносимые гидрометеорами.

Общие потери оцениваются следующим образом:

$$A_i = FSL_i + A_{r_i},$$

где: $FSL_i = 10\lg\left(\frac{4\pi d_i f}{c}\right)$ – потери в свободном пространстве;

f – частота передачи данных;

c – скорость света;

i – номер канала;

A_{r_i} – терм, описывающий затухания сигнала из-за дождя.

Данная реализация моделирования актуальна при больших отношениях сигнал/шум, и показывает преимущество использования MIMO системы перед SISO в конкретном случае.

Эмпирически-статистическая модель MIMO канала для спутника строится на базе данных множества серий экспериментов и измерений. В этой модели также рассматривается 2x2 МИМО канал, т.е. используется две приёмные и 2 передающие антенны с разными поляризациями. Соответственно, в модели также рассматривается 4 канала, два между антеннами с одинаковой поляризацией, и два между кросс-поляризационными антеннами. Отличительная особенность данной модели состоит в том, что она позволяет проводить оценку не только узкополосных, но и широкополосных каналов. Данные измерений полностью представлены в [4]. В модели для описания различных состояний каналов передачи данных используются цепи Маркова, где каждое состояние цепи симулирует одно из возможных состояний канала. Следует отметить, что и в узкополосной и в широкополосной моделях эффекты затухания подчиняются логнормальному закону, и учитываются в каждом состоянии цепи Маркова. Метод моделирования позволяет определить коэффициент кросс-корреляции между двумя каналами с учётом эффектов долгосрочных затуханий, и вероятность нахождения исследуемой системы или канала в конкретном состоянии. Широкополосная модель описывается матрицей состояний, в которой задаётся поляризация антенн. Амплитуды, задержки распространения и фазы для каждого случая распространения сигнала, являются функциями зависимости от времени, так как или терминал или спутник (в любом случае) являются подвижным. Необходимо ещё раз подчеркнуть, что данный метод моделирования строится на основании измерений.

В работе были рассмотрены аналитические модели для расчета и оценки спутниковых каналов с использованием технологии MIMO. Можно сделать вывод, что стандартные модели играют основную

роль при оценке производительности и качества проектируемых сетей связи. Все описанные подходы моделирования направлены на уменьшения влияния таких факторов, как ограниченная мощность передатчика, установленного на спутнике, значительные потери и искажения при распространении сигнала, отсутствие прямой видимости.

Физическо-статистическая, учитывающая концепцию разделения по поляризации излучаемых сигналов, актуальна для L и S диапазонов излучения и позволяет моделировать каналы передачи данных, для которых может использоваться от одного до нескольких спутников. Если используется один спутник, то передаваемые сигналы необходимо обязательно разделять по поляризации.

Аналитическая модель описана для случая 2x2 MIMO системы, где передающие сигналы имеют одинаковую поляризацию, или она не учитывается. Этот подход даёт возможность исследовать эффекты дифракции, возникающие в канале передачи данных и рассчитать ёмкость канала.

Эмпирически-статистическая модель позволяет работать как с узкополосными, так и с широкополосными системами, и полностью построена на данных, полученных из различных серий измерений. Система эмпирически-статистического моделирования в первую очередь описана для 2x2 MIMO канала, и используется для оценки затуханий в спутниковых MIMO каналах.

Таким образом, выбор подхода моделирования зависит не только от диапазона излучения и возможной архитектуры сети, но и от необходимости исследовать конкретные параметры системы.

Список литературы

1. Hult, T., and Mohammed, A. (2008). Evaluation of Depolarization Effects on the Performance of High Altitude Platforms (HAPs). IEEE 67th Vehicular Technology Conference, VTC08-Spring, Singapore.

2. Hult, T., Mohammed, A. Yang, Z., and Grace, D. (2010). Performance of a Multiple HAP System Employing Multiple Polarization. Invited Paper, Special Issue, Springer Wireless Personal Communications Journal, 52(1), 105–117.

3. King, P.R., Evans, B.G., and Stavrou, S. (2005). Physical-Statistical Model for the Land Mobile-satellite Channel Applied to Satellite/HAP MIMO. 11th European Wireless Conference.

4. King, P.R. (2007). Modelling and Measurement of the Land Mobile Satellite MIMO Radio Propagation Channel. Ph.D. Thesis, Centre for Communication Systems Research, University of Surrey, Guildford, UK.

УДК 004.051 (043.2)

М.Г. Булах
Национальный авиационный университет, г. Киев

МОДИФИЦИРОВАННЫЙ АЛГОРИТМ МУЛЬТИПЛИКАТИВНОГО ИНВЕРТИРОВАНИЯ В ДВОИЧНОМ ПОЛЕ

Криптографические преобразования с открытым ключом получили широкое применение в различных информационного-телекоммуникационных системах. Среди таких преобразований, наиболее активно применяются криптографические преобразования на эллиптических кривых (ЭК) над конечными полями. Так, в качестве национального стандарта электронной цифровой подписи на Украине принят ДСТУ 4145-2002, в основе которого лежат криптографические преобразования на ЭК над двоичным полем. Основной операцией в преобразованиях на ЭК является операция скалярного умножения точки ЭК, основывающаяся на операциях сложения и удвоения точек ЭК. Результирующая точка в удвоении и сложении точек ЭК вычисляется по формулам на основе координат складываемых и удваиваемых точек. Над координатами точек выполняются операции умножения, сложения, возведение в квадрат и мультипликативное инвертирование в двоичном поле. Операция мультипликативного инвертирования является наиболее вычислительно сложной среди перечисленных: занимает 10-20 операций умножений. Поэтому актуальной научно-технической задачей является сократить вычислительную сложность операции мультипликативного инвертирования.

Для вычисления мультипликативного инвертирования $a \in \mathbf{GF}(2^m)$ используется расширенный алгоритм Эвклида (РАЭ). Алгоритм основан на цикличной модификации двух инвариантов $ba + df = u$ и $ca + ef = v$, для некоторых d и e, которые вычисляются неявно, а f-неприводимый полином. В цикле производится уменьшение u и увеличение b, причем на каждой итерации вычисляется $\deg(u)$ и $\deg(v)$. Отметим, что степень u уменьшается, а степень b – растёт. Таким образом, ключевыми операциями в алгоритме являются операции над полиномами: вычисления степени, сложения и сдвига.

Автором предлагается уменьшить сложность операции вычисления степени полинома за счет того, что степень u постоянно уменьшается, хотя бы на 1. Это позволяет отказаться от вычисления степени u, в общем виде, на каждой итерации цикла, а лишь заниматься ее уточнением, основываясь на текущем значении степени. То есть вычисления степени полинома на текущей итерации происходит с учётом известной степени предыдущей итерации. Что сокращает количество операций над элементами массива, представляющем элемент поля, в 2 раза.

С другой стороны, степень v, является либо постоянной, либо равна степени u, с предыдущей итерации. Это позволяет избавиться от вычисления степени v, в принципе.

Так как степень v и u постоянно уменьшается, а степень b и c постоянно растет, предлагается сдвигать и складывать не все элементов массива, представляющем элемент поля, а лишь значимые – заведомо отличные от нуля. Что сокращает количество операций над элементами массива в 2 раза.

При программной реализации предложенного модифицированного алгоритма, учитывалась особенность суперскалярной архитектуры 32-х разрядных процессоров и возможности современных компиляторов по предсказанию переходов, параллельному выполнению команд, разворачиванию циклов.

Программная реализация выполнялась на языке высокого уровня C++, в среде Microsoft Visual Studio, в конфигурации Release с помощью компилятора Intel C++ Compiler XE2013 (/O3, поддержка SSE4.2) для 32-разрядных платформ. В экспериментах было учтено, что степень инвертируемого полинома, может влиять на количество итераций основного цикла, поэтому рассматривались полиномы степени близкой к максимальной, для полей, из ДСТУ 4145-2002 и FIPS-186-3. Замеры производительности производились на наиболее распространенных настольных процессорах 3-го поколения Intel Core i5-3570 и 4-го поколения Intel Core i5-4670 под управлением ОС Windows 7 SP1 x86-64.

Предложенные подходы к оптимизации алгоритма мультипликативного инвертирования в поле $\mathbf{GF}\left(2^m\right)$, позволили уменьшить вычислительную сложность модифицированного РАЭ (МРАЭ) в 2 раза, что подтверждается экспериментальными оценками.

Программная реализация МРАЭ, обладает, в среднем, большей на 15-20% производительностью, чем РАЭ.

УДК 004.056.53 (043.2)

О.Г. Голубничий, Г.Ф. Конахович
Національний авіаційний університет, м. Київ

АНАЛІЗ НОРМАТИВНИХ РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ НАСКРІЗНОГО ЗВ'ЯЗКУ «ПОВІТРЯ–ЗЕМЛЯ» У МЕРЕЖІ ATN

Відповідно до нормативного документа ICAO [1], основні положення якого щодо забезпечення інформаційної безпеки мережі авіаційного зв'язку (ATN) були проаналізовані в [2], захист наскрізного зв'язку (end-to-end communication) «повітря–земля» в ATN, яка використовує пакет протоколів Інтернет (IPS), повинен здійснюватися з використанням протоколу обміну ключами в Інтернеті версії 2 (IKEv2) та протоколу управління шифруванням (ESP) захисту Інтернет-протоколів (IPsec).

На рис. 1 показані варіанти захисту наскрізного зв'язку «повітря–земля» [1], які використовують інтерфейс вузла-кореспондента з сервером, що має сертифікат PKI (інфраструктура відкритих ключів).

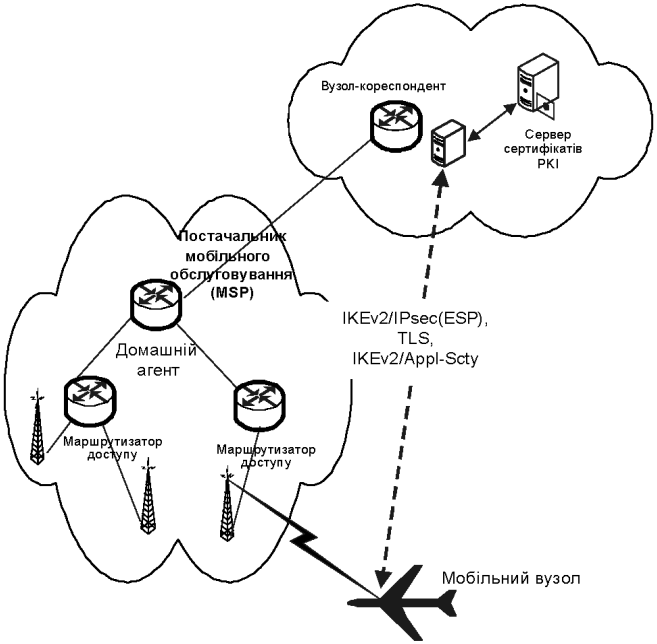

Рис. 1. Структура організації захисту наскрізного зв'язку «повітря–земля»

Вибір інтерфейсу проводиться на локальному рівні. Це може бути інтерфейс з базою даних сертифікатів X.509 та списків відкликаних сертифікатів (CRL) з використанням спрощеного протоколу доступу до каталогів (LDAP) або іншого протоколу управління сертифікатами. Для ESP та IKEv2 використовується пакет алгоритмів «Suite-B», який зазначено в RFC 4869. Профіль сертифікатів і CRL «Suite-B» ідентифікує повідомлення управління сертифікатами за допомогою протоколу CMS (відповідно до вказівок RFC 2729), який є прийнятнішим протоколом. Питання про вибір фактичного метода автентифікації в адміністративному домені вирішується на локальному рівні та залежить від застосування. IKEv2 допускає використання спільно використовуваних ключів або цифрових сертифікатів, причому надійнішим методом вважаються цифрові сертифікати. Спільно використовувані ключі можуть використовуватися в напрямку «вниз», а цифрові сертифікати – в напрямку «вгору». Оскільки в мобільному вузлі відсутній практичний спосіб незалежної перевірки списку відкликаних сертифікатів (CRL), у напрямку «вгору» можуть використовуватися сертифікати з коротким строком дії. У напрямку «вниз» у випадку використання цифрових сертифікатів рекомендують, щоб мобільний вузол замість надсилання фактичного сертифікату використовував формат «hash and URL». За допомогою цього методу мобільний вузол надсилає URL сервера сертифікатів PKI, в якому вузол-кореспондент може отримати власний сертифікат. Цей метод використовує сертифікати для автентифікації, якщо необхідна надійна ідентифікація. Такий підхід є прийнятнішим в умовах наскрізного зв'язку, хоча в цьому випадку можна використовувати IKEv2 та розширюваний протокол автентифікації (ESP) з інфраструктурою автентифікації, авторизації та обліку (AAA). Очікується, що концепція моста PKI, яка була запропонована Робочою групою з захисту цифрового зв'язку (DSWG) Асоціації повітряного транспорту (ATA), пришвидшить впровадження PKI на глобальній основі. Відповідно до концепції моста PKI кожен адміністративний домен може направляти сертифікат на центральний міст замість проведення кожним адміністративним доменом перехресної сертифікації з іншими адміністративними доменами.

Захист наскрізного зв'язку «повітря–земля» на транспортному рівні передбачає використання мобільними вузлами та вузлами-кореспондентами в ATN/ IPS протоколу захищеного передавання даних (TLS) відповідно до вказівок RFC 5246. Таким чином, застосуван-

ня, які вже використовують TLS, можуть використовуватися в зв'язку «повітря–земля» в мережі ATN/ IPS. При використанні TLS необхідний такий метод шифрування, який визначений в RFC 4492: TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA.

Цей метод шифрування передбачено використовувати в таких варіантах:

1) Протокол захищеного передавання даних (TLS). Допускається використання версій 1.0 або 1.1.

2) Погодження про обмін ключами з використанням еліптичної кривої Дифі-Хелмана (ECDH).

3) Алгоритм еліптичної кривої для створення цифрового підпису (ECDSA) для автентифікації клієнта.

4) Стандарт криптографічного захисту (AES) з розміром блока 128 в режимі зчеплення блоків шифротексту (CBC) для забезпечення конфіденційності.

5) Алгоритм криптографічного хешування (SHA), версія 1 для забезпечення цілісності (тобто для хеш-коду автентифікації повідомлення HMAC).

Цей метод шифрування було обрано тому, що він має спільні алгоритми з алгоритмами для IPsec та IKEv2 у зв'язку «повітря–земля». Слід враховувати, що цей метод шифрування є обов'язковим для серверів, і клієнти також можуть використовувати його для забезпечення відповідності вимогам RFC 4492.

Захист наскрізного зв'язку «повітря–земля» на прикладному рівні передбачає можливість мобільним вузлам та вузлам-кореспондентам в ATN/IPS використовувати заходи захисту прикладного рівня на границі діалогового сервісу IPS. Цей альтернативний варіант призначений для застарілих застосувань ATN, які вже використали заходи захисту прикладного рівня в мережі ATN/OSI. В цьому випадку мобільні вузли та вузли-кореспонденти включають до повідомлення о застосуваннях код автентифікації повідомлень HMAC-SHA-256. Код HMAC-SHA-256 вже є необхідним для ESP та IKEv2, тому такий варіант не передбачає необхідності використання додаткових криптографічних методів. Тег HMAC, усічений до 32 біт, розраховується через конкатенацію даних користувача з порядковим номером відправлення для захисту при повторі. Протокол IKEv2 є стандартним, тому, якщо у зв'язку «повітря–земля» використовуються заходи захисту на прикладному рівні, IKEv2 також використовується для визначення ключів.

Вищенаведені матеріали показують, що процедури захисту інформаційних ресурсів при здійсненні наскрізного зв'язку «повітря–земля» в мережі ATN/IPS, які рекомендовані нормативними документами ICAO, повинні реалізовуватися на мережному, транспортному та прикладному рівнях систем цифрового авіаційного зв'язку. При цьому чітко не зазначаються жорсткі критерії необхідного (гарантованого) рівня захисту (критерії оцінки захищеності інформації від несанкціонованого доступу) і в той же час регламентуються до використання заходи із захисту інформації на основі IPsec, IKEv2 та ESP.

Пропонується розроблення моделей загроз та визначення функціональних профілів захищеності для автоматизованих систем (АС) авіаційного призначення, які використовують наскрізний зв'язок «повітря–земля» в мережі ATN/IPS, виконувати з урахуванням досвіду розроблення моделей загроз та визначення функціональних профілів захищеності для АС класу «2» та класу «3», функціонування яких базується на стандартних телекомунікаційних каналах, що використовують стандарти та протоколи пакету протоколів Інтернет (IPS).

Враховуючи концепцію впровадження у перспективні системи цифрового авіаційного зв'язку способів передавання, що використовують багатопозиційні методи модуляції та широкосмугові технології, також пропонується підвищувати ступінь захищеності таких систем зв'язку на їх фізичному рівні (наприклад, використовуючи властивість прихованості складних сигнально-кодових конструкцій).

Список літератури

1. Руководство по сети авиационной электросвязи (ATN), использующей стандарты и протоколы пакета протоколов Интернет (IPS): Doc 9896 AN/469. – Издание первое. – Международная организация гражданской авиации (ICAO), 2010. – 112 с.

2. Голубничий О.Г. Аналіз вимог та рекомендацій ICAO щодо забезпечення інформаційної безпеки мережі ATN / О.Г. Голубничий // Захист інформації. – Жовтень-грудень 2013. – Том 15, № 4. – С. 376 – 382.

УДК 004.735 (043.2)

А.М. Афанасьєв
Національний авіаційний університет, м. Київ

АНАЛІЗ ВПРОВАДЖЕННЯ МЕРЕЖ СТАНДАРТУ LTE В СВІТІ

Мережні оператори в усьому світові працюють, щоб переконати своїх користувачів перейти на LTE. Термін «4G» виступає як зручний ярлик у маркетологів, щоб підкреслити переваги цього нового стандарту над його попередниками. Але як оцінити реальний досвід користувачів на LTE?

Додаток компанії OpenSignal дозволяє користувачам внести свій внесок у незалежні карти покриття мобільних мереж. Компанія взяла дані 6 мільйонів користувачів LTE і зосередилася на двох ключових показниках: швидкості завантаження й частку часу доступу до LTE. Всі дані, включені у звіт компанії, відносяться до другої половини 2013 року.

Середній час на 4G LTE: нова метрика оцінки покриття. Цей показник являє собою новий спосіб подивитися на покриття на основі користувальницького досвіду, а не географії. Найбільш важливо, де користувачі насправді проводять свій час, особливо для LTE (тому що ця послуга забезпечує рівень сервісу, що не є необхідним на випадок надзвичайних ситуацій, на відміну від голосу або основного підключення до Інтернету). Метрика OpenSignal (рис. 1) дивиться на частку часу, коли користувач має доступ до мережі LTE, що дає більш точну картину в реальному світі. Коли справа доходить до охвату LTE, не всі місця рівні.

Для цієї метрики, ми наглядно бачимо, що Південна Корея лідирує – звичайний користувач має доступ до LTE 91% часу. Найефективніші індивідуальні мережі – в Tele 2 (Швеція), чиї користувачі мають LTE-доступ 93% часу. Однак загальний показник по країні складає тільки 88% часу. Російський показник поки становить лише 42%.

Топ країн (рис. 2) істотно змінюється, коли ми дивимося на швидкість доступу. Найшвидший LTE виявляється в Австралії – 24,5 Мбіт/с. Росія на тринадцятому місці за цим показником, що складає 12,4 Мбіт/с. Але це не заважає країні обійти США, де швидкість удвічі менше – 6,5 Мбіт/с, і прогресивну в технологіях Японію, де середня швидкість складає порядку 11,8 Мбіт/с.

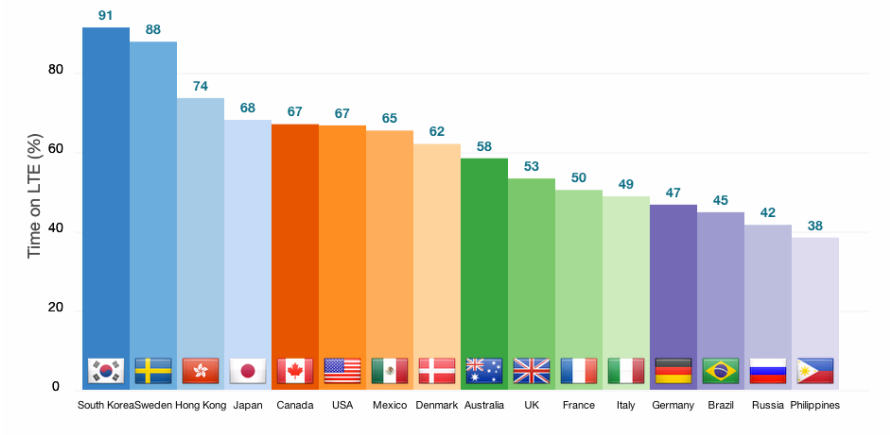

Рис. 1. Метрика OpenSignal щодо впровадження LTE у світі

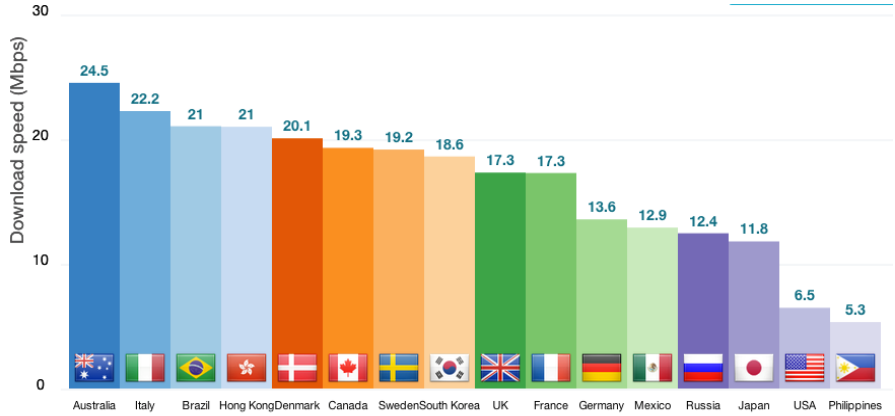

Рис. 2. Рейтинг країн за швидкістю доступу в мережі LTE

Головний козир 4G LTE – це значне збільшення швидкостей у порівнянні з технологіями 3G (дослідження враховує HSPA+ як форму технології 3G, хоча вона часто підносить як 4G маркетологами різних країн).

Мобільні мережі не застигають у розвитку, оператори постійно вносять поліпшення у свої мережі. З іншого боку, постійне збільшення навантаження на мережі через розвиток абонентських пристроїв знижує середню швидкість. Це причина того, що деякі країни

поліпшили показники звіту, зібраного рік назад, у той час як інші - погіршили.

Австралія і Японія домоглися найбільших поліпшень, середня швидкість в Австралії виросла на 42%, у Японії - на 66%. У США ж навпаки - швидкості впали на 32%.

Усе більше країн розвивають у себе LTE. Дослідження підтвердило (рис. 3), що в середньому LTE є найшвидшою бездротовою технологією передачі даних, що надає реальне збільшення швидкостей у порівнянні з 3G й HSPA+.

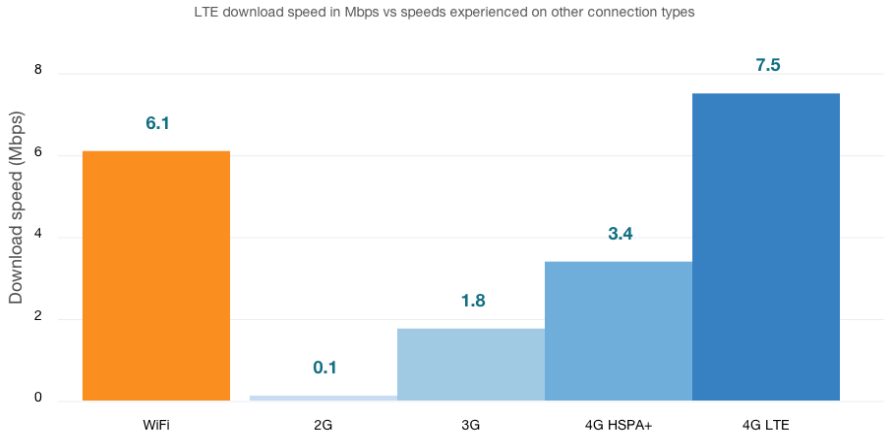

Рис. 3. Дослідження швидкостей технологій передачі даних

4G LTE більш ніж в 5 разів швидше, ніж 3G і більш ніж у два рази швидше HSPA + й являє собою величезний крок уперед у технологіях бездротового зв'язку.

Не всі LTE мережі створені рівними. Тільки біля чверті мереж мають і гарне покриття й високу швидкість.

Залишається ще дуже багато роботи, перш ніж LTE повністю розкриє свій потенціал.

УДК 004.056.5 (043.2)

С.В. Соколовский
НТУУ «Киевский политехнический институт», г. Киев

ЭФФЕКТИВНАЯ ИДЕНТИФИКАЦИЯ АБОНЕНТОВ С ИСПОЛЬЗОВАНИЕМ БУЛЕВЫХ ФУНКЦИЙ

Динамическое расширение и углубление информационной интеграции во всех сферах человеческой деятельности стимулирует количественное и качественное развитие многопользовательских компьютерных систем. В рамках таких систем реализуется коллективный доступ к информационным ресурсам. Идентификация абонента таких систем является важным звеном в организации контроля над доступом к этим ресурсам.

Идентификации абонентов интегрированных систем к настоящему времени выполняется либо с использованием паролей, либо основе теоретической концепции “нулевых знаний”. В литературе использование паролей получило название “слабой” идентификации, что связано возможностью их перехвата, а также потенциальной возможностью доступа к ним со стороны системы. Идентификация на основе концепции “нулевых знаний” лишена этих недостатков. Сущность самой концепции состоит в том, что каждый абонент может генерировать сеансовые пароли. В системе есть средства проверки корректности этих паролей. Такая идентификация исключает всякую возможность получения паролей путем доступа к информации, хранящейся в системе, а также делает бесполезным перехват паролей.

Вместе с тем, на практике идентификация с использованием паролей используется достаточно широко. Это обусловлено сложностью реализации известных механизмов реализации концепции “нулевых знаний” на основе мультипликативных модулярных операций, выполняемых над числами большой разрядности.

Предлагается механизм реализации идентификации на основе концепции “нулевых знаний” с использованием булевых функциональных преобразований. Существующие механизмы реализации идентификации на основе концепции “нулевых знаний”, основаны на аналитической неразрешимости задачи дискретного логарифмирования. Аналитически неразрешимые задачи есть и в булевой алгебре. На их основе можно построить алгоритмы, реализующие концепцию “нулевых знаний” с использованием булевых преобразований, вычисли-

тельная реализация которых на порядки проще по сравнению с мультипликативными операциями модулярной арифметики, выполняемыми над числами, разрядность которых превышает тысячу.

Сущность предлагаемого подхода состоит в том, что абонентом генерируется булево необратимое функциональное преобразование $Y = F(X)$, такое, что обратное к нему преобразование $X = \Psi(Y)$ является неоднозначным. Это значит, что абонент имеет множество $\Omega = \{X_1, X_2, \ldots, X_m\}$ входных кодов (сеансовых паролей) для которых результат функционального преобразования $F(X)$ одинаков: $F(X_1) = F(X_2) = \ldots = F(X_m) = Y$. Необратимое булево функциональное преобразование $F(X)$ формируется абонентом по разработанной методике в специальном процедурной форме (то есть в виде процедуры его вычисления). Эта процедурная форма, подобно известному алгоритму DES, содержит таблицы нелинейных преобразований (S-блоки). Эти таблицы, вместе с кодом Y составляют открытый ключ абонента, который сообщается системе в процессе его регистрации. По таблицам и коду Y, в силу необратимости преобразования $F(X)$ невозможно восстановить значение X, для которого $F(X) = Y$. Поэтому вся сохраняемая в системе информация об открытых ключах зарегистрированных абонентов не является секретной.

При обращении абонента к системе, он посылает ей один из сеансовых паролей X_t, принадлежащих множеству Ω: $X_t \in \Omega$. Система, используя таблицы процедурной формы вычисляет значение $F(X_t)$ и сравнивает полученный результат с Y. Если $F(X_t) = Y$, то абонент успешно идентифицирован системой.

Основным достоинством предложенного подхода является простота и высокая скорость реализации. Так, экспериментально доказано повышение скорости идентификации на 2–3 порядка по сравнению с известными механизмами реализации “строгой” идентификации. При длине сеансового пароля кода доступа 256 бит, множество Ω содержит около 4000 сеансовых паролей, для которых результат преобразования $F(X)$ одинаков.

Экспериментальные исследования доказали, что по критерию сложности и скорости идентификации, предложенный способ вполне соизмерим с использованием паролей. При этом, при его использовании обеспечивается значительно больший уровень надежности идентификации по сравнению с использованием паролей.

УДК 004.735 (043.2)

Т.Я. Малік
Національний авіаційний університет, м. Київ

ПРОЕКТУВАННЯ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ ПІДПРИЄМСТВА ЗА ДОПОМОГОЮ САПР

Для автоматизації проектних робіт у різних галузях виробництва розроблені й успішно експлуатуються системи автоматизованого проектування (САПР). Ці системи значно збільшують продуктивність роботи конструктора, істотно скорочують терміни розробки, а у деяких складних галузях (як проектування інтегральних схем) взагалі є просто необхідними. При проектуванні нової мережі, треба врахувати великий об'єм інформації, визначити яке обладнання використати, як його налаштувати, і багато іншого. Цей процес значно спрощує використання САПР. Найбільшого розвитку у світі досягли системи автоматичного проектування графічних моделей, деталей. Такі системи активно використовуються, просто необхідні при роботі, у сферах тяжкої промисловості, інтегральних мікросхем, і багатьох інших напрямах, де є необхідність у великомасштабних і точних проектах. До таких САПР відносяться Autodesk AutoCAD, Autodesk Inventor, DSS SolidWorks, АСКОН КОМПАС 3D та інші. Доля САПР, розроблених для проектування мереж, є значно менш затребуваною, але деякі системи дуже допомагають у цій сфері проектування.

Я спроектував мережу для підприємства, робота якого базується на обробці даних, заявок, проведенні різних розрахунків і прогнозів, базуючись на інформації з баз даних (БД). Подібні організації часто називають Дата-центрами. Для свого проекту я задіяв ресурси відомої російської САПР – «NetWizard». Робота із системою «NetWizard» відбувається в інтерактивному режимі на сайті www.netwizard.ru. При цьому досвідчений інженер може оперувати численними параметрами відповідно до міжнародних стандартів RFC і IEEE і вручну уточнювати пропоновані системою варіанти встаткування. У найпростішому ж випадку Web-проектувальник попросить відповісти на кілька нескладних питань, а потім автоматично сформує готовий звіт.

Основною метою мого проекту, є практичне застосування САПР для проектування великої мережі підприємства. За допомогою САПР, вносячи необхідні дані про майбутнє підприємство, я підібрав активне

і пасивне мережеве обладнання. Мій проект мережі розрахований на 300 робочих станцій (PC) і 4 файлових сервера, на яких зберігаються БД, різні програмні утілити і документація, для вільного доступу працівників. Щоб об'єднати всі ці компоненти я, за рекомендацією САПР, використовую вісім комутаторів D-Link DGS-3620-52T які, за допомогою восьми десятигігабітних кабелів DEM-CB300CX об'єднані у два стеки по чотири. Одна з переваг вибору продукції D-Link, заключається у спроможності такого об'єднання у стек, в результаті якого проектувальник отримає фактично 2 комутатори з великою кількістю портів (по 192 порта Gigabit Ethernet і по 16 SFP портів для конкретно мого проекту). Підключення до серверів і PC реалізується за допомогою кабелю «витої пари»; між собою два стекових комутатора з'єднуються за допомогою оптоволоконних ліній зв'язку (ВОЛЗ). Підключення з провайдером (вихід до всесвітньої мережі інтернет) також відбувається за допомогою ВОЛЗ, так як підприємство подібних масштабів має забезпечити високу пропускну спроможність для своїх працівників. Для розміщення мережі підприємства, зважаючи на кількість працівників, я вважаю доцільним орендувати три поверхи офісної будівлі. Дані про площу і параметри поверхів були занесені до системи проектування, і враховувалися при розрахунку пасивного мережевого обладнання (кабелів, патч-панелей…). Крім заощадження часу, використання САПР у проектуванні дає можливість перевірити різні підходи до майбутнього проекту, наприклад яку топологію мережі буде краще використовувати, порівняти вартість обладнання різних вендорів (виробників мережевої продукції) в цілому прийняти оптимальні рішення, які потребують високого досвіду від проектувальника.

У результаті проведеної роботи, я розробив проект великої корпоративної мережі (на 300 PC) за допомогою САПР. Використання системи автоматизованого проектування заощадило багато часу і розрахунків. Підбір різного обладнання, і проектувальні рішення, які були задіяні у даній роботі, зайняли би додаткових 8 годин, а якщо проектом займалася би недосвідчена особа, то ця цифра була би значно більшою. Ефективність використання САПР вже давно оцінена у різних сферах виробництва, і вона очевидна кожному.

УДК 004.735 (043.2)

О.В. Дубров
Національний авіаційний університет, м. Київ

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВПРОВАДЖЕННЯ МЕРЕЖІ МОБІЛЬНОГО ЗВ'ЯЗКУ 4G

Технологія 4G – це перспективне покоління технологій мобільного зв'язку, яке тільки розвивається на теренах України. Вона характеризується високою швидкістю передачі даних і підвищеною якістю голосового зв'язку.

Пропонується розгортання мережі на базі технології LTE та визначення показників економічної ефективності. Спочатку пропонується розробити покриття на території центра міста Києва з можливістю подальшого розширення до національної мережі. Оскільки це територія ділового центру столиці та найбільш населена вона має найбільший попит на послуги мобільного зв'язку та доступу в Інтернет.

Впровадження технології LTE дозволить операторам зменшити капітальні і операційні затрати і, як наслідок, підвищить доходи від надання послуг передачі даних, розширить можливість в області конвергенції (зближення) послуг і технологій, надасть можливість одночасної роботи значної кількості активних користувачів в кожній соті. З боку абонента різке збільшення швидкості передачі даних серйозно поліпшить якість надаваних послуг, що, в свою чергу, сприятиме поширенню нових платних мультимедійних сервісів (соціальних мереж, багатокористувацьких ігор, систем моніторингу, відеоконференцій).

У роботі розглянуто кілька варіантів впровадження мережі 4G та обрано найбільш ефективний варіант її використання. Розрахунки показали, що у випадку застосування запропонованого варіанту впровадження інвестор почне отримувати прибутки вже на п'ятому році існування мережі. В інвестиційному менеджменті цей період розглядається як середньотривалий. Відповідно до даної інвестиційної пропозиції створена на практиці мережа LTE буду мати переваги перед конкуруючими варіантами технологічних рішень, в неї буде перспектива стати ефективною та принести значний прибуток.

УДК 004.772 (043.2)

О.В. Андрощук
Національний авіаційний університет, м. Київ

МЕХАНІЗМИ РЕАЛІЗАЦІЇ ПОСЛУГ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ПЕРЕДАЧІ ДАНИХ

Для значної кількості важливих прикладних застосувань необхідний рівень забезпечення гарантій захисту – Г4 і вище. Проблемність реалізації вказаного рівню захисту полягає в тому, що в Україні не має сертифікованих технічних засобів захисту, що здатні реалізувати названий вище рівень гарантій. При передачі даних через незахищене середовище існує можливість перехоплення їх зловмисниками. Цю можливість необхідно нейтралізувати. Застосування алгоритмів шифрування до IP пакетів у цілому не є ефективним, оскільки у цьому випадку не буде здійснюватися маршрутизація. Тому в більшості випадків використовується технологія VPN. VPN (англ. Virtual Private Network – віртуальна приватна мережа) (рис. 1) – узагальнена назва технологій, що дозволяють забезпечити одне або декілька мережевих з'єднань(логічну мережу) поверх іншої мережі (наприклад, Інтернет).

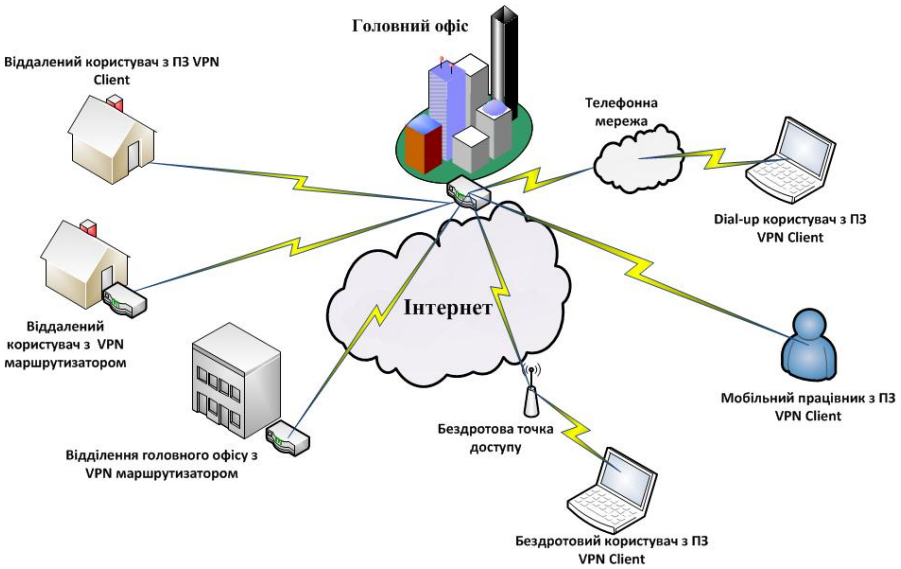

Рис. 1. Корпоративна віртуальна приватна мережа

Сьогодні технологія VPN завоювала загальне визнання і будь-який адміністратор вважає своїм обов'язком організувати VPN-канали для співробітників, що працюють поза офісом. VPN представляє собою об'єднання окремих машин або локальних мереж у віртуальній мережі, яка забезпечує цілісність і безпеку переданих даних. Вона має властивості виділеної приватної мережі і дозволяє передавати дані між двома комп'ютерами через проміжну мережу, наприклад, Internet. VPN відрізняється низкою економічних переваг в порівнянні з іншими методами віддаленого доступу. По-перше, користувачі можуть звертатися до корпоративної мережі, не встановлюючи з нею комутоване з'єднання, таким чином, відпадає потреба у використанні модемів. По-друге, можна обійтися без виділених ліній.

У роботі показано, що найкращим засобом реалізації технології VPN є IPsec. IPsec (скорочення від IP Security) – набір протоколів для забезпечення захисту даних, що передаються засобами протоколу IP, дозволяє здійснювати підтвердження достовірності і шифрування IP-пакетів. IPsec призначений для безпечної взаємодії на основі криптографії для IPv4 і IPv6. Набір сервісів безпеки включає управління доступом, цілісність з'єднання, автентифікацію вихідних даних, захист від Replay-атак (цілісність послідовності), конфіденційність (шифрування) і конфіденційний потік трафіку.

Після аналізу засобів захисту інформації при передачі даних, варіантів використання між мережного екрану та варіантів реалізації технології VPN засобами між мережного екрану, можна зробити такі висновки:

– існує можливість включення алгоритму шифрування ГОСТ 28147-89 в стек протоколів IPSec;

– вітчизняний алгоритм шифрування ГОСТ 28147-89 можливо використовувати у складі між мережного екрану.

Отже, для забезпечення захисту інформації при передачі даних в українських реаліях потрібно удосконалити технологію VPN. Це здійснюється шляхом добавлення у стек протоколів IPSec алгоритму шифрування ГОСТ28147-89, що в свою чергу, дає змогу побудувати систему захисту, що відповідає рівням гарантії Г-4 і вище.

УДК 004.031.2 (043.2)

О.В. Марченко
Національний авіаційний університет, м. Київ

АНАЛІЗ КОНЦЕПЦІЇ АРХІТЕКТУРИ СИСТЕМ CLOUD MONITORING

Загальновідомо, що віртуальні середовища можуть суттєво прискорити вихід на ринок автоматизованих та високонавантажених рішень, котрі призначені для використання багатьма користувачами одночасно, одним із таких прикладів може бути віртуалізація серверних рішень для організації корпоративної мережі IP-телефонії. Проте залишається необхідність об'єктивного моніторингу стану завантаженості самої мережі. Тому що Cloud платформа може провести моніторинг звернень лише до певного сервісу чи послуги що розгорнуто на ній. Далі буде запропоновано архітектуру побудови системи моніторингу розподіленої інфраструктури корпоративної мережі, котра поєднує в собі як локальні ресурси так і використовувані ресурси Cloud платформи (рис. 1).

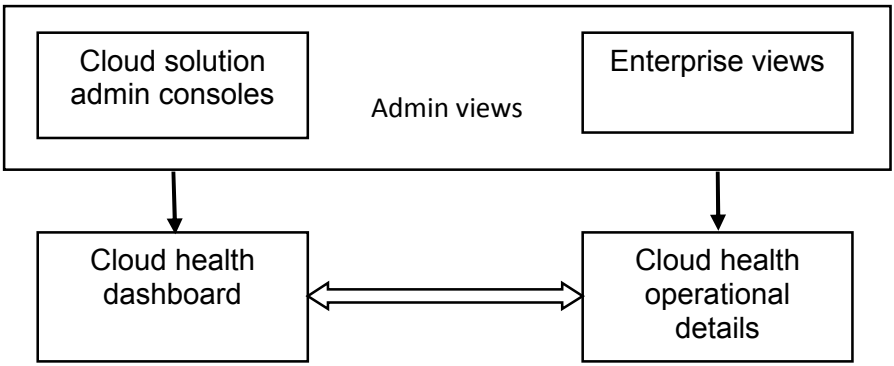

Рис. 1. Запропонована архітектура системи моніторингу Cloud-інфраструктури підприємства

В рамках даного підходу можливо проводити моніторинг корпоративних ресурсів у режимі реального часу. Оскільки основні компоненти Health dashboards та Admin views враховують те що, віртуальні інфраструктури можуть стати дуже великим, дуже швидко, і з їх віртуальних пулів зберігання, мереж і процесів буде передаватися все бі-

льше інформації, котра потребуватиме місце для консолідації. Даний підхід дозволяє актуальну інформацію передати користувачам через інформаційні Heath dashboards. Ці панелі надають можливість швидко переглянути загальний стан всієї хмари, що було б неможливо побачити з традиційними інструментами управління підприємством, які дозволяють переглядати стан тільки окремих серверів. SmartCloud панелі моніторингу дозволяють користувачам швидко отримати можливість зазирнути в загальний стан їх хмарних середовищ, в режимі реального часу про-активними і прогностичними повідомленнями допомагати користувачам виявляти і усувати проблеми швидко.

Окрім цього даний підхід дозволяє інтегрувати програмні рішення для вирішення наступних питань на підприємстві:

- управління апаратними та програмними ліцензіями;
- поліпшення щільності Cloud системи, знаючи, скільки буферних ресурсів можна виділити;
- контролювати дозвіл навантаження для запуску протягом тривалого часу без перегрупування ресурсів та віртуальних машин.

Також апаратна віртуалізація серверних складових IP-телефонії дозволяє розмістити розподілені копії критичної інформації та використовувати розширені можливості управління навантаження використовуючи ресурс Balance loader, що поставляється у пакеті Microsoft Lync Server (на рис. 2 позначено як Cloud App – оскільки може міститися у віртуальній машині що використовуються для інших потреб).

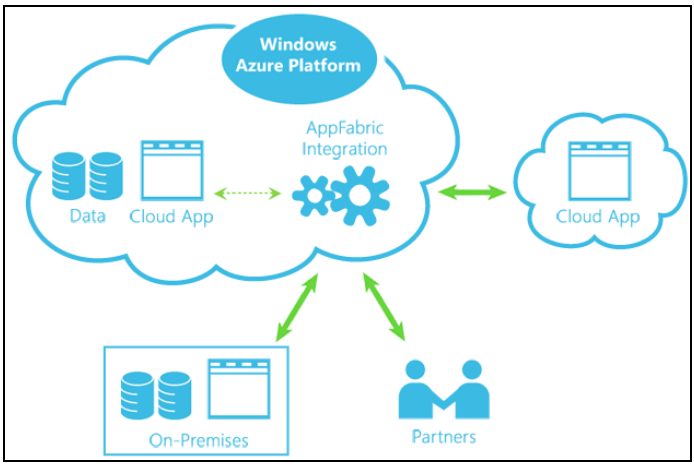

Рис. 2. Розподілена інтеграція Cloud рішень у корпоративну мережу

УДК 004.056.53 (043.2)

П.О. Вікулов, В.Г. Павлов
Національний авіаційний університет, м. Київ

ЗАХИСТ КОРИСТУВАЧІВ ХМАРНИХ ТЕХНОЛОГІЙ

Постановка проблеми. Інформаційно-комунікаційні системи повинні забезпечувати доступ користувачів до необхідних інформаційних ресурсів. Звичайно, дуже зручно та безпечно, якщо ці ресурси розміщуються на особистому комп'ютері користувача. Якщо ж інформаційні ресурси мають використовуватися спільно групою користувачів, то застосовуються мережні сервера для їхнього зберігання та мережні протоколи для організації доступу до них. Але обробка інформації знову ж таки зосереджується на робочих комп'ютерах користувачів, де повинні бути встановлені певні програмні додатки. До того ж усі сервера мають бути ідентифіковані у комп'ютерний мережі.

Наступним кроком у розвитку інформаційно-комунікаційних систем є використання комп'ютерної мережі для розміщення програмних засобів обробки інформації, яка до того ж не "прив'язана" до певних серверів.

Метою роботи є аналіз аспектів безпеки, які виникають при застосуванні хмарних технологій. При розгортанні хмарних послуг виключно важливу роль грає надійний захист особистих даних користувачів. У хмарних технологіях кінцеві ресурси та управління архітектурою сервісів є невидимими для користувачів, тому природно, що постійно виникає питання безпеки подібної системи, у якій користувачі не мають фізичного контролю і доступу до ресурсів.

При сучасних методах хакерських атак, традиційних систем безпеки доступу (аутентифікації) для доступу до хмарним системам найчастіше виявляється недостатньо – особливо для систем із конфіденційними даними, що використовуються в таких галузях, як фінансовий бізнес, охорона здоров'я і торгівля, а також в державних організаціях. Оскільки інтерес до хмарних сервісів росте на всіх рівнях – від домашніх користувачів до великих підприємств, – постійно пропонуються нові підходи до забезпечення інформаційної безпеки хмарних технологій.

З технологічної точки зору безпека даних користувача може бути відображена в наступних правилах впровадження хмарних технологій:

- Конфіденційність зберігання призначених для користувача даних. Збережені дані користувача не можуть бути переглянуті або змінені іншими людьми, включаючи операторів, що обслуговують систему.
- Захист інформації користувача під час перегляду або виконання інших операцій. Користувацькі дані не можуть бути показані або змінені іншими людьми під час їх виконання.
- Конфіденційність під час передачі персональних даних по мережі. Це включає в себе захист переданої інформації в віддалений хмарний обчислювальний центр.
- Для доступу користувачів до своїх даних необхідне встановлення авторизації. Користувачі можуть отримати доступ до своєї інформації лише правильним шляхом і можуть дозволити авторизацію інших людей для доступу до свого аккаунту.

Додатковий важливий фактор в питаннях безпеки хмарних обчислень пов'язаний з тенденцією виходу хмарних систем в Інтернет: приватні хмари сьогодні часто взаємодіють з публічними хмарними сервісами і навпаки.

У доповненні до технологічних рішень, необхідно застосовувати також правові та юридичні рекомендації, що можуть посилити безпеку персональних даних, з гарантіями прав користувача та відшкодуванням матеріальних збитків при порушенні безпеки або конфіденційності інформації в процесі використання хмарних технологій.

У той же час використання надлишкових заходів безпеки може бути фінансово обтяжливим для власника системи. Тому система безпеки хмарного сервісу повинна бути водночас повноцінною і гнучкою та фінансово виправданою.

Висновки: забезпечення безпеки користувачів хмарних технологій потребує комплексного підходу для вирішення задачі. Це означає, що робота з забезпечення захищеного використання хмарного сервісу повинна вестися у таких напрямках як: аналітика загроз безпеці користувацької інформації, впровадження технічних та програмних методів захисту даних користувача, регулярне оновлення програмного забезпечення системи та постійний моніторинг наявності уразливостей та загального стану безпеки хмарного сервісу. Комплексна взаємодія цих напрямків дає максимальний захист користувацьких даних та забезпечує високий рівень захищеності усього хмарного сервісу.

УДК 004.738 (043.2)

М.О. Шрамко, О.П. Ткаліч
Національний авіаційний університет, м. Київ

БЕЗПРОВОДОВА МЕРЕЖА ДЛЯ ДОСТУПУ ДО БАЗ ДАНИХ

На сучасному етапі розвитку телекомунікаційних систем постає безліч проблем, пов'язаних із забезпеченням певного набору послуг, необхідних для користувачів портативних мобільних пристроїв. Кількість користувачів смартфонів та планшетів щорічно зростає разом з вимогами до програмних та апаратних засобів.

Метою проекту є створення безпроводової мережі для доступу до бази даних широкого застосування. Передбачено застосування такої мережі в певному торгівельному приміщенні. Відвідувачі, що мають портативні мобільні пристрої, підключившись до мережі, зможуть синхронізувати список своїх покупок з базою даних торгівельного центру та отримати інформацію про ціну та місцезнаходження необхідних їм товарів. На мобільний пристрій завантажується карта приміщення та під час переміщення всередині на екрані пристрою з'являються спливаючі вікна з інформацією про наявність акцій на товари поблизу яких знаходиться клієнт. Крім цього, користувач може скласти список необхідних покупок до приходу в магазин, чи отримати його від іншого пристрою, а спеціальне програмне забезпечення, використовуючи базу даних, складе оптимальний маршрут, по якому задані товари можна зібрати.

Під час розробки проекту було виконано моделювання топології безпроводової мережі Wi-Fi. Для об'єднання точок доступу використовується централізована система управління на базі контролера. Тож для певного торгівельного приміщення визначається необхідна кількість точок доступу, які будуть раціонально розміщенні з урахуванням зон покриття та зон перекриття для забезпечення роумінгу клієнтів. Вибирається тип обладнання, що здатне задовільнити умови, які висуваються до мережі. Зокрема такі параметри як: швидкість передачі даних у мережі, кількість каналів, максимальна кількість клієнтів, що одночасно обмінюються даними у мережі. Після вибору типу та кількості обладнання проводиться його конфігурація та настройка.

УДК 621.396 (043.2)

О.Ю. Негрішний
Національний авіаційний університет, м. Київ

МЕТОДИ ПОБУДОВИ ЗАХИЩЕНИХ КАНАЛІВ КЕРУВАННЯ ПОВІТРЯНИМ РУХОМ

Проблема полягає в тому, що існуючі технології передавання конфіденційної мовної інформації через стандартний вузькосмуговий авіаційний радіоканал не здатні задовольнити в комплексі існуючі норми щодо критеріїв захисту інформації, розбірливості прийнятих мовних повідомлень та забезпечення стабільності зв'язку.

На сьогоднішній день єдиним шляхом забезпечення можливості ефективного захисту мовної інформації в вузькосмуговому авіаційному стандартному радіоканалі, є використання криптографічних систем у комплексі із вокодерами.

Вокодери – це пристрої синтезу мови на основі довільного сигналу з широким спектром. Замість власне мовного сигналу передаються тільки значення його певних параметрів, які на приймальній стороні керують синтезатором мови. Вокодери забезпечують високий ступінь стиснення інформації, а також хорошу узгодженість з системами канального кодування і шифрування, в результаті чого порівняно легко забезпечити високу захищеність систем зв'язку від завад та витоку інформації.

Для вирішення задачі кодування і шифрування найоптимальнішим є використання стеку протоколів IPsec. IPsec – це набір протоколів що використовується для забезпечення сервісів приватності та аутентифікації. Ці протоколи можна розділити на два класи – протоколи захисту вихідних даних та протоколи обміну ключами.

У роботі розглянуто побудову захищеного каналу керування повітряним рухом на основі вище згадуваних технологій та основні принципи переходу до майбутньої системи авіаційного зв'язку (ATN). Проаналізовано вимоги та рекомендації ІСАО щодо переходу на майбутні системи зв'язку. Впровадження даної системи має значні переваги, основними з яких є:

1) глобальна можливість з'єднання та взаємодії будь-яких абонентів;
2) передавання звичайних повідомлень у формі цифрових даних, голос буде використовуватись тільки у надзвичайних ситуаціях.

Переваги зв'язку на основі передавання даних над голосовим зв'язком очевидні (табл. 1).

Таблиця 1

Порівняння передавання даних та голосу

Голос	**Дані**
Акцент може призвести до хибного сприйняття	Забезпечується якість і однозначність інформації
Низька швидкість передавання інформації	Висока швидкість передавання інформації
Процес передавання і приймання інформації протікає у реальному часі	Можуть зберігатися, копіюватися, відновлюватися
Викликає переповнення радіодіапазону	Запобігають переповненню діапазону
Низька захищеність: доступний для усіх абонентів даного каналу	Селективні: пересуваються між парою абонентів
Труднощі (неможливість) передавання деяких видів інформації	Цифрова форма універсалізує подання будь-якої інформації

Впровадження даної системи створює значні складності в процесі переходу від існуючих систем зв'язку до майбутніх. Наприклад, що стосується покриття то тут проблема пов'язана зі створення інфраструктури, проблема інтеграції, тощо.

УДК 004.031.2 (043.2)

Д.Г. Пластун
Національний авіаційний університет, м. Київ

ПОРІВНЯЛЬНИЙ АНАЛІЗ СХЕМ АДМІНІСТРУВАННЯ МЕРЕЖЕЮ WCDMA

В роботі здійснено порівняльний аналіз схем адміністрування мережею WCDMA. Розглянуто мережі внутрішньосмугового та позасмугового адміністрування. Показано переваги та недоліки внутрішньосмугового керування (або керування типу In-band) та позасмугового керування (або керування типу Out-of-band). Якщо керуючі сигнали проходять через той же канал, що і користувальницькі дані (наприклад, повідомлення протоколу керування, згідно з котрим взаємодіють агенти з менеджером, транспортуються тими ж каналами IP-мережі, що і пакети користувачів цієї мережі), то маємо справу із внутрішньосмуговим керуванням. Якщо ж менеджер вузлу керування контролює IP-маршрутизатор і взаємодіє із своїми агентами, що в нього вбудовані, через канали окремої спеціально виділеної мережі керування, то маємо справу із позасмуговим керуванням. Зрозуміло, що на створення окремої мережі керування потрібні значні фінансові ресурси. Проте позасмугове керування є набагато більш надійнішим і захищеним від несанкціонованого доступу. Для мережних структур основним параметром, що визначає рівень якості захисту інформації, є тип мережного керування: «in band» або «out of band». При керуванні типу «in band» потоки управлінської та іншої технологічної інформації фізично не відокремлюються від потоків даних користувачів мережних послуг в той час, як при керуванні типу «out of band» створюється фізично відокремлена від основної мережі спеціалізована мережа керування. Фізичне відокремлення каналів та вузлів управлінської мережі створює більш сприятливі умови для організації захисту інформації. Тому є доцільним при побудові систем захисту з рівнем Г2 спиратися на структуру управління типу «in band», а при побудові систем захисту з рівнем Г3 спиратися на структуру управління типу «out of band».

У роботі розглянуто сучасні методи адміністрування як внутрішньосмуговим так і позамуговим обладнанням.

УДК 621.391 (043.2)

А.О. Димерлій
Національний авіаційний університет, м. Київ

РОЗРОБКА ТА ПРОЕКТУВАННЯ МЕРЕЖІ LTE ДЛЯ ЧЕРНІГІВСЬКОЇ ОБЛАСТІ

Розвиток телекомунікаційних мереж наразі є однією з найпріоритетніших задач, оскільки щодня збільшується потреба в широкосмуговому доступі і цю проблему покликана вирішити технологія Long Term Evolution (LTE). Впроваджуючи цю технологію, забезпечується підвищення пропускної здатності, збільшення швидкості та зниження вартості передачі даних. Користувачі зможуть відкрити для себе нові послуги, які раніше не були доступні при мобільному бездротовому доступі. Цей проект має на меті розібратися на прикладі Чернігівської області в даній технології, її особливостях побудови і принципах впровадження.

Було проведено техніко-економічне обґрунтування побудови LTE мережі, розрахунок пропускної здатності, розрахунок кількості потенціальних абонентів, які можуть обслуговуватись в даній області, вибір обладнання транспортної мережі. Також було вибране обладнання та проведений розрахунок зон радіопокриття, розглянуті аспекти екології, техніки безпеки та охорони праці.

Інтерес мобільних операторів до технології LTE цілком зрозумілий, оскільки це – вигідний проект. Вона представляє собою наступний етап розвитку мобільних мереж, тому що краще використовує частотний спектр, відрізняється меншим значенням затримки, а також підвищеною ємністю. Мережі LTE мають спрощену архітектуру платформи, а також є єдиною на сьогоднішній день технологією, яка дозволяє використовувати одну й ту саму платформу для непарного та парного сектору, за рахунок чого зменшуються витрати операторів.

На жаль, в Україні LTE досі вважається технологією «наступного» дня, хоча вже сьогодні вона реалізована в багатьох країнах світу. Масштабність, завадостійкість, швидкість передачі та адаптованість до важких умов передачі сигналів чітко відповідає сучасним вимогам до мультисервісних мереж. Впровадження такої мережі дозволить операторам значно зменшити капітальні затрати, розширити спектр послуг і технологій та відчутно підвищити доходи.

УДК 621.391 (043.2)

А.В. Савченко
Національний авіаційний університет, м. Київ

ПРОЕКТУВАННЯ МЕРЕЖІ LONG TERM EVOLUTION В КИЇВСЬКІЙ ОБЛАСТІ

В період бурхливого технічного прогресу, коли все швидше розвиваються мобільні пристрої передачі даних і все більше операцій проводяться в глобальній мережі «Інтернет», з кожним днем зростає потреба мати можливість широкосмугового доступу не тільки дома або в офісі, а й на вулиці і в транспорті. Основними цілями розробки технології LTE є: збільшення швидкості передачі даних, розширення і удосконалення надаваних послуг, зниження вартості передачі даних, повномасштабне використання наявних мережевих ресурсів. Головна відмінність стандарту LTE від інших технологій мобільного зв'язку полягає в повній побудові мережі на базі IP-технологій. Радіоінтерфейс LTE забезпечує покращені технічні характеристики, включаючи максимальну швидкість передачі даних понад 300 Мбіт/с, час затримки пересилання пакетів менше 10 мс, а також значно більш високу спектральну ефективність, гнучкість радіоспектру, управління рівнем випромінюваної потужності. Метою даного проекту є вивчення цієї технології, її особливостей, загальних принципів побудови на основі LTE/SAE мережі бездротового зв'язку, особливо проектування опорного сегменту для обслуговування великої території, а саме Київської області.

Основу транспортної мережі проектованої мережі LTE становить IP-протокол, який служить для транспортування трафіку мережі. Головним вихідним значенням розрахунку являється спектральна ефективність технології LTE, яка заявлена в 3GPP Release 9. Розрахована пропускна здатність планованої мережі та частотний діапазон, обрано частотний тип дуплексу. Також проведено розрахунок кількості абонентів, яку зможе обслужити планована мережа. Також розглянуті різні види обладнання транспортної мережі та обрано найоптимальніші, для реалізації транспортної мережі LTE є кращим за багатьма параметрами рішення компанії «Cisco Systems». Транспортна мережа проектованої мережі LTE реалізована за допомогою оптоволоконних ліній передач за технологією Ethernet. Зроблений вибір оптичного кабелю. У проекті використовуються три види оптичних кабелів: для прокла-

ки в грунті, для прокладки в каналізації та підвісний. В якості керуючого обладнання мережі LTE вибрано рішення компанії «Cisco Systems», що реалізується за допомогою мультисервісної платформи. Вибрано обладнання базової станції eNode. Також проведено вибір обладнання електроживлення, в ході якого проведені розрахунки: споживаної потужності базових станцій, джерело безперебійного живлення змінного струму, автоматичних вимикачів і групи обліку, розрахунок контуру заземлення базових станцій. Для організації радіодоступу за технологією LTE в Київський області у проекті проведено розрахунок зон покриття радіозв'язком. Розраховано радіус стільників та площа покриття, проведено частотно-територіальний поділ Київської області. З метою захисту населення від впливу електромагнітних випромінювань радіочастотного діапазону в проекті були розраховані межі зон обмеження забудови, максимальна довжина зон обмеження забудови. В економічній частині проекту проведено розрахунок капітальних вкладень, прибуток та рентабельність. У проекті також розглянуті питання охорони праці, екології та техніки безпеки обслуговуючого персоналу обладнання бездротового доступу.

Впровадження мережі LTE в Україні є дуже актуальним на даний час, тому що це мережа «завтрашнього» дня, архітектура якої скорочує кількість вузлів, підтримує гнучкі конфігурації мережі і забезпечує високий рівень доступності послуг. Також слід відмітити високі характеристики абонентського мобільного пристрою в порівнянні з пристроями попередніх систем. Використовуючи мобільний доступ, користувачі можуть краще організовувати свій час, ніж налаштовуючи підключення до бездротової LAN, ризикуючи при цьому безпекою або втратою покриття. Важливим аспектом є те, що з точки зору на витрати, впровадження інфраструктури LTE є дуже простим та ефективним. Наприклад, «апгрейдити» існуючі базові станції радіоподмережі до LTE використавши легко замінні модулі, які зможуть працювати, як з одним частотним діапазоном, так і з парними наборами частот. Також сучасне обладнання GSM / WCDMA потребує більш складної установки, ніж базові станції для LTE.

УДК 004.056:621.12 (043.2)

І.С. Харечко
Національний авіаційний університет, м. Київ

МЕТОДИКА ПОБУДОВИ МОДЕЛІ ЗАГРОЗ ІНФОРМАЦІЇ

Вступ. Для будь-якої системи обробки інформації (СОІ), як правило, існують певні загрози та гостро постають питання моделювання та оцінки загроз безпеки інформації. Ситуація ускладнюється тим фактом, що кількість погроз швидко зростає і не завжди оперативно служби безпеки встигають реагувати на певні загрози і своєчасно протидіяти їм.

Мета – розробити методику аналізу загроз інформації та запропонувати моделі функціонування і використання ресурсів СОІ.

Основна частина. Можливим рішенням даної проблеми може виступити моделювання та оцінка небезпеки загроз. Сформулюємо основні завдання при побудові моделі загроз СОІ:

1. Розробити модель функціонування СОІ та модель використання її ресурсів. Результатом буде технологічна схема функціонування СОІ $\{TS\}$ і безліч параметрів використання ресурсів СОІ $\{PR\}$.

2. На підставі результатів попереднього етапу будується модель уразливостей СОІ. Зазначений етап дозволить надалі розробити модель розподілених атак на СОІ. Результатом стане безліч уразливостей компонентів СОІ $\{UK\}$ (до компонентів СОІ відносяться: власне інформація, апаратне та програмне забезпечення, обслуговуючий персонал і фізичне середовище).

3. Виходячи з безлічі уразливостей компонентів СОІ, формується модель розподіленої атаки на СОІ. Результатом моделювання стане повний перелік можливих атак на СОІ $\{PA\}$.

4. На підставі технологічної схеми СОІ будуємо модель противника, оцінюємо його попередні можливості. Результатом побудови зазначеної моделі стануть відомості про категорії противників $\{KP\}$, їх можливості з реалізації певних видів атак.

5. Розробляється модель загроз інформації, що оброблюється в СОІ. Результатом цього етапу моделювання є створення списку загроз інформації $\{SZ\}$. При цьому для кожної загрози СОІ буде поставлений

у відповідність спосіб її реалізації (елемент множини $\{SR\}$), а також необхідні умови для реалізації загрози (елемент множини $\{UZ\}$).

Модель функціонування COI може бути формально представлена у вигляді функції:

$$F_{ф}(COI) \to \{TS\}.$$

Модель використання ресурсів COI являє собою функцію:

$$F_{в}(COI, \{TS\}) \to \{PR\}.$$

Модель уразливостей COI представляє наступну функцію:

$$F_{у}(COI, \{PR\}) \to (\{UK\}, \{PA\}).$$

Модель атаки на інформацію представлена функцією:

$$F_{а}(\{PA\}, \{KP\}, \{SZ\}) \to (\{UZ\}, \{SR\}).$$

Розглянемо порядок взаємодії запропонованих моделей.

На першому етапі проводиться розробка моделі функціонування COI. Результати будуть використані у всіх наступних моделях процесів захисту інформації. Підсумком моделювання стане технологія функціонування COI, яка описана формально. Далі необхідно визначити ресурси COI, тобто визначити, які ресурси використовуються COI для вирішення завдань з обробки інформації. Також необхідно формально описати схему використання ресурсів. Ця схема буде потрібна для визначення можливих об’єктів атак зловмисників, вона також знадобиться при аналізі каналів витоку інформації.

На другому етапі проводиться розробка моделі уразливостей COI. Результатом моделювання буде перелік пасивних загроз інформації. Список можливих розподілених атак на COI є вектором можливих шляхів реалізації розподілених атак на COI. Кожен шлях реалізації атаки включає безліч уразливостей компонентів COI, які можуть бути використані порушником політики безпеки.

Висновки. Запропонована формальна модель загроз містить сукупність записів в базі даних загроз, поля якої містять інформацію про всі їх параметри, що підлягають захисту. При такому способі організації зручно підтримувати її в актуальному стані: доповнювати новими записами і видаляти відомості про загрози, що втратили свою актуальність. Вдало розроблена технологічна схема функціонування COI та перелік можливих атак зменшить ризик втрати інформації.

УДК 004.8 (043.2)

О.М. Половий
НТУУ «Київський політехнічний інститут», м. Київ

АЛГОРИТМ ПАРАМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ БАЗ НЕЧІТКИХ ЗНАНЬ

У даній роботі розглянуто алгоритм ідентифікації системи націленої на підтримку прийняття рішень, котра використовує нечітку логіку – бази нечітких знань. Базою нечітких знань (БНЗ) називається сукупність нечітких правил "Якщо – то", що описують взаємозв'язок між входами і виходами деякого об'єкта, використовуючи лінгвістичні змінні (ЛЗ). Значення ЛЗ визначається множиною якісних характеристик – термів. Однак, при доволі складній структурі модульованої системи, сучасні алгоритми ідентифікації БНЗ не дозволяють отримати результуючу оптимальну БНЗ. Оптимальна БНЗ – БНЗ у якої для всіх допустимих вхідних значень точність логічного виводу відбувається з мінімальною похибкою.

Для підвищення точності логічного виводу БНЗ запропоновано використовувати модифікований генетичний алгоритм. Він є модифікацією канонічного генетичного алгоритму Джона Холланда [1]. Модифікований алгоритм застосовується для параметричної ідентифікації БНЗ. У ньому пропонується приймати за хромосому не одне з правил певної БНЗ, а цілу БНЗ і вже в подальшому проводити операції схрещування, відбору та мутації не над правилами, а над БНЗ. Генетичною інформацією котра зберігається в хромосомі є множина нечітких правил та функції належності всіх термів кожної ЛЗ цієї БНЗ.

Особливістю даного модифікованого алгоритму є оператор схрещування, при виконанні якого відбувається обмін між хромосомами лише тією інформацією, що стосується опису нечітких правил. Значення функцій належності всіх термів для всіх ЛЗ з однієї хромосоми залишається сталим. За рахунок цього вирішується проблема, коли правило з однієї БНЗ краще описує предметну область знаходячись в іншій БНЗ. Даний модифікований оператор схрещування слід застосовувати разом з загальноприйнятими операторами схрещування в генетичних алгоритмах, адже обмін інформацією стосовно функцій належності термів в модифікованому операторі схрещування не відбувається. Блок-схема модифікованого алгоритму параметричної ідентифікації БНЗ приведена на рис. 1.

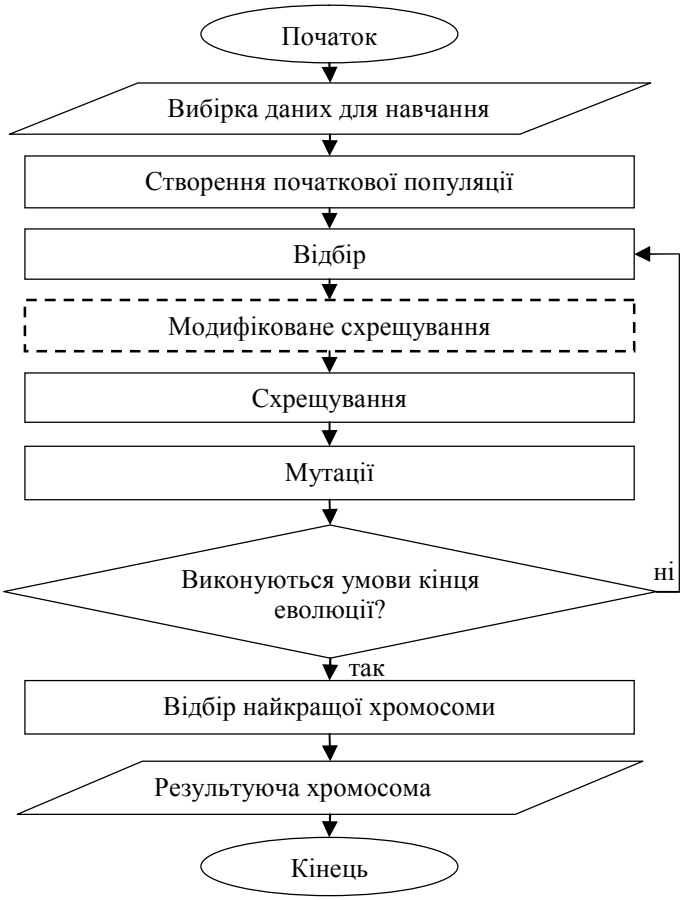

Рис. 1. Блок-схема модифікованого алгоритму

У роботі запропоновано модифікований генетичний алгоритм для параметричної ідентифікації баз нечітких знань. Використання даного алгоритму дозволяє підвищити точність логічного виводу результуючої БНЗ.

Список літератури

1. Holland J. H. Adaptation in Natural and Artificial Systems: An Introductory Analysis With Applications to Biology, Control, and Artificial Intelligence J. H. Holland. – The MIT Press, Cambridge, 1992.

УДК 004.735 (043.2)

Є.Ю. Шеремет
Національний авіаційний університет, м. Київ

ДОСЛІДЖЕННЯ СЕРВІСНОЇ ЧАСТИНИ IP-ТЕЛЕФОНІЇ НА БАЗІ ТЕХНОЛОГІЇ ASTERISK

Задача дослідження: розробити та запустити IP-телефонію на базі технології Asterisk.

У IP-телефонії є достатня кількість переваг, щоб незабаром поширитися по всій нашій країні, головна перевага послуги – в її дешевизні. Нові технології дозволяють значно ефективніше використовувати найдорожчу частину комунікацій – канали зв'язку. Їх пропускна спроможність у багато разів перевищує традиційні (канали одночасно використовуються відразу багатьма абонентами).

Asterisk – відкрита комунікаційна платформа, котра використовується для розгортання програмних АТС, систем голосового зв'язку, VoIP-шлюзів, організації IVR-систем (голосове меню), голосової пошти, телефонних конференцій і call-центрів.

Asterisk може взаємодіяти за стандартами Голос-по-IP [VoIP] (SIP, H.323, IAX та інші), а також з громадськими комутованими телефонними мережами (Public Switched Telephone Network – PSTN) за допомогою підтримуваного апаратного забезпечення.

Для використання Asterisk потрібен персональний комп'ютер архітектури x86 з PCI-картою для аналогових портів. Проте можлива й альтернатива , що дозволяє отримати ту ж функціональність в маленькому, дешевому, тихому пристрої з малим енергоспоживанням. Прикладом такого рішення є IP04 – дешева VoIP-система, яка може передавати телефонні дзвінки між аналоговими телефонами або телефонними лініями і мережею Інтернет.

Проект планується реалізувати на кафедрі телекомунікаційних систем Національного авіаційного університету з використанням такого обладнання: ПК (як серверна частина), IP-телефони, softphone – на ПК і ноутбуки, маршрутизатор; який буде виступати, як IP-телефонія, так і лабораторний стенд, на якому буде можливість досліджувати канали зв'язку, трафік, в тому числі і захищеність мережі.

УДК 621.396.933.4 (043.2)

Д.В. Ковалевський
Національний авіаційний університет, м. Київ

ОПТИМІЗАЦІЯ ЗАХИЩЕНОГО КАНАЛУ УПРАВЛІННЯ ПОВІТРЯНИМ РУХОМ

На сьогоднішній день єдиним можливим шляхом забезпечення ефективного захисту мовного трафіку у стандартному радіоканалі є використання вокодерного утиснення й дискретизацію мовного сигналу з наступним його шифруванням засобами, що реалізують один із ефективних алгоритмів криптографічного шифрування

Вокодерний пакет мовних повідомлень або даних V/D (voice/data) складається з чотирьох сегментів: налаштовуючої послідовності, після якої слідують заголовок, сегмент інформації користувача та лінійно спадаюча характеристика передавача. Сегмент інформації користувача складається з 192 3-бітних символів. При передачі в режимі мовного зв'язку застосовується FEC (пряме виправлення помилок) для аналізу вихідних сигналів вокодера. Вокодер забезпечує задовільні характеристики при BER, рівному 10^{-3} (при цільовому рівні 10^{-2}). В цілому швидкість передачі вокодера, включаючи FEC, дорівнює 4800 біт/с (за виключенням режиму усічення, за якого швидкість передачі складає 4000 біт/с).

Некогерентні модеми із багатопозиційною частотно-фазовою модуляцією краще за інших підходять для вирішення даної проблеми. Такий модем, що використовується разом із низькошвидкісним вокодером та ефективним засобом криптографічного захисту інформації, може являти компромісне технічне рішення, що забезпечує необхідний для авіаційних застосувань рівень захисту мовного трафіку без втрати якості зв'язку.

Застосування наведеної технології надало б змогу засобам, які використовуються сьогодні для передавання критично важливої мовної інформації через стандартний авіаційний радіоканал спроможності задовольнити норми щодо критеріїв захисту інформації та розбірливості прийнятих мовних повідомлень за умов, коли висуваються підвищені вимоги щодо забезпечення стабільності зв'язку.

УДК 621.391 (043.2)

Л.Л. Грицюк
Національний авіаційний університет, м. Київ

ОФІСНА ВІРТУАЛЬНА АТС

Технологія пакетної передачі голосу по IP мережах (VoIP) за допомогою ряду протоколів і голосових кодеків дозволяє здійснювати дзвінки в рамках однієї локальної мережі, між територіально рознесеними локальними мережами, а також на зовнішню міську лінію. На даний момент для здійснення телефонного зв'язку в кожному з перерахованих вище випадків може використовуватися не один, а кілька протоколів сигналізації і голосових кодеків.

Вибір конкретного протоколу та кодека робиться виходячи з пропонованих до мережі IP телефонії вимог, її масштабів і територіального розміщення. Для невеликої організації, що складається з 20 – 40 чоловік можна використовувати безкоштовне програмне забезпечення і протоколи з відкритим вихідним кодом для створення телефонної мережі на основі технології пакетної передачі голосу по IP мережах. Проте в даному випадку можна зіткнутися з низкою проблем щодо забезпечення якості обслуговування і передачі голосу, а також з обмеженістю використання всіляких сервісів VoIP.

Кодек – це алгоритм, який перетворює аудіо-сигнали в цифрові пакети і назад. Кодеки характеризуються різними частотами дискретизації і розрядністю. У різних кодеках реалізовані різні методи компресії, які засновані на різних вимогах до мережевого навантаження і обчислювальних ресурсів. Вибір найкращого кодека для конкретних мережевих умов може істотно підвищити якість передачі звуку. Вибір в мережі з вузькою смугою пропускання такого кодека з відмінною якістю як G.711 буде помилкою, оскільки якість звуку постраждає через обмеження в пропускної здатності і втрати пакетів. Якщо пропускна здатність мережі не перевищує 64 кбіт/с, то слід вибрати кодеки G.729 або G.723, у яких низький бітрейт і високий ступінь стиснення. Незважаючи на високу пропускну здатність локальної мережі, зовнішні дзвінки можуть надалі проходити через сегменти з меншою смугою пропускання. У провайдерів ADSL і кабельних мереж пропускна здатність вихідного каналу часто обмежена, що призводить до його перевантаження при великій кількості одночасних дзвінків. У цьому випадку вузькосмугові кодеки будуть більш кращі. Широкосмуговий

кодек G.711 дає найвищу якість звуку, але має при цьому найвищий рівень трафіку. Кодеки G.729a, .723.1 і G.726 мають різну ступінь якості звуку, в порядку його зменшення. Вибір кодека не відбувається автоматично. Системний адміністратор повинен вказати і розташувати кодеки в порядку їх пріоритету в VoIP-системі. Правильний вибір кодека може істотно поліпшити якість звуку. Відображаючи дані VoIP-сесії, аналізатор VOIP мереж дозволяє спостерігати процес узгодження кодеків, тобто кодеки, доступні пристроям, а також той кодек, який був у підсумку узгоджений для передачі даних.

Було розраховано смугу пропускання, яка необхідна для невеликої організації, що складається з 20 – 40 чоловік. Використовується різне кінцеве обладнання, аналогічно і різні кодеки. Проведено аналіз впливу смуги пропускання на якість встановленого телефонного з'єднання. Якщо використовується кодек G.711, то при найменшому зменшенні смуги пропускання погіршується якість голосу. Якщо смуга пропускання буде обмежена на 20 %, то якість зв'язку залишається прийнятною, а більше 20 – неможливим. Це пов'язано з тим, що кодек G.711 вимагає досить велику смугу для кодування голосу – 84 кбіт/с і тому невеликі обмеження не вплинуть на якість передачі. Кодеки iLBC, Speex і GSM більш критичні до обмеження смуги пропускання, ніж кодек G.711. Цей факт пояснюється тим, що дані кодеки для більш сильного стиснення голосу використовують складніші алгоритми кодування. Ці кодеки створювалися для передачі голосу по IP-мережах в умовах малої пропускної здатності каналу зв'язку, а також у випадках великої кількості користувачів IP телефонної мережі. Розглянуті кодеки крім критичності до величини смуги пропускання мають ще один недолік. Так як вони використовують складні алгоритми кодування, то вимагають більшої обчислювальної потужності серверів. Тому при використанні цих кодеків необхідно враховувати продуктивність серверів і кількість абонентів, інакше неправильний розрахунок може привести до зависання обладнання і непрацездатності телефонної мережі.

Тому перед побудовою і під час експлуатації мереж IP-телефонії необхідно контролювати і не допускати істотного пониження граничних норм пропускної здатності мережі, так як це може привести до погіршення зв'язку і, як наслідок, незадоволеності абонентів IP-телефонної мережі.

УДК 004.258:004.031.2 (043.2)

Є.В. Рибальченко
Національний авіаційний університет, м. Київ

ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ ВУЗЛОВОГО ОБЛАДНАННЯ ШЛЯХОМ ВИКОРИСТАННЯ МЕХАНІЗМІВ ПРОГНОЗУВАННЯ ПОТОКІВ ТРАФІКУ

Оскільки вузлове обладнання (ВО) сучасних пакетних мереж є високо вартісним, то одна з ключових проблем експлуатації пакетних мереж полягає у недостатній ефективності наявних технологій обробки протокольних блоків даних, які в умовах пульсуючого трафіку поки, ще не в змозі забезпечити високий коефіцієнт завантаження такого ВО. Виходячи з точки зору економічної складової, необхідно намагатися збільшувати ступінь використання ресурсів мережевих комутаційних пристроїв, щоб опрацьовувати більші обсяги даних у співвідношенні на одиницю вартості задіяного обладнання. Реальний коефіцієнт завантаження обладнання сучасних пакетних мереж в середньому не перевищує величини 0,45 – 0,5. При більших значеннях цього коефіцієнту різко падає якість обробки пакетів під час значних пульсацій трафіка. Як бачимо, існує достатньо вагомий резерв збільшення економічної ефективності використання ресурсів мережі за рахунок збільшення коефіцієнту завантаження її ВО корисним тафіком, шляхом застосування засобів прогнозування у контурі системи адаптивного керування ресурсами.

Поставлену задачу підвищення продуктивності використання ресурсів ВО (без погіршення якості обробки потоків пакетів) пропонується вирішити за рахунок реалізації засобів прогнозування у контурі системи адаптивного перерозподілу пропускної спроможності комутаційного обладнання між його портами у реальному часі. Тоді робота системи адаптивного керування буде полягати в тому, що пропускна спроможність комутатора буде розподілятися між його портами пропорційно інтенсивності потоків пакетів, що надходять до цих портів, а динаміка процесу перерозподілу буде співпадати із динамікою пульсацій трафіка. Дана технологія забезпечить виділення більшої частки від загальної пропускної спроможності комутатора для того порту, на вводі якого збільшилася інтенсивність потоку протокольних блоків даних, за рахунок частки пропускної спроможності порту, на якому в цей час спостерігається її зменшення або незмінність. Система адап-

тивного керування дозволить завантажити комутуюче обладнання мережі на 55 – 60 %. Недоліком запропонованої системи адаптивного керування є виникнення системних помилок регулювання, пов'язаних із недостатньої швидкодією системи, адаптивністю та дискретністю процесу такого перерозподілу. Системні помилки регулювання (недостатньої прогнозованості та високої динамічності пакетного трафіка) можуть суттєво знизити корисний ефект від застосування адаптивного способу управління комутаційного обладнання.

Аналіз літературних джерел показав, що ідея адаптивного керування потоками даних на портах ВО не нова, але ідея використання самих механізмів прогнозування в процесі адаптивного керування ще не висвітлювалась у публікаціях і не впроваджена в експлуатаційну практику. Дослідження основних характеристик пакетного трафіку показують, що пульсації потоку пакетів носять мало прогнозований характер та характеризуються високою динамікою виникнення, великим діапазоном амплітуд і тривалості існування. Виходячи з вище сказаного, механізми, які будуть забезпечувати реалізацію перерозподілу повинні мати високі динамічні характеристики. Зокрема, в моменти часу, коли інтенсивність потоку пакетів на якомусь порту швидко збільшується, то цьому порту треба практично миттєво виділити більшу частку пропускної спроможності комутатора (звісно, за рахунок зменшення часток пропускної спроможності, що виділяються іншим портам). І навпаки, якщо потік пакетів на якомусь порту швидко зменшується, то з відповідною динамікою необхідно зменшити і частку пропускної спроможності комутатора, яка цьому порту виділяється.

Для підвищення якості адаптивного управління в умовах значних пульсацій трафіку та боротьби з переліченими недоліками пропонується вдосконалити відому систему адаптивного управління за рахунок застосування засобів прогнозування пульсацій пакетного трафіку в задачах адаптивного керування. Це полягає в пристосуванні методу прогнозування пульсацій пакетного трафіку і швидкодіючих програмних механізмів їхньої реалізації до умов, коли ці механізми вбудовуються у контур системи адаптивного перерозподілу пропускної спроможності ВО між його портами і функціонують із швидкістю, що дозволяє змінювати смуги пропускання портів синхронно із пульсаціями пакетного трафіку. Встановлення механізмів прогнозування дозволяє використовувати в процесі управління раніш виміряну (апостеріорну) інформацію, що дає можливість системі прогнозувати можливу пове-

дінку потоків трендів на наступних кроках управління. Проте для ефективної роботи механізмів прогнозування, необхідно аби трафік, що надходить до ВО, відносився до асимптотично самоподібних процесів.

Введення цих елементів дозволяє якісно підвищити завантаженість мережевого обладнання, а також зменшити кількість системних помилок управління. Внаслідок цього мінімізується кількість проміжків часу, на яких інтенсивність трафіка більша за смуги пропускання портів і перевантаження обладнання виникає рідше.

У роботі поставлено та вирішено такі основні завдання:

– здійснено аналіз та дослідження впливу утворення помилок адаптивного регулювання та особливостей побудови моделі адаптивного управління, що забезпечує можливість зменшення негативного впливу цих помилок на якість прийняття управлінських рішень;

– досліджено представницькі вибірки пакетного трафіку, сучасних комп'ютерних мереж, для аналізу ймовірнісних характеристик та фрактальних властивостей; розроблено процедури віднесення пакетного трафіка до класу самоподібних процесів; аналіз можливих алгоритмів прогнозування, що можуть бути використані в механізмах керування перерозподілом пропускної здатності пакетного комутатора між його портами; вибір основних показників якості прогнозу, що враховують виявлену структуру пульсацій пакетного трафіку; вибір за результатами оцінювання найбільш ефективного алгоритму прогнозування;

– розроблено алгоритм та розрахункову схему технології прогнозування пульсацій потоків пакетів на портах ВО шляхом реалізації обраного на попередньому етапі найбільш ефективного методу прогнозування (метод прогнозування з використанням похідних).

– розроблено програмні механізми реалізації методу прогнозування пульсацій потоків пакетів з використанням похідних та відповідної структури програмного середовища, орієнтованого на здійснення порівняльного аналізу показників ефективності методу;

– експериментальні дослідження ефективності застосування названого вище методу прогнозування на експериментально отриманих типових вибірках пульсацій трафікового навантаження, зокрема оцінювання якості прогнозування цих пульсацій, а також швидкодії заділяної обчислювальної схеми, що відтворює розроблені механізми прогнозування; експериментальна оцінка технології адаптивного управління щодо можливостей підвищення завантаженості обладнання.

Включення в контур системи адаптивного регулювання перерозподілом пропускної спроможності ВО механізмів прогнозування пульсацій пакетного трафіка на його портах дає змогу забезпечити можливість збільшення завантаженості ВО комп'ютерних мереж та забезпечують ефективну роботу засобів адаптивного керування розподілом ресурсів пакетних мереж. Процедура усереднення потоків пакетів дозволяє певною мірою згладжувати пульсації трендів, що сприяє якості прогнозування трафіку, а встановлення механізму прогнозування – зменшувати кількість втрачених через системні помилки управління пакетів. Загалом маємо можливість значною мірою підвищити завантаженість ВО. Запропонована технологію адаптивного керування потоками даних на портах комутатору, дозволяє більш точно відслідковувати у реальному часі високу динаміку пульсацій реального трафіку пакетних даних у сучасних комп'ютерних мережах. Також метод прогнозування «поведінки» потоків даних на портах пакетних комутаторів (або маршрутизаторів) є оптимізованим для використання в технології адаптивного керування перерозподілом пропускної здатності комутатору між його портами.

Практичне значення отриманих результатів, полягає в тому, що розроблений метод прогнозування та інтерполяції пакетного трафіку і створена на основі цього методу технологія адаптивного керування ресурсами ВО комп'ютерних мереж придатні для реального застосування з більш ефективними характеристиками у порівнянні з існуючими технологіями керування завантаженням цього обладнання. Використання механізмів прогнозування трафіку на портах ВО дозволяє знизити вимоги до його швидкодії, що, у свою чергу, дозволяє суттєво знизити капітальні витрати на придбання такого обладнання для його експлуатації у реальних умовах функціонування комп'ютерних мереж.

Удосконалена технологія адаптивного перерозподілу пропускної спроможності ВО пакетних мереж зменшує негативний вплив утворюваних помилок адаптивного регулювання на якість управління цим обладнанням. Зокрема, впровадження цієї технології в експлуатаційну практику, як свідчать результати експериментальних досліджень, дозволяє забезпечити високий рівень завантаженості ВО (із значеннями коефіцієнту використання пропускної здатності комутуючого обладнання у діапазоні 0,65 – 0,75), не порушуючи при цьому сервісні угоди з клієнтами щодо забезпечення необхідних рівнів якості надання послуг.

УДК 004.72 (043.2)

С.В. Агеєнко
Національний авіаційний університет, м. Київ

ПРОЕКТУВАННЯ МЕРЕЖІ ЗАХИЩЕНОГО ТЕЛЕФОННОГО ЗВ'ЯЗКУ

Не дивлячись на широке впровадження автоматизованих і комп'ютеризованих систем обробки інформації, людська мова залишається одним з найважливіших шляхів інформаційної взаємодії. Більш того, при децентралізації економічної і політичної систем та відповідному збільшенні частки оперативної інформації, що безпосередньо зв'язує самостійних, в ухваленні рішень, людей, значущість мовного обміну зростає. Одночасно посилюється потреба в забезпеченні конфіденційності мовного обміну.

У даний час суб'єкт, зацікавлений в захищеному обміні інформацією між двома пунктами, може вибрати два шляхи.

Перший – підключення до захищеної державної системи зв'язку. Пропонований перелік послуг дозволяє задовольнити потреби у всіх видах зв'язку. Застосовуються сучасні методи криптографічного захисту, що практично виключають можливість несанкціонованого доступу до передаваної інформації з метою її розкрадання або спотворення.

У той же час цей шлях має ряд особливостей, що обмежують його застосування:

• захист забезпечується на рівні жорстких вимог захисту інформаційних ресурсів, що робить її достатньо дорогою і у багатьох випадках для комерційних цілей – надмірною;

• управління зв'язком, зокрема доступом до інформації опиняється в руках державної організації, довіра до якої з боку комерційних організацій не знаходиться на належному рівні.

У багатьох випадках переважним виявляється другий шлях – шлях організації інформаційного обміну по мережах зв'язку загального користування із забезпеченням захисту власними силами, як від перехоплення або спотворення інформації в каналі зв'язку, так і від перехоплення в місці розташування абонента, тобто створення налагодженої корпоративної захищеної мережі.

Таким чином виникає необхідність у мережі телефонного зв'язку, що забезпечить необхідним рівнем захищеності абонентів.

Проектована мережа – це шестизонова стільникова мережа мобільного та фіксованого електрозв'язку (телефонії і передачі даних) з комутацією пакетів, організована за радіально-вузловим принципом. У шести містах-центрах зон гіпотетично можливої мережі (це – міста Київ, Дніпропетровськ, Донецьк, Харків, Одеса та Тернопіль) встановлюються вузлові системи комутації абонентських радіоканалів з віддаленим винесенням базових станцій у сусідні обласні центри та інші великі населені пункти України, таким чином кожна зона обслуговування охоплює не одну, а кілька поруч розташованих адміністративних областей України. У містах-центрах зон поряд з комутаційним обладнанням встановлюється обладнання управління відповідним зоновим фрагментом мережі, а обладнання в м. Києві, крім того, виконує функції управління всією мережею у цілому. Комутаційна система київської зони з'єднується з п'ятьма іншими зоновими комутаційними системами за допомогою орендованих виділених міжміських каналів зв'язку типу Е1 з пропускними здатностями 2 Мбіт/с кожний. Усередині кожної зони обслуговування базові станції (в т.ч., винесені в інші міста) з'єднуються з відповідним зоновим комутаційним пристроєм за допомогою радіомодемних каналів зв'язку з пропускними здатностями n x Е1 (значення цілого числа n залежать від обсягів трафіку в цих каналах і знаходяться в межах $n > 2...16$).

Вибір місць розташування зонових комутаторів визначається топологією опорної мережі каналів міжміського зв'язку, в якості якої обрана мережа Frame Relay компанії телекомунікаційного сервісу ІНФОКОМ, що забезпечує високий рівень захисту інформації від несанкціонованого доступу та невисоку вартість.

Отже, за рахунок використання сучасних телекомунікаційних технологій забезпечується надання практично всіх відомих на сьогоднішній день послуг зв'язку (у тому числі, і послуг мобільного стільникового зв'язку з високою якістю зв'язку і захищеності інформації) у шкалі цін на послуги телефонної мережі загального користування. Мережа орієнтована на обслуговування вітчизняних та іноземних ділових кіл, які здійснюють свою діяльність в Україні, при цьому не виключається можливість користування її ресурсами будь-якими платоспроможними суб'єктами. Істотним також є те, що дана мережа під'єднується до елітних регіональних телефонних мереж в Україні.

УДК 004.056.34 (043.2)

І.Є. Терентьєва
Національний авіаційний університет, м. Київ

АНАЛІЗ НАДІЙНОСНИХ ХАРАКТЕРИСТИК ОБЛАДНАННЯ МЕРЕЖ ШИРОКОСМУГОВОГО РАДІОДОСТУПУ UMTS/WCDMA

В сучасному житті телекомунікаційні системи (ТКС) стандарту 3G UMTS/WCDMA набули широкого поширення у всіх сферах виробництва, військової галузі та в побуті. Це вимагає нового підходу до забезпечення якості обслуговування та зниження рівня відмов обладнання. Простої систем можуть принести великі фінансові збитки і знижують рівень інформаційної безпеки.

Для виключення подібних випадків, в даний час висуваються жорсткі вимоги до забезпечення готовності телекомунікаційних систем. Ця проблема є досить складною і потребує вирішення технічних завдань і математичного обґрунтування показників надійності.

Одним з методів вирішення цієї проблеми є резервування телекомунікаційного обладнання. Для забезпечення високого рівня готовності використовується трьох і навіть чотириразове резервування, але це вимагає великих капітальних вкладень, оскільки обладнання є дуже дорогим.

Аналіз вітчизняних і зарубіжних джерел [1–5] показує, що в даний час відсутній науковий підхід до обґрунтування структури резервування, переважно оцінки виконуються інтуїтивно на інженерному рівні, ґрунтуючись на досвіді експлуатації. Саме тому пропонується розробка наукового підходу до оптимізації структури і параметрів резервованих телекомунікаційних систем.

Для вирішення поставленого завдання пропонується розробити математичну модель процесу технічної експлуатації телекомунікаційного обладнання (ТКО) мереж широкосмугового радіодоступу UMTS/WCDMA, яка дає можливість враховувати максимальну кількість показників і факторів, що впливають на процес експлуатації; розробити критерії оптимізації технологій резервування ТКО; розробити методику вибору оптимальної технології резервування ТКО з ряду альтернативних варіантів; провести розрахунок показників ефективності телекомунікаційних систем, математичне моделювання та підтвердження адекватності розроблених моделей.

Пропонується оцінювати ефективність резервування комплексним критерієм, який засновано на максимізації коефіцієнта готовності при обмеженні з вартісної характеристики систем. Оцінка коефіцієнта готовності виконується на основі побудови математичної моделі процесу технічної експлуатації ТКС. Визначаються стани, в яких система може перебувати в процесі експлуатації, отримуються аналітичні вирази для оцінки середнього часу знаходження системи в кожному зі станів. Використовуючи ці вирази, знаходяться вирази для оцінки коефіцієнта готовності при різних законах розподілу напрацювання на відмову та різних видах резервування.

Оскільки резервування ТКО безпосередньо пов'язане з додатковими капітальними та експлуатаційними витратами, в якості вартісного показника пропонується використовувати показник ТСО (Total cost of Ownership – сукупну вартість володіння). Цей показник в даний час є найбільш універсальним для оцінки економічної ефективності інформаційно-комунікаційних систем і включає в себе основні складові експлуатаційних та капітальних витрат.

Таким чином, запропоновані показники та критерії дозволяють провести комплексну техніко-економічну оцінку ефективності введення різних видів резервування, що дає можливість забезпечити істотне підвищення готовності ТКС. Дані результати мають теоретичне і практичне значення і корисні для розробників телекомунікаційного обладнання, а також у процесі його експлуатації

Список літератури

1. Вишневский В.М. Энциклопедия WiMAX Путь к 4G / В.М. Вишневский, С.Л. Портной, И.В. Шахнович. – М.: Техносфера, 2009. – 472 с.

2. Диллон Б., Сингх Ч. Инженерные методы обеспечения надежности систем: пер. с англ. – М.: Мир, 1984. – 318 с.

3. Барлоу Р., Прошан Ф. Статистическая теория надежности и испытание на безотказность: пер. с англ. – М.: «Наука», 1984.

4. Nakagava T. Maintenance theory of reliability. – Springer: London. – 2005. – 269p.

5. Holma H., Toskala A. LTE for UMTS-OFDMA and SC-FDMA based radio access. – John Willey&Sons, Ltd.: London. – 2009. – 432 p.

УДК 004.716 (043.2)

В.С. Демченко
Національний авіаційний університет, м. Київ

СЕНСОРНІ МЕРЕЖІ ДЛЯ ОПТИМІЗАЦІЇ ЗАТРАТ НА ТЕПЛО ТА СВІТЛО

Безпровідні сенсорні мережі – це нова перспективна технологія, на основі якої інтенсивно ведуться прикладні розробки і виконуються масштабні проекти для різних галузей промисловості і систем спеціального призначення. За допомогою них можна вирішити завдання моніторингу та контролю. Об'єднані в бездротову сенсорну мережу датчики утворюють територіально-розподілену самоорганізовану систему збору, обробки і передачі інформації. Основною областю застосування являється контроль і моніторинг вимірюваних параметрів фізичних середовищ і об'єктів.

Оскільки, ціни на комунальні послуги зростають, в зв'язку з тим, що ціни на газ та світло різко підвищуються, було запропоновано розробити проект, аби розрахувати економічну ефективність сенсорних мереж для оптимізації затрат на тепло на світло. Для прикладу брався житловий будинок з розставленими в ньому сенсорами, які мають датчики тепла та світла. Це дало можливість для аналізу роботи сенсорних мереж та оцінки рентабельності їх використання.

Завжди були ситуації, коли був надлишок тепла чи світла, або ж навпаки, їх недостача, що в першому випадку приводить до марних витрат фінансів. Задача полягає в тому, щоб перевірити, наскільки ефективні сенсорні мережі для вирішення цих проблем.

Розрахунки показали, що сенсорні мережі ефективні для оптимізації витрат на тепло та світло, також дуже зручні завдяки своїм розмірам, зручності використання, довготривалості роботи, можливістю хаотичного їх розміщення, що дозволяє випадковим чином розташовувати їх у важкодоступних місцях. В цілому область застосування сенсорних мереж постійно розширюється і можна прогнозувати, що в перспективі всі фізичні об'єкти будуть забезпечені сенсорами, що мають IP-адреси з можливістю формування «Глобальної сенсорної мережі».

УДК 004.8 (043.2)

В.С. Волков
НТУУ «Київський політехнічний інститут», м. Київ

ВИКОРИСТАННЯ АЛГОРИТМУ МУРАШИНИХ КОЛОНІЙ ДЛЯ ІДЕНТИФІКАЦІЇ БАЗ НЕЧІТКИХ ЗНАНЬ

В роботі запропонований алгоритм параметричної ідентифікації баз нечітких знань (БНЗ) на основі модифікованого методу мурашиних колоній. Використання даного алгоритму дозволяє налаштувати параметри функцій належності та підвищити швидкість збіжності до оптимального значення за рахунок модифікації розрахунку вірогідності переходу.

Технологія нечіткого моделювання сьогодні стає все більш актуальною. Вона може бути успішно застосована при моделюванні складних систем з безліччю входів і виходів, в той час, як створення коректної математичної моделі досліджуваного об'єкта супроводжуються значними труднощами, а іноді й неможливістю реалізації. Також технологія знайшла широке використання і у системах націлених на управління та прийняття рішень. Одною з таких систем є БНЗ – сукупність логічних висловлень типу: ЯКЩО ($x_1 = a_1$) ТА ($x_2 = a_2$) ТО ($y = d_1$), що відображають вплив факторів $X = \{x_1, x_2\}$ на значення параметра y [1], де x_1, x_2 – лінгвістичні змінні (ЛЗ); a_1, a_2 – нечіткі терми, якими оцінюються змінні x_1 та x_2 відповідно. Однак, точність логічного виводу напряму залежить від налаштування структури та параметрів нечіткої моделі.

Для вирішення задачі параметричної ідентифікації будемо використовувати модифікований алгоритм мурашиних колоній (АМК), який базується на природній здатності мурах знаходити найкоротший шлях до їжі за рахунок виділення мурахами феромону. З часом феромон випаровується, тому найкоротші маршрути матимуть найбільшу кількість феромону й будуть пріоритетними [2].

Кожна ЛЗ описується кількома функціями належності (ФН), кожна ФН задається набором параметрів. Так для трикутної ФН – це три параметри, для трапецевидної – 4 і т.д. Для використання методу необхідно побудувати граф, вершинами (вузлами) якого будуть параметри ФН. Знаходженням параметрів кожної ФН займається окрема колонія [3]. Чисельність колонії дорівнює кількості параметрів ФН, так як в такому випадку спостерігається краща швидкість збіжності [2].

Кожен мураха, користуючись формулою вірогідності переходу p_{ij}, має відвідати рівно стільки вузлів, скільки параметрів в ФН.

$$p_{ij}^{k}(t) = \frac{\tau_{ij}(t)^{\alpha} \cdot \left(\frac{f_{ij}}{L^{k}(t)}\right)^{\beta}}{\sum_{i=1}^{N} \tau_{ij}(t)^{\alpha} \cdot \left(\frac{f_{ij}}{L^{k}(t)}\right)^{\beta}}, \qquad (1)$$

де $\tau_{ij}(t)$ – кількість феромону між *i*-ю та *j*-ю вершиною на *t*-ій ітерації; α, β – параметри, що вказують пріоритетність феромону чи помилки виводу; $L^{k}(t)$ – значення помилки виводу на *t*-ій ітерації для параметрів, обраних *k*-им мурахою; f_{ij} – «направляюча» функція, що має вигляд перевернутої параболи (див. рис. 1), яка в залежності від відстані між вершинами *i* та *j* приймає значення від 0 до 1. В класичному алгоритмі мурахи починають майже хаотично переміщуватись вузлами в пошуках кращого шляху. Так, як ФН одного терма навряд чи буде займати сусідні або далеко рознесені точки з області визначення ЛЗ, то вірогідність переходу до близько та далеко розташованих вершин буде менша. Вводячи «направляючу» функцію, мурахи з більшою вірогідністю перейдуть у вершини, які знаходяться на середній відстані від них, тим самим, швидкість збіжності алгоритму підвищиться.

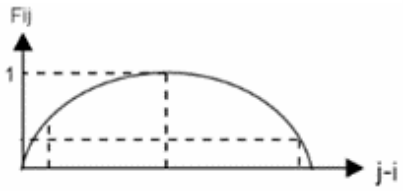

Рис. 1. Форма«направляючої» функції

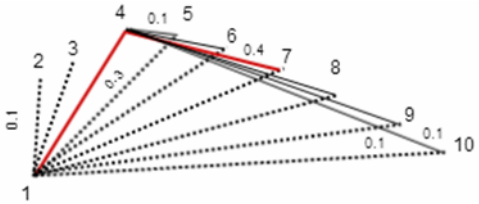

Рис. 2. Граф для 1-го мурахи

Після кожного переходу мурахи в наступний вузол, вершини, що знаходяться між *i*-м та *j*-м вузлом заносяться в табу-лист, тим самим забезпечується правильна форма ФН.

Після того як параметри ФН знайдені, визначається $L^{k}(t)$ та оновлюється значення феромону:

– приріст феромону: $\Delta\tau_{ij}^{k}(t) = \frac{1}{L^{k}(t)}$; (2)

– нанесення феромону: $\tau_{ij}(t+1) = \sum_{i=1}^{M}\left(\Delta\tau_{ij}^{k}(t) + \tau_{ij}(t)\right)\cdot\rho$; (3)

– випаровування феромону: $\tau_{ij}(t+1) = \tau_{ij}(t)\cdot(1-\rho)$, (4)

де M – кількість мурах, що пройшли ребром ij; $\rho \in [0;1]$ – коефіцієнт зниження феромону.

Умовою зупинення алгоритму є або виконання встановленої кількості ітерацій, або помилка менше заданої.

Отже, запишемо алгоритм параметричної ідентифікації БНЗ.

Крок 1. Задати початкові параметри.

Крок 2. Згенерувати мурах в колоніях.

Крок 3. Для кожного мурахи з колонії визначити параметри ФН використовуючи формулу вірогідності переходу (1).

Крок 4. Передати визначені параметри в систему та розрахувати помилку виводу. Якщо значення помилки менше за усі попередні – зберегти нові значення параметрів.

Крок 5. Якщо є наступна колонія – зробити її поточною та перейти на крок 3. Інакше – крок 6.

Крок 6. Оновити значення феромону за формулою (3).

Крок 7. Розрахувати випаровування феромону за формулою (4).

Крок 8. Якщо умова закінчення алгоритму виконана – зупинити алгоритм, інакше – перейти на крок 2.

В роботі запропоновано алгоритм параметричної ідентифікації БНЗ на основі методу мурашиних колоній. Модифікація розрахунку вірогідності переходу за рахунок введення «направляючої» функції дозволила збільшити швидкість логічного виводу результуючої БНЗ.

Список літератури

1. Суботін С.О. Подання й обробка знань у системах штучного інтелекту та підтримки прийняття рішень. – Запорізький національний технічний університет, 2008.

2. M. Tim Jones. Al Application Programming. – Charles River Media, 2003.

3. И.А. Ходашинский, И.В. Горбунов, П.А. Дудин. Алгоритмы муравьиной и пчелиной колонии для обучения нечётких систем. – Доклады ТУСУРа, № 2 (20), декабрь 2009.

УДК 654.165 (043.2)

С.В. Колотуша
Національний авіаційний університет, м. Київ

ТЕХНІКО-ЕКОНОМІЧНІ ХАРАКТЕРИСТИКИ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙНИХ ПІДПРИЄМСТВ

Розвиток ринку послуг зв'язку призводить до появи нових завдань, які вимагають свого вирішення. Одним з найважливіших є розробка концептуального підходу до комплексного аналізу ринку послуг зв'язку, нових економічних відносин і організаційних взаємозв'язків.

Дослідження ринку на сьогодні проводяться кожним оператором окремо, що задовольняє їхні потреби в отриманні інформації щодо стану локального ринку послуг зв'язку, але не може служити базою для формування комплексного підходу до аналізу стану, тенденцій та перспектив розвитку сфери телекомунікаційних послуг в цілому. Це також суттєво ускладнює оцінку впливу телекомунікацій на можливості використання телекомунікаційної інфраструктури для вирішення загальноекономічних завдань у масштабах національної економіки.

Проте, поява нових операторів зв'язку в якості самостійних підприємницьких структур і, як наслідок, зростання конкуренції між ними, позитивно впливає на розвиток ринку телекомунікаційних послуг і формування нових макро- і мікроекономічних процесів в галузі.

Безпосередньо питанням регулювання ринку телекомунікаційних послуг з точки зору розвитку його малоприбуткових сегментів приділено недостатньо уваги.

Мета дослідження полягає у визначенні специфіки ринку телекомунікацій і формулюванні на цій основі пропозицій щодо підвищення конкурентоспроможності телекомунікаційних компаній.

Для досягнення поставленої мети було вирішено наступні теоретичні і практичні завдання, що відображають логічну структуру і послідовність етапів проведеного дослідження:

1. Проаналізували особливості структури та умов функціонування ринку телекомунікаційного бізнесу в національному господарстві.

2. Проаналізували генезис розвитку телекомунікаційного бізнесу в економіці. На основі аналізу уточнені національні риси телекомунікаційного бізнесу, які полягають в тому, що елементи ринкових відносин у сфері телекомунікацій до теперішнього періоду значною мірою залежать від державної політики, здійснюваної в даній сфері.

3. Уточнили національні риси ринку телекомунікацій. На сучасному етапі розвитку, ринку телекомунікаційних послуг пріоритетним стає перехід від державної до підприємницької моделі організації діяльності телекомунікаційних компаній.

4. Дослідили специфіку функціонування телекомунікаційних компаній. Уточнена специфіка полягає в тому, що телекомунікації забезпечують державу інструментом управління та збереження національної безпеки; є великою галуззю, що динамічно розвивається, темпи зростання якої перевищують темпи зростання національної економіки.

5. Визначили характер взаємозв'язків учасників ринку телекомунікаційних послуг.

6. Вивчили економічні та організаційні можливості підвищення конкурентоспроможності телекомунікаційної компанії. З метою підвищення конкурентоспроможності запропонована імітаційна модель ринку телекомунікацій. Вона дозволяє управляти внутрішніми і зовнішніми факторами конкурентних відносин підприємств телекомунікаційних компаній.

7. Сформулювали рекомендації щодо вдосконалення бізнес-процесів на локальних ринках телекомунікаційних послуг на основі структурних перетворень.

В якості основних галузевих ризиків, характерних для сфери телекомунікаційних послуг, можна виділити:

1. Лібералізація ринку телекомунікації, яка тягне за собою появу нових конкурентів у сфері надання послуг міжміського та міжнародного зв'язку. Це призведе до витіснення вітчизняних операторів або, як мінімум, зниження їх частки ринку і одержуваних доходів .

2. Організаційно-технічні проблеми – брак кваліфікованого персоналу і нерозвиненість інформаційних та білінгових систем, що в довгостроковій перспективі може негативно відбитися на ринкових позиціях і фінансових результатах.

3. Недосконалість системи агентських відносин при наданні телекомунікаційних послуг призводить до того, що якість і своєчасність обслуговування кінцевих користувачів можуть виявитися незадовільними, що в свою чергу, може привести до втрати деяких існуючих і потенційних клієнтів.

4. Недосконалість системи державного регулювання тарифів і виплат по міжоператорським розрахункам перешкоджає встановленню

конкурентоспроможних тарифів з необхідним рівнем рентабельності по послугах міжміського зв'язку.

5. Незбалансованість фінансової системи телекомунікаційної компанії за рахунок того, що фактично основні телекомунікаційні послуги надаються в кредит з подальшою їх оплатою споживачами після закінчення звітного періоду.

6. Труднощі введення нових телекомунікаційних послуг, пов'язані як з фінансовими проблемами і недоліком технічних можливостей, так і з виникненням конкуренції між самими послугами.

Проведене дослідження дозволяє обґрунтовано говорити про те, що поставлені цілі і завдання досягнуті, завдяки чому отримані наступні висновки та узагальнення. В якості основних стимулів, які обумовлюють ефективність використання телекомунікаційних технологій економічними суб'єктами в ході господарської діяльності виступають:

- економічний інтерес – підвищення прибутку і рентабельності за рахунок використання технологій в просуванні власних послуг;

- можливість розробити нові види продукції і підвищити ефективність цього процесу за рахунок побудови контактів із споживачами, а також прискорення виведення нових продуктів на ринок;

- розширення сегмента ринку, можливість освоєння нових ринків за рахунок оперативного використання інформаційних потоків;

- можливість виходу підприємства на глобальні ринки за рахунок представлення в світовому інформаційному просторі та побудови комунікаційних мереж з потенційним партнером.

Розроблено імітаційну модель телекомунікаційного ринку, що дозволяє вирішувати більшість завдань, які виникають перед системним аналізом телекомунікаційного ринку, зокрема: за допомогою дослідження ринкового мікросередовища і внутрішніх факторів, які впливають на функціонування операторів, оцінити фактичний рівень споживання послуг і частку ринку, який займає кожен із суб'єктів ринку; на основі вивчення різних категорій споживачів визначити основні причини переваги тих чи інших послуг для споживачів різних категорій, визначити фактори і причини, які впливають на зміну попиту; на основі аналізу параметрів мікро- і макросередовища ринку визначити пріоритетні напрямки розвитку кожного з операторів, а також рівень конкурентоспроможності та ризику для кожного оператора і т.д. В якості основних елементів, що формують конкурентоспроможність, виділені: ціна, якість і маркетингові заходи.

УДК 004.056.34 (043.2)

Р.І. Рак
НТУУ «Київський політехнічний інститут», м. Київ

ОПТИМІЗАЦІЯ ПРОЦЕСУ ПЕРЕДАЧІ ОБСЛУГОВУВАННЯ В МЕРЕЖАХ LTE ЗА ДОПОМОГОЮ ІНТЕРФЕРЕНЦІЙНОЇ КООРДИНАЦІЇ

Long Term Evolution (LTE) – перспективний стандарт для систем стільникового зв'язку наступного покоління, який створений задля отримання пікової низхідної швидкості передачі на рівні 150 Мбіт/с. Однак, оскільки суміжні комірки використовують ту ж частоту, інтерференція між суміжними стільниками може погіршити швидкість передачі на краях стільників, перешкоджаючи отриманню достатньої пропускної здатності [1]. Тому інтерференційна координація між стільниками (Inter Cell Interference Coordination – ICIC) є перспективною технологією для вирішення цієї проблеми та підвищення швидкості передачі в бітах на краях стільників.

До цих пір було виконано багато досліджень з різними алгоритмами «жорсткого» HO (handover (HO) – передача обслуговування) для оптимізації продуктивності HO. В працях [2] і [3] адаптивні алгоритми HO представлені задля підвищення продуктивності HO. Конкретні проблеми, пов'язані з процесом HO в LTE розглядаються в [4], [5] і [6]. Емпірична модель для прогнозу та отримання точних рішень HO описується в роботі [4]. Дослідження [5] рекомендує нам діапазон HOM (handover hysteresis margin – коефіцієнт гістерезису, що дозволяє звести до мінімуму повторні передачі обслуговування між сусідніми стільниками) в дБ, розглядаючи середнє число HO для різних користувацьких швидкостей. Контекст [6] надає нам лінійні і доменні способи підвищення продуктивності L3-фільтра в умовах глобальної кількості передач обслуговування. Так більшість цих робіт розглядали окремий або спільний вплив вимірювального інтервалу, вимірювального усереднення, гістерезису і порогових рівнів HO і поліпшило продуктивність HO, динамічно адаптуючи алгоритм HO або параметри HO. Тим не менш прийняті методи шукають найкращий компроміс між числом HO і відмовами лінії радіозв'язку через помилковий прийом повідомлень HO.

У стандарті LTE інтерфейс між суміжними базовими станціями визначений для обміну інформацією про ICIC. Проте ніякі методи або алгоритми управління не були конкретно визначені для використання цього інтерфейсу, цим самим надаючи постачальникам базових станцій право розробляти їх самостійно. Та все ж при відсутності будь-якого зменшення інтерференції або координаційного механізму, інтерференція між стільниками в LTE стає критичною, особливо на краях стільників. Тому були запропоновані декілька конкретних схем, які б допомогли у вирішення проблеми ICI (Inter Cell Interference). Ці схеми класифіковані на основі типу їх координаційних механізмів інтерференції та розрізняють такі види: статичні та динамічні. Що ж стосується даної роботи, то в ній представлені результати дослідження і аналізу лише статичної схеми ICIC, яка також відома як схема із повторним використанням частоти.

Та незалежно від схем, велика частина робіт по моделюванню і дослідженню ICIC задля того, щоб показати виграші в продуктивності, була все ж зроблена на основі підвищення пропускної здатності на краях стільників. Проте, крім задачі забезпечення достатньої пропускної здатності, виникає й інша проблема, яка також може бути вирішена за допомогою ICIC, це проблема передачі обслуговування. Так HO має великий вплив на повнопродуктивні системи. В LTE продуктивність HO дуже сприйнятлива до інтерференції між стільниками (ICI). У першу чергу, це гостро відчувається на границях стільників, і по-друге, успішна процедура HO вважається завершеною тільки тоді, коли обладнання користувача (UE – User Equipment) отримує командне повідомлення HO від свого вихідного стільника. У цей час UE вже знаходиться в новому стільнику, і прийом команди HO від попереднього вихідного стільника дуже сильно піддається впливу ICI. Та ситуація стає більш критичною тоді, коли новий цільовий стільник є одночасно ще і джерелом інтерференції. Тому підвищення продуктивності HO в LTE було оцінено за допомогою ICIC.

Одне з рішень щодо пом'якшення ICI забезпечується використанням стандартної схеми повторного використання частот. Але цей метод не є досить доцільним в системах LTE через зменшення спектральної ефективності і втрати дорогоцінних частотних ресурсів.

Основна концепція, що використовується в даному дослідженні для ICIC полягає у тому, що вся смуга частот розділена на R підмно-

жин. Кожен стільник в мережі передає, щонайменше, одну підмножину зі зниженою потужністю. Така підмножина налаштована у відповідності з моделлю повторного використання в мережі. Конфігурація може бути здійснена або шляхом мережевого планування, або шляхом використання нових методів самоконфігурації. Дані про підмножини зі зменшеною потужністю від конкретного стільника та інших суміжних стільників забезпечує основу для інтерференційної координації. Оптимальне підсилення за допомогою даної схеми досягається лише тоді, коли алгоритм планування підходить для обладнання користувача на границях стільників з частотою підмножини, яка використовується зі зниженою потужністю в сусідньому стільнику.

В свою чергу UE здійснює моніторинг відфільтрованих значень RSRP (RSRP – Reference Signal Received Power – середнє значення потужності прийнятих пілотних сигналів) всіх виявлених стільників. Коли ж для заданого часу передачі обслуговування до тригера (TTT – time-to-trigger) має місце умова (1), UE посилає звіт про здійснені виміри до базової станції обслуговуючого стільника.

$$r_{ni} \geq r_{ns} + h\,, \tag{1}$$

де, r_{ni} – n-зразок фільтрованого RSRP будь-якого виявленого сектора i, крім обслуговуючого сектора;

r_{ns} – n-зразок фільтрованого RSRP обслуговуючого сектора;

h – заданий НОМ.

Після отримання звіту, поточна обслуговуюча базова станція готується до НО для нового цільового стільника за допомогою використання внутрішньої процедури мережі. Передбачається, що цільовий стільник завжди має доступні ресурси для вхідного UE. Час підготовки моделюється тут як стала протоколу затримки. Після того, як підготовка завершена, обслуговуючий стільник посилає повідомлення у вигляді команди НО на UE в низхідній лінії зв’язку.

Неточні вимірювання і невідповідні рішення НО можуть призвести до великої кількості непотрібних передач обслуговування. Для того, щоб визначити ці непотрібні НО, ми повинні відрізняти їх від необхідних передач обслуговування. Однією з головних причин виникнення непотрібних передач обслуговування є наявність завмирань у реальному середовищі. З цієї причини були використані рівні НО без

логу нормального затінення і без швидких завмирань в якості орієнтира для мінімальної кількості необхідних передач обслуговування. Також в результаті були нормалізовані абсолютні швидкості НО з еталоном і використанням нормованого рівня НО в якості другого показника продуктивності для оцінки кількості передач обслуговування.

При одночасному розгляді алгоритмів НО з L3-фільтром, НОМ і ТТТ було встановлено, що ICIC може використовуватися поверх цих методів для подальшого вдосконалення продуктивності НО, покращуючи радіоумови на кордонах стільників через інтерференційну координацію. А оскільки майбутнє поширення служб LTE робить мобільний широкосмуговий зв'язок реальністю, поліпшення швидкості передачі на краях стільників стане нагальною проблемою. Тому в подальшому планується вирішення цієї проблеми і сприяння майбутньому розширенню систем мобільного зв'язку, застосовуючи різні алгоритми ICIC до обладнання базових станцій LTE.

Список літератури

1. Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures, 3GPP TS36.213

2. An Adaptive Hard Handoff Algorithm for Mobile Cellular Communication Systems, Huamin Zhu, and Kyung Sup Kwak, ETRI Journal, vol. 28, no. 5, Oct. 2006, pp. 676–679.

3. Prakash, R., Veeravalli, V.V, "Adaptive Hard Handoff Algorithms", IEEE Trans. On Vehicular Technology Conference, 1991.

4. Prakash, R., Veeravalli, V.V, "Adaptive Hard Handoff Algorithms", IEEE Trans. On Vehicular Technology Conference, 1991.

5. Tae-Hyong Kim, Qiping Yang, Jae-Hyoung Lee, Soon-Gi Park, Yeon-Seung Shin, "A Mobility Management Technique with Simple Handover Prediction for 3G LTE Systems", IEEE Trans. On Vehicular Technology Conference, 2007.

6. M. Anas, F.D. Calabrese, P.E. Mogensen, C. Rosa and K.I. Pedersen, "Performance Evaluation of Received Signal Strength Based Hard Handover for UTRAN LTE", IEEE 65th Vehicular Technology Conference, April 2007.

УДК 621.391 (043.2)

А.Ю. Лавриненко, А.И. Давлетьянц
Национальный авиационный университет, г. Киев

СЖАТИЕ И ФИЛЬТРАЦИЯ РЕЧЕВЫХ СИГНАЛОВ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Одной из основных задач сжатия речевых сигналов является уменьшение потока передаваемых данных по цифровому каналу связи при незначительном ухудшении качества восстановленной речи на приемной стороне.

Поскольку речевой сигнал представляет собой нестационарный случайный процесс, то для его обработки было предложено использовать вейвлет-преобразование (ВП), которое позволяет разложить сигнал по функциям, локализованным как в частотной области, так и во временной области. В силу этого, ВП позволяет эффективно выделять временные и частотные особенности речевого сигнала. Свойства частотно-временной локализации и хорошо разработанные алгоритмы быстрого вейвлет-преобразования (БВП) обуславливают широкое применение ВП в области анализа нестационарных сигналов.

БВП может быть реализовано в виде каскадного соединения низкочастотных и высокочастотных фильтров или пирамидального алгоритма Малла. В этом случае полосовой фильтр для каждого масштаба состоит из пары дополняющих друг друга фильтров низких и высоких частот, относящихся к классу квадратурных зеркальных фильтров. Особенностью этого класса фильтров является то, что фильтр высоких частот получается из соответствующего фильтра низких частот простой перестановкой его коэффициентов в обратном порядке и изменением знака половины из них (только четных или только нечетных).

Процесс субполосовой фильтрации исходного сигнала $s(n)$, состоящего из N отсчетов ($N = 2^J$, где J – число масштабов или число каскадирования фильтров), может быть представлен в матричной форме дискретного вейвлет-преобразования: $\vec{c}_j = H_j \vec{c}_{j-1}$, $\vec{d}_j = G_j \vec{c}_{j-1}$, где $\vec{c}_j = \left(c_j(0), c_j(1), ..., c_j\left(N/2^j - 1\right)\right)$ и $\vec{d}_j = \left(d_j(0), d_j(1), ..., d_j\left(N/2^j - 1\right)\right)$ – векторы-столбцы выходов скейлинг-фильтра и вейвлет-фильтра для некоторого j, состоящие из коэффициентов, характеризующих спектр сигнала $s(t)$ и прореженных в два раза.

В качестве коэффициентов $c_j(n)$ на начальном значении масштаба $j = 0$ принимаются временные отсчеты исходного сигнала, т.е. $\vec{c}_0 = (c_0(0),..., c_0(N-1)) = (s(0), s(1),..., s(N-1))$ или $\{c_0(n)\}_{n=0}^{N-1} = \{s(kn)\}_{n=0}^{N-1}$. Итерационная процедура, заканчивается при некотором значении $j = J$, которое выбирается исходя из априорной информации о сигнале, т.е. из его продолжительности. На первом шаге многошаговой итерационной процедуры производится обработка временных отсчетов сигнала $\{s(n)\}_{n=0}^{N-1}$, а на каждом последующем – соответствующих коэффициентов c_j. На первом шаге вейвлетные коэффициенты $\{d_1(n)\}_{n=1}^{N/2}$ сохраняются как конечный результат, а скейлинговые коэффициенты $\{c_1(n)\}_{n=1}^{N/2}$ используются в качестве исходных данных и рекурсивно обрабатываются вплоть до конечного масштаба *J*. В результате рекурсивного выполнения процедуры будем иметь один вектор коэффициентов $\{c_J(n)\}$, вычисленный на последнем масштабе, и набор векторов коэффициентов $\{d_j(n)\}_1^J$, вычисленных на предыдущих масштабах. Дерево второго уровня разложения показано на рис. 1.

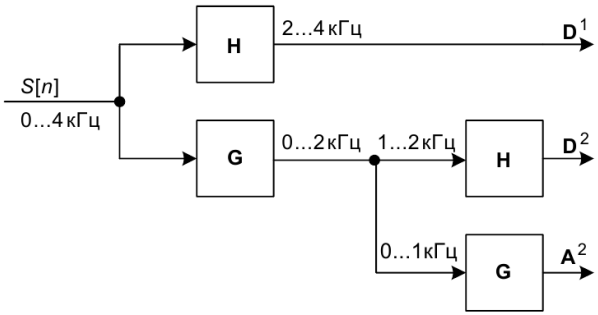

Рис. 1. Дерево второго уровня разложения

Интерпретация коэффициентов дискретного вейвлет-преобразования несколько сложнее, чем коэффициентов Фурье. Если анализируемый сигнал дискретизирован на частоте 8 кГц и состоит из 256 отсчетов, то верхняя частота сигнала 4 кГц. Тогда коэффициенты первого уровня разложения (128) занимают полосу частот

[2,0;4,0] кГц. Вейвлет-коэффициенты второго уровня (64) «отвечают» за полосу частот [1,0;2,0] кГц. Они отображаются перед вейвлет-коэффициентами первого уровня. Процедура повторяется до тех пор, пока не останется 1 вейвлет-коэффициент и 1 скейлинг-кэоффициент на 9 уровне. Всего получается (1 + 1 + 2 + 4 + 8 + 16 + 32 +64 + 128) = = 256 коэффициентов. То есть, число коэффициентов равно числу отсчетов в исходном сигнале. Если основная энергия сигнала была сосредоточена возле частоты 1,0 кГц, то вейвлет-коэффициенты второго уровня будут большими, а вейвлет-коэффициентами первого уровня можно пренебречь.

Обычно в качестве параметра, определяющего выбор вида материнского вейвлета, выступает внешнее сходство вида исследуемого сигнала и функции преобразования. Исходя из этого в качестве материнской вейвлет-функции использованы вейвлеты Добеши. Это один из самых известных вейвлетов и его основные свойства таковы:

1) функции имеют конечное число нулевых значений, т.е. система вейвлетов Добеши обладает свойствами гладкости и исключения моментов;

2) функции обладают свойствами компактности носителя (т.е. быстро нарастают и быстро спадают) и ортогональности, что обусловливает возможность точного восстановления произвольного сигнала;

3) вейвлеты имеют как вейвлет-функцию, так и скейлинг-функцию, что делает возможным кратномасштабный и быстрый вейвлет-анализ. То, что вейвлеты Добеши обладают свойством исключать моменты, означает, что они хорошо подойдут для сжатия сигналов, которые имеют большие гладкие области.

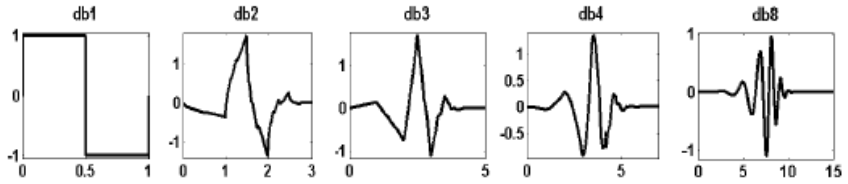

Рис. 2. Вейвлет-функции 1-, 2-, 3-, 4-, 8-го порядка семейства вейвлетов Добеши

Вейвлет-функция *db*2, представленная на рис. 2, имеет ряд интересных свойств. Она непрерывная, но не дифференцируемая. Функция

равна нулю вне интервала [0;3]. Нетрудно заметить, что гладкость вейвлетов возрастает по мере увеличения их номера. Одновременно растет и частота осцилляций. Эти вейвлеты имеют характерную асимметрию – нарастание функции растянуто по сравнению со спадом.

Уникальные свойства ВП позволяют сконструировать базис, в котором представление данных может выражаться небольшим количеством ненулевых коэффициентов. Это свойство делает ВП привлекательным для использования его, в качестве метода первичной обработки речевого сигнала для повышения эффективности его сжатия.

Процедура удаления шума либо сжатия сигналов выполняется с помощью ортогональных вейвлетов и включает в себя следующие операции:

– Вейвлет-разложение. На этом этапе происходит разложение сигнала, при котором задается уровень декомпозиции сигнала и тип вейвлета.

– Задание порогового уровня. При этом выбирается тип и определенный пороговый уровень очистки (сжатия) для детализирующих коэффициентов. Пороговые уровни бывают гибкими (в зависимости от номера уровня разложения) или жесткими (глобальными).

– Вейвлет-реконструкция. Восстановление сигнала на основе коэффициентов аппроксимации и модифицированных коэффициентов детализации, которые были модифицированы в соответствии с установленными условиями очистки (сжатия).

Для решения задач сжатия и очистки сигналов от шума с использованием вейвлетов есть метод ограничения уровня детализирующих коэффициентов. Задав определенный порог для их уровня и «отсекая» коэффициенты ниже этого порога, можно значительно снизить уровень шума и сжать сигнал. При этом устанавливаются различные правила выбора порога: адаптивный порог, эвристический, минимаксный и др. Но самое главное состоит в том, что пороговый уровень можно устанавливать для каждого коэффициента отдельно. Это позволяет строить адаптивные к изменениям сигнала способы очистки от шума и компрессии.

Список литературы

1. Воробьев В.И., Грибунин В.Г. Теория и практика вейвлет-преобразования. – СПб.: Изд-во ВУС, 1999. – 208 с.

2. Чуи К. Введение в вэйвлеты. – М.: Мир, 2001.

УДК 621.391.883:681.586.5 (043.2)

І.В. Харламов
Національний авіаційний університет, м. Київ

ОПТИМІЗАЦІЯ ПАРАМЕТРІВ АНАЛОГО-ЦИФРОВОГО ПЕРЕТВОРЕННЯ СИГНАЛУ

Значення аналого-цифрового перетворення в сучасних телекомукаційних та інших електронних системах важко переоцінити, оскільки переважаюча більшість сучасних засобів обробки сигналів розрахована на вхідний сигнал саме в цифровій формі. Але, як відомо, будь-яка перевага має свою альтернативну вартість. У випадку аналого-цифрового перетворення альтернативна вартість виражається у появі додаткового шуму - шуму квантування.

Потужність шуму квантування ідеального аналого-цифрового перетворювача (АЦП) залежить лише від його розрядності.

Потужність шуму квантування реального АЦП залежить, крім розрядності, від великої кількості його паспортних та експериментально виміряних параметрів. Дані параметри визначають нелінійність характеристик конструктивних елементів АЦП.

Боротьба з нелінійністю характеристик окремих елементів потребує втручання в апаратну частину АЦП, тому в більшості випадків не є можливим. Заміна АЦП на аналогічний (заданого типу та заданої розрядності) з покращенням передавальних характеристик не дає істотного ефекту зі зменшення похибки квантування. Тому пропонується здійснювати певне нелінійне перетворення сигналу до того, як він потрапить на вхід АЦП.

Відомо, що потужність шуму квантування може бути знижена шляхом врахування імовірнісних характеристик перетворюваного сигналу. При цьому, в області значень сигналу, що відповідають більш високому рівню щільності розподілу, рівні квантування повинні розташовуватися частіше, а в області низького рівня щільності розподілу - рідше. Нелінійна розстановка порогів квантування зокрема застосовується у відомих А і μ-законах перетворення, що враховують особливості мовних сигналів. В літературі пропозиції з урахування імовірнісних характеристик аналогового сигналу базуються на гіпотезі про необхідність використання нелінійного перетворення сигналу, що приводить його щільність розподілу до рівномірного закону розподілу. Проведене статистичне моделювання цифрового перетворення з

наступним відновленням сигналів показало, що нелінійні перетворення, які призводять до рівномірного розподілу сигналу, не є оптимальними з точки зору мінімізації шуму квантування.

Запропоновано й обґрунтовано методику визначення параметрів шуканого нелінійного перетворення. Параметри визначаються базуючись на законі розподілу дискретних відліків вихідного сигналу.

Запропонований підхід до оптимізації аналого-цифрового перетворення дозволяє найпростішими засобами знизити рівень шуму квантування без збільшення розрядності АЦП.

Отримані в процесі моделювання результати показали, що даний підхід дозволяє значно покращити якість відновленого на приймальній стороні аналогового сигналу. Ступінь покращення залежить від закону розподілу вихідного сигналу і є тим більшою, чим більше цей закон розподілу відрізняється від рівномірного.

Так, в процесі моделювання визначено, що за використання запропонованої методики потужність шуму квантування зменшилася на 27% при нормальному розподілі сигналу (математичне сподівання $M = 0{,}5$, СКВ $\sigma = 1/6$); на 29% при експоненціальному розподілі (параметр $\lambda = 4$) та на 32% при релеєвському розподілі (параметр $y = 0{,}25$).

Апріорна невизначеність, пов’язана з відсутністю повних імовірнісних характеристик перетворюваного сигналу може бути подолана використанням адаптивних модифікацій запропонованого алгоритму. Такі модифікації мають забезпечити побудову й аналіз закону розподілу сигналу в межах певного часового інтервалу, а також формування характеристики квантування в разі, якщо закон розподілу істотно відрізняється від рівномірного.

Запропоновано та випробувано один із варіантів адаптивного алгоритму. До кожного часового інтервалу перетвореного сигналу додається службове слово, що дозволяє виконати зворотне перетворення на приймальній стороні.

Для моделювання роботи адаптивного алгоритму були сформовані сигнали, в яких закон розподілу дискретних відліків змінюється у часі. В результаті адаптації характеристик перетворення отримано зменшення шуму квантування 20–35% в різних часових інтервалах, а довжина службового слова склала 0,1–0,5% від довжини корисних даних. Якщо динамічний діапазон вихідного сигналу менший за динамічний діапазон АЦП, зменшення шуму буде більш істотним.

УДК 004.716 (043.2)

І.В. Якименко, Р.С. Одарченко
Національний авіаційний університет, м. Київ

РІШЕННЯ ВІРТУАЛІЗАЦІЇ ДЛЯ ЦЕНТРІВ ОБРОБКИ ДАНИХ

У сучасному світі обсяг інформації щорічно подвоюється, і при цьому швидкість ведення бізнесу – збільшується. Щоб бути успішною, сучасній компанії доводиться не просто оперувати великими обсягами даних, а оперувати ними швидко та ефективно. Розуміючи потреби сучасного бізнесу, створюються ефективні та надійні рішення для зберігання і обробки даних (ЦОД). В основі рішення ґрунтується принцип доступу до корпоративних ресурсів по мережі та віртуалізація, яка дозволить раціонально розподілити навантаження на обладнання та забезпечити безперебійну роботу різних додатків. Рішення забезпечить зберігання, резервне копіювання та відновлення даних, гарантований доступ до всіх корпоративних додатків. При цьому територіальне розташування даних і серверів не буде мати значення, працювати з даними можна буде з будь-якого місця, маючи інтерфейс доступу та підключення до Інтернет.

Рішення віртуалізації дозволять зменшити витрати підприємства на апаратне забезпечення та електроенергію, а так само підвищать доступність надаваних мережевих сервісів. Центр обробки даних є основою інформаційної інфраструктури, і надає можливості ефективної роботи мережевих сервісів в мережі підприємства, а так само взаємодія між внутрішньою мережею і зовнішніми інформаційними ресурсами.

Використання центру обробки даних в компанії це грамотний спосіб побудови інформаційної системи, він забезпечує централізацію апаратних, програмних і керуючих ресурсів. ЦОД дозволяє знизити ризики втрати даних в слідстві аварій або помилок персоналу.

Надійність і безперервність роботи даної інформаційної системи обумовлена наявністю відмовостійких систем зберігання даних і мережевих вузлів, наявністю резервного каналу в інтернет, доступністю мережевих сервісів, підсистеми резервного живлення від джерел безперебійного живлення.

У випадку росту підприємства дана інформаційна система дозволить гнучко і ефективно нарощувати обчислювальні потужності, і пропускну здатність мережевих каналів без зупинки роботи і простоїв

мережевих сервісів, що особливо актуально для активно зростаючих і підприємств, що розвиваються.

У разі аварій або виведення з експлуатації (наприклад, для модернізації апаратної складової) фізичного сервера система даного ЦОД дозволить виконання його сервісів на обчислювальних потужностях, які залишилися.

Віртуалізація – це процес подання набору обчислювальних ресурсів, або їх логічного об'єднання, який дає певні переваги перед оригінальною конфігурацією.

Переваги застосування подібних рішень віртуалізації дуже значні:

- підвищення відмовостійкості;
- можливість плавного оновлення та нарощування апаратної платформи;
- збільшення можливостей масштабування інформаційної системи;
- ізоляція служб;
- можливість гнучкого розподілу ресурсів між службами;
- використання операційної системи, яка найкраще підходить для вирішення завдання.

Використання систем віртуалізації дозволить ефективно розподілити сервіси центру обробки даних, зменшити кількість простоїв і непродуктивної роботи серверного обладнання. Так само за допомогою цих систем буде можливо автоматичне відновлення працездатності сервісів у разі апаратних або програмних збоїв серверів. Для забезпечення цих можливостей необхідно використовувати як мінімум два фізичних сервера, однаковість мережевого середовища в сегменті віртуалізації і єдине сховище для реалізації концепції кластера віртуалізації. При цьому, у разі відмови одного сервера, потужності серверів, що залишилися, має бути достатньо для виконання всіх сервісів.

УДК 004.738 (043.2)

О.С. Тимошенко, О.П. Ткаліч
Національний авіаційний університет, м. Київ

ІНТЕГРАЦІЯ МЕРЕЖ ПЕРЕДАЧІ IP-ТРАФІКУ З СИСТЕМАМИ ВІДЕОСПОСТЕРЕЖЕННЯ ОБ'ЄКТІВ

На сьогоднішній день одим з найважливіших елементів системи безпеки є камера відеоспостереження. Окрім системи безпеки вони можуть виконувати й інші задачі. В процесі збільшення користувачів смартфонів, планшетів та постійного покращення технологій, з'являється все більше потреб та варіантів, які покращують та спрощують дії, що виконуються щоденно.

Метою проекту є інтеграція провідної та безпровідної мережі, які знаходяться в торгівельному приміщенні. Провідна мережа містить: касові апарати, систему відеоспостереження та сервери. Безпровідна мережа містить Wi-Fi точки доступу, які надають покупцю доступ до мережі торгівельного приміщення. Покупець, встановивши програму магазина на свій смартфон, може вдома зіставити список потрібних йому речей, а при вході в магазин отримає інформацію про ціну та наявність продукту, а у випадку відсутності, запропонує наявні альтернативи. Програма зображує місцезнаходження людини у магазині та пропонує оптимальній маршрут для купівлі всіх товарів зі списку. За допомогою програмного продукту, користувач отримує з камери відеоспостереження зображення, на якому червоною рамкою виділяється місцезнаходження на полиці даного товару, що спрощує його пошук, а отже й скорочує час для купівлі.

В проекті проводиться аналіз та вибір кодування й стиснення відео, враховуючи потрібну чіткість зображення, вибір камер відеоспостереження та регістратору, для потрібної якості зображення. Згідно зі статистикою відвідуваності та одночасним обміном даних розраховується максимальна та середня завантаженість мережі. Проводиться моделювання топології мережі касових апаратів з серверами та системою відеоспостереження. Описується функціонування програмного продукту, актуальність, зручність та корисність даного проекту.

УДК 004.056.53 (043.2)

А.Б. Кочубей
Національний авіаційний університет, м. Київ

ЗАХИСТ ХОСТУ ВІД ХИБНОГО МАРШРУТУ З ВИКОРИСТАННЯМ ПРОТОКОЛА ICMP З МЕТОЮ СТВОРЕННЯ В МЕРЕЖІ INTERNET ХИБНОГО МАРШРУТИЗАТОРА

Інформаційні технології в усіх галузях життя бурхливо розвиваються. Інформація, в дедалі більшій мірі, стає стратегічним ресурсом держави, продуктивної силою і найдорожчим товаром. Це може викликати прагнення держав, громадських організацій і окремих осіб отримати переваги за допомогою оволодіння інформацією, недоступної опонентам, і навіть заподіяти шкоду інформаційним ресурсам супротивника задля своїх потреб. А в зв'язку з широким впровадженням інформаційних технологій, об'єднання телекомунікаційних систем істотно актуальною стала проблема забезпечення інформаційної безпеки в телекомунікаційних мережах. Для ефективного вирішення даної задачі необхідний аналіз усіх можливих способів та методів несанкціонованого доступу до інформації в комп'ютерних системах, що дозволяє вчасно вжити заходів для протидії можливим загрозам.

У мережі Internet використовується керуючий протокол ICMP, однією з функцій якого є віддалене управління маршрутизацією на хостах всередині сегмента мережі. Віддалене управління маршрутизацією необхідно для запобігання можливої передачі повідомлень по неоптимальному маршруту. У мережі Internet віддалене управління маршрутизацією реалізовано у вигляді передачі з маршрутизатора на хост керуючого ICMP-повідомлення: Redirect Message. Дослідження протоколу ICMP показало, що повідомлення Redirect буває двох типів:

– перший тип повідомлення носить назву Redirect Net і повідомляє хост про необхідність зміни адреси маршрутизатора, тобто default-маршруту;

– другий тип – Redirect Host – інформує хост про необхідність створення нового маршруту до вказаної в повідомленні системи і внесення її в таблицю маршрутизації. Для цього в повідомленні вказується IP-адреса хоста, для якого необхідна зміна маршруту (адреса буде занесена в поле Destination), і нову IP-адресу маршрутизатора, на який необхідно направляти пакети, адресовані даному хосту (ця адреса заноситься в поле Gateway).

Необхідно звернути увагу на важливе обмеження, що накладається на IP-адресу нового маршрутизатора: він повинен бути в межах адрес даної під мережі.

Що стосується керуючого повідомлення ICMP Redirect Host, то єдиним ідентифікуючим його параметром є IP-адреса відправника, який повинен співпадати з IP-адресою маршрутизатора, так як це повідомлення може передаватися тільки маршрутизатором. Особливість протоколу ICMP полягає в тому, що він не передбачає ніякої додаткової аутентифікації джерел повідомлень. Таким чином, ICMP-повідомлення передаються на хост маршрутизатором однонаправлено, без створення віртуального з'єднання.

Отже, ніщо не заважає атакуючому послати помилкове ICMP-повідомлення про зміну маршруту від імені маршрутизатора. Наведені вище факти дозволяють здійснити типову віддалену атаку «Впровадження помилкового об'єкта шляхом нав'язування хибного маршруту».

Для здійснення цієї віддаленої атаки необхідно підготувати хибне ICMP Redirect Host повідомлення, у якому вказати кінцеву IP-адресу маршруту (адреса хоста, маршрут до якого буде змінений) і IP-адресу помилкового маршрутизатора. Далі це повідомлення передається на хост, який атакується, від імені маршрутизатора. Для цього в IP-заголовку в полі адреси відправника вказується IP-адреса маршрутизатора.

Розглянемо функціональну схему здійснення цієї віддаленої атаки, яка показана на рис. 1: передача на хост, який атакується, хибного ICMP Redirect Host повідомлення; відправлення ARP-відповіді у разі, якщо прийшов ARP-запит від хоста, який атакується; перенаправлення пакетів від хоста, який атакується, на справжній маршрутизатор; перенаправлення пакетів від маршрутизатора на хост, який атакується; при прийомі пакету можливий вплив на інформацію за схемою «Помилковий об'єкт».

Було розглянуто віддалену атаку, яка полягала у передачі на хост помилкового ICMP Redirect повідомлення про зміну вихідного маршруту. Ця атака призводила як до перехоплення атакуючим інформації, так і до порушення працездатності хоста, який атакується.

Для того, щоб захиститися від даної віддаленої атаки, необхідно або фільтрувати дане повідомлення (використовуючи Firewall або фільтруючий маршрутизатор), не допускаючи його попадання на кінцеву систему, або відповідним чином вибирати мережну ОС, яка буде ігнорувати це повідомлення.

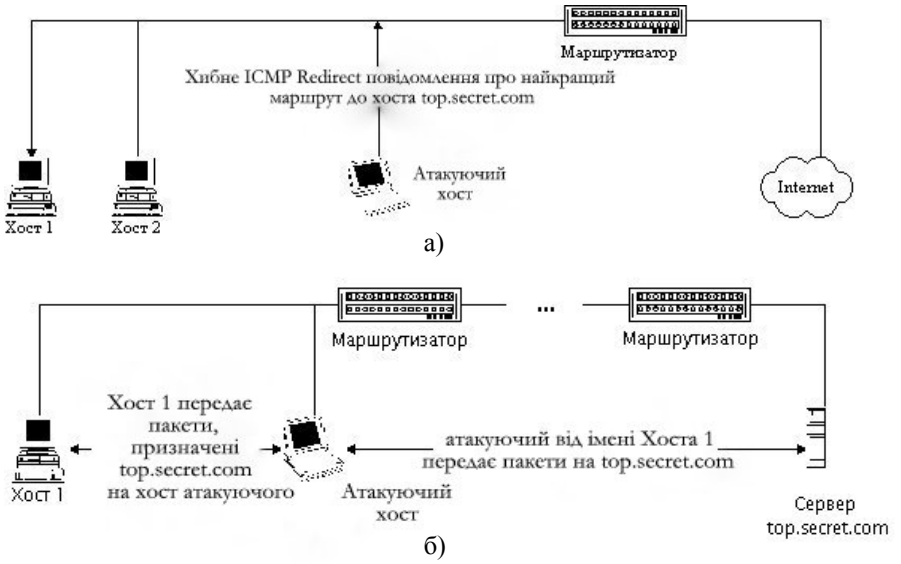

Рис. 1. Внутрішньосегментне нав'язування хосту хибного маршруту при використанні протоколу ICMP: а) – фаза передачі хибного ICMP Redirect повідомлення від імені маршрутизатора; б) – фаза прийому, аналізу, впливу і передачі перехопленої інформації на хибному сервері

Проте зазвичай не існує адміністративних способів вплинути на мережеву ОС так, щоб заборонити їй змінювати маршрут і реагувати на дане повідомлення. Єдиний спосіб, наприклад, у випадку ОС Linux полягає в тому, щоб змінити вихідні тексти і перекомпілювати ядро ОС. Очевидно, що такий екзотичний для багатьох спосіб можливий тільки для вільно розповсюджуваних разом з вихідними текстами операційних систем. Зазвичай на практиці не існує іншого способу дізнатися реакцію використовуваної ОС на ICMP Redirect повідомлення, як відправити дане повідомлення і подивитися, яким буде результат. Слід зазначити, що продукти компанії Microsoft не відрізняються особливою захищеністю від можливих віддалених атак, властивих IP-мереж. Отже, використовувати дані ОС в захищеному сегменті IP- мережі представляється небажаним. Це і буде тим самим адміністративним рішенням по захисту сегмента мережі від даної віддаленої атаки.

УДК 004.8 (043.2)

Ю.В. Василенко
НТУУ «Київський політехнічний інститут», м. Київ

МЕТОД СТРУКТУРНОЇ ІДЕНТИФІКАЦІЇ БАЗ НЕЧІТКИХ ЗНАНЬ

У даній роботі розглянуто вдосконалений метод структурної ідентифікації нечітких систем, робота якого заснована на нечіткому алгоритмі с-середніх у комбінації з рандомізованим алгоритмом пошуку кількості кластерів. У роботі [1] було запропоновано застосування алгоритмів нечіткої та гірської кластеризації для структрної ідентифікації БНЗ. Проте, результати моделювання показали, що ці методи мають ряд недоліків, а саме: необхідність апріорного знання кількості кластерів, великі обчислювальні витрати, недостатня якість виводу результуючої системи.

В запропонованому методі для ініціалізації алгоритму нечітких с-середніх застосовується рандомізований алгоритм пошуку кількості кластерів заснований на індексній функції Сьюгер-Джеймса [2]. Використання даного алгоритму дозволяє значно зменшити час виконання структурної ідентифікації порівняно з методом заснованим на гірській кластеризації та отримати систему з достатньою точністю виводу.

Після знаходження кількості кластерів, проводиться кластеризація нечітким с-середніми та подальша структурна ідентифікація нечіткої системи, тобто знаходження правил та термів БНЗ. Проте використаний у [1] підхід з апроксимацією матриці належності для побудови функцій належності лінгвістичних змінних пропонується замінити використанням центроїдів. Побудова функцій належності відповідно до центроїдів значно легша з обчислювальної точки зору, та дає якісні результати, що перевірено під час моделювання бази нечітких знань.

На етапі побудови функцій належності пропонується об’єднувати близько розташовані терми, так як це підвищує якість отриманої системи та зменшує кількість термів. В якості функцій приналежності можна обрати одну із стандартних функцій. В даній роботі була обрана трапецієвидна.

Блок-схема запропонованого методу структурної ідентифікації нечітких баз знань приведена на рис. 1.

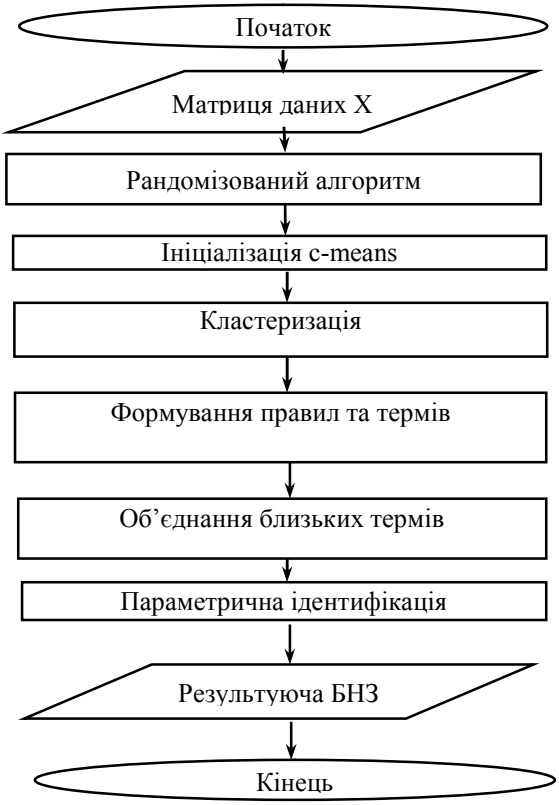

Рис. 1. Блок-схема методу структурної ідентифікації нечітких баз знань

Проведено огляд методу структурної ідентифікації, який дозволить зменшити час побудови правил та термів нечітких систем при достатній якості виведення.

Список літератури

1. Штовба С.Д. Проектирование нечётких систем средствами MATLAB / С.Д. Штовба. – М.: Горячая линия. – Телеком, 2007. – 288 с.

2. О.Н. Гринчин, Д.С. Шалымов, Р. Аврос, З. Волкович Рандомизированный алгоритм нахождения количества кластеров, 2011 г.

УДК 004.7 (043.2)

М.О. Коренюк
Національний авіаційний університет, м. Київ

НАДАННЯ ПОСЛУГ ІНТЕРНЕТ З ВИКОРИСТАННЯМ ШИРОКОСМУГОВИХ БЕЗДРОТОВИХ СИСТЕМ НА БАЗІ ОБЛАДНАННЯ MIKROTIK

Важко уявити собі сьогодні персональний комп'ютер без мережі – будь це локальна мережа або Інтернет. Головна характеристика, яка при цьому цікавить користувача – швидкість передачі даних між комп'ютерами або комутаторами. Як відомо, міські жителі «мегаполісів», а також жителі невеликих міст України користуються проводовим або оптоволоконним доступом в Інтернет. Доступ до Інтернету в містах надають Інтернет провайдери, оператори стільникових мереж, які мають дуже розвинену дротову або бездротову мережу, з'єднану з високошвидкісними каналами передачі даних. Саме завдяки інфраструктурі міста, наявності багатоквартирних будинків, а також щільно заселених територій, підключитися до глобальної мережі в міських умовах не є складним. У містах бездротовим Інтернетом практично ніхто не користується, виняток становлять мешканці приватного сектора, а також приватні ділянки, куди Інтернет провайдери ще не дійшли, тобто не протягнули свої мережі. Якщо ж у місті підключитися до глобальної мережі не проблема, то виїжджаючи за місто, наприклад, на дачу, стає зрозумілим, що міського Інтернету, який є звичним, там немає. Без високоякісного Інтернету багато людей почувають себе відірваними від цивілізації. Розуміючи важливість даної проблеми, було вирішено спеціально для дачних жителів представити нову технологію бездротового Інтернет доступу. Для виходу в Інтернет на дачі чи в селі, за умов використання цієї технології, не будуть потрібні наземні комунікації, тобто метою проекту є створення сегменту мережі доступу до Інтернет в місцях не охоплених проводовими технологіями надання послуг з передавання даних. З економічної та технічної точки зору найбільш реальним є використання безпроводових технологій для втілення масового проекту, а саме проектування мережі буде відбуватися на базі стандарту IEEE 802.11n з використанням обладнання радіодоступу виробництва MikroTik. Таким чином, новий сегмент повинен забезпечити можливість покриття великої площі з низькою середньою концентрацію домогосподарств в населених пунктах з відсутньою наземною оптичною інфраструктурою.

УДК 004.413 (043.2)

А.Ю. Спиридонов, Ж.А. Шевчук, Р.С. Одарченко
Национальный авиационный университет, г. Киев

МНОГОУРОВНЕВЫЙ АНАЛИЗ СБОЕВ В РАБОТЕ СЕТИ

Контроль состояния сети и оперативное исправление неполадок является ключевой задачей администрирования сети. Одним из подходов к диагностике неполадок сетей является распределение всего процесса коммутации на участки (этапы). В данной работе были рассмотрены возможность разделения на этапы диагностики на основе модели взаимодействия открытых систем OSI**.**

В частности, предложено было проводить диагностику поэтапно в соответствии с уровнями модели OSI. При отсутствии неполадок на определенном уровне необходимо двигаться вверх на один уровень и проверять возможное наличие неисправности на данном уровне.

Поэтапно процесс диагностики следующий. На физическом уровне диагностику возможно выполнить несколькими способами:

- программно – с помощью командной строки (например, команда ping) для проверки работы и доступности сетевых устройств;
- инструментально – с помощью сетевых тестеров для проверки целостности сети.

С помощью программ мониторинга и анализа сети возможно проверить следующие 6 уровней модели OSI:

- на канальном – целостность кадров (проверка подуровней MAC, LLC);
- на сетевом – целостность пакетов дейтаграмм (с помощью ICMP);
- на транспортном – целостность сегментов и работу протоколов данного уровня (например, TSP ,UDP, RDP и т.д.);
- на сеансовом – проверка контрольных точек, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, а не начинать всё с начала; на практике немногие приложения используют сеансовый уровень и он редко реализуется в виде отдельных протоколов, хотя функции этого уровня часто объединяют с функциями прикладного уровня и реализуют в одном протоколе;
- на представительском – корректность синхронизации работы различных систем в данной сети;
- на прикладном – правильность настройки протоколов данного уровня (DNS, FTP, HTTP, NFS, POP, POP3, SMTP).

УДК 004.733 (043.2)

І.М. Смолянюк
Національний авіаційний університет, м. Київ

ВИСОКОШВИДКІСНА МЕРЕЖА ІНТЕРНЕТ

Сьогодні суттєвим напрямом розвитку мережевих технологій є отримання найбільшої продуктивності як локальних мереж, так і глобальних каналів зв'язку. У сучасних умовах якість та швидкість обміну даними є найважливішим фактором. Проектування високошвидкісної мережі для житлових комплексів є актуальним так як сучасні комплекси вимагають забезпечення якісної роботи наступних технологій: передача даних до 1000 Мбіт/с, IPTV, точки доступу WiFi на території, відеоспостереження, система охорони, дистанційна передача показників лічильників.

Для забезпечення всіх перерахованих послуг використано технологію GPON. PON (Passive optical network) – технологія пасивних оптичних мереж, «G» – гігабітні. Суть технології PON полягає в тому, що між приймально-передавальним модулем центрального вузла OLT (Optical line terminal) і віддаленими абонентськими вузлами OLT створюється повністю пасивна оптична мережа, що має топологію дерева. У проміжних вузлах дерева розміщуються пасивні оптичні розгалужувачі (сплітери) – компактні пристрої , які не потребують живлення та обслуговування. Один приймально-передавальний модуль OLT дозволяє передавати інформацію безлічі абонентських пристроїв ONT. Число ONT, підключених до одного OLT, може бути настільки великим, наскільки дозволяє бюджет потужності і максимальна швидкість приймально-передавальної апаратури. Маємо високу пропускну здатність каналу і як наслідок можливість підключення декількох послуг по одній лінії – Інтернет, IPTV, телефон. За основу GPON було прийнято базовий протокол SDH (а точніше SDH на протоколі GFP) з усіма витікаючими перевагами та недоліками. GPON підтримує ATM, IP, мову і відео (інкапсульовані в кадри GEM – GPON Encapsulated Method), а також модулі SDH. Мережа працює синхронно з постійною тривалістю кадру.

Мережі SDH відносяться до класу мереж з комутацією каналів, що використовують синхронне мультиплексування з розділенням часу (Time Division Multiplexing, TDM), при якому інформація від окремих абонентів адресується відносним часовим положенням усередині

складеного кадру, а не явною адресою, як це відбувається в мережах з комутацією пакетів. Схема мультиплексування стандартизована на міжнародному рівні, що забезпечує сумісність устаткування різних виробників. Мережі SDH володіють високим ступенем «живучості» – технологія передбачає автоматичну реакцію устаткування на такі типові відмови, як обрив кабелю, відмову порту, вихід з ладу мультиплексора або окремої його карти, направляючи трафік по резервному шляху або переходячи на резервний модуль. Перехід на резервний шлях відбувається дуже швидко – зазвичай протягом 50 мс.

M-Bus (Meter-Bus) – комунікаційний протокол. Заснований на стандартній архітектурі «клієнт-сервер». Один з поширених протоколів передачі даних для ряду специфічних пристроїв, таких як прилади обліку електричної енергії (електролічильники), теплової енергії (теплолічильники), витратоміри води і газу. Дані передаються на комп'ютерну станцію (сервер) безпосередньо або через концентратори шини M- Bus, а також підсилювачі-повторювачі сигналу. Дані системі передаються, використовуючи завадозахищений протокол M-Bus. Цей протокол використовується в схемі один майстер – багато Slave. У кожному сегменті мережі використовується один майстер, який направляє запити і отримує відповідь від кожного пристрою. Така схема дозволяє уникнути конфліктів в мережі. Дані передаються по шині в послідовному режимі. Щоб передати біт даних, майстер змінює в шині напругу. Кожен з пристроїв прослуховує даний сигнал, дізнаючись, яке з них отримує запит. Пристрій, до якого йде звернення передає біти даних у відповідь, змінюючи напругу в шині, які зчитує майстер. Для передачі даних в різні типи мереж (локальну, глобальну, по оптоволоконних мережах), використовуються конвертери.

З використанням даних технологій у проектуванні мережі в новозбудованому сучасному комплексі отримуємо безпечний комплекс, високошвидкісний та якісний зв'язок і додатково забезпечуємо роботу технології дистанційної передачі показників лічильників.

УДК 004.722 (043.2)

О.А. Вегер
Національний авіаційний університет, м. Київ

ЛОКАЛЬНА МЕРЕЖА ПІДПРИЄМСТВА

В даний час одним з основних стратегічних напрямків розвитку і техніки є інтеграція телекомунікаційних систем (ТС) та їх технічних засобів для передачі і прийому неоднорідного трафіку. Це завдання вирішується шляхом створення багатофункціональних та інтелектуальних мереж. Такі комплекси повинні створюватися на основі функціонально-блокових систем (маршрутизатори, комутатори, шлюзи, інтерфейси, концентратори і елементи управління).

Метою проекту є створення локальної мережі підприємства за допомогою відомих топологій та технологій сімейства Ethernet. Створення та реалізація технології локальної мережі виконується з урахуванням цілей для яких буде використана дана мережа її користувачами. А саме для передачі змішаного трафіку: мультимедійні додатки, наприклад, потокове відео, відеоконференції в локальній мережі, голосовий зв'язок по мережі тощо. Пакет Microsoft Office для підтримки постійно оновленої версії для кожного користувача, – зручніше здійснювати мережну установку цього продукту, додатки клієнт-сервер для роботи з базами даних, Intranet-додатки де характерна багаторівнева обробка. Для виконання однієї програми використовується кілька серверів: Web, БД, бізнес-логіки і т.д. Необхідна висока пропускна здатність для зв'язку цих серверів між собою і з клієнтами.

Відповідно до вищевикладеного, у процесі виконання проекту були вирішені такі основні завдання: моделювання раціональної топології локальної мережі з урахуванням вимог до неї та обраних технологій передачі даних. Для обраної топології локальної мережі було обрано тип та кількість мережевого обладнання, яке здатне задовольнити висунуті вимоги. Здійснено аналіз якості функціонування, стану розробки, систематизація основних характеристик їх ефективності, зокрема: пропускної здатності, швидкості передачі даних, час реакції на запит та максимальна кількість трафіку, який одночасно передається у мережі. Здійсненна конфігурація та налагодження обраного мережевого обладнання.

УДК 629.7.054 (043.2)

Д.В. Шемет
Національний авіаційний університет, м. Київ

МЕТОДИ СТВОРЕННЯ ЗАХИЩЕНОГО РАДІОКАНАЛУ КЕРУВАННЯ БЕЗПІЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ

В час розвитку робототехніки постає питання захищеного каналу керування пристроями такими як БПЛА. Є декілька способів управління БПЛА віддалено за допомогою різного обладнання та каналів зв'язку. Використовуючи частоту таку як 433 МГц потрібно враховувати при передачі керування швидкість шифрування даних.

Наприклад алгоритм шифрування ГОСТ 28147-89, одним з його режимів є так званий метод простої заміни. Цей алгоритм відноситься до розряду блокових шифрів, в архітектурі яких інформація розбивається на кінцеву кількість блоків, кінцевий звичайно може бути не повним. Процес шифрування відбувається саме над повними блоками, які і утворюють шифрограму. Кінцевий блок, якщо він неповний доповнюється чим-небудь і шифрується так само як і повні блоки.

Для роботи даного методу алгоритму необхідно розбити інформацію на блоки розміром в 64 біта, згенерувати або ввести в систему шифрування наступну ключову інформацію: ключ і таблицю замін.

Саме шифрування полягає у використанні, так званих базових циклів, які в свою чергу включають в себе *n*-у кількість основних кроків криптоперетворень. Базовим циклам можна надати маркування: *n-m*, де *n* – кількість основних кроків криптоперетворень в базовому циклі, а *m* – «тип» базового циклу, тобто мова йде про «З» – зашифровування або «Р» – розшифровування даних. Базовий цикл шифрування 32-З складається з 32-х основних кроків криптоперетворень. У функцію, що реалізує дії кроку подають блок *N* і елемент ключа К, причому перший крок відбувається з к1, другий над отриманим результатом з елементом к2 і т.д. Процес розшифрування 32-Р відбувається аналогічним чином, але елементи ключа подаються у зворотній послідовності.

Таким чином даний метод шифрування для захищеного каналу керування БПЛА має такі позитивні властивості: виключається вплив перекриття шифру на стійкість шифрування, можливо розшифрувати будь-який блок незалежно від його місця розташування в криптограмі, простота синхронізації.

УДК 621.391 (043.2)

І.В. Іванченко
Національний авіаційний університет, м. Київ

РОЗРОБКА УДОСКОНАЛЕНОЇ СИСТЕМИ КЕРУВАННЯ РІВНЕМ ВИПРОМІНЮВАНОЇ ПОТУЖНІСТІ БАЗОВИХ СТАНЦІЙ МЕРЕЖ LTE

Однією з технологій, призначених для вирішення нагальних завдань сучасних телекомунікацій, є технологія Long Term Evolution, або, скорочено, LTE-технологія. Long Term Evolution (довготривалий розвиток) – це інтеграція з вже існуючими протоколами, підвищення швидкості та ефективності передачі даних, зниження витрат, а також поліпшення і розширення послуг, що надаються. Сервіси, які може запропонувати мережа четвертого покоління, починаються від передачі голосу і даних до мультимедіа та відео. Розвиток нових мережевих технологій, що забезпечують надання все більшого числа різноманітних послуг, змушують світове телекомунікаційне співтовариство поглянути на питання якості послуг зв'язку та систему їх управління як на один з найважливіших чинників ефективного розвитку конкуруючого ринку надання послуг зв'язку. Система управління якістю – це сукупність параметрів і механізмів, які забезпечують відповідність якості послуг встановленим вимогам. Метою введення такої системи є максимізація задоволення користувача наданою послугою для підвищення попиту на неї. В даному випадку йдеться про керування рівнем випромінюваної терміналами потужності для того, щоб збільшити ємність мережі, розширити зону радіопокриття, підвищити якість зв'язку і знизити енергоспоживання. Для досягнення перерахованих цілей механізми регулювання потужності, як правило, домагаються максимального збільшення рівня корисного сигналу при одночасному зниженні рівня радіоперешкод.

Однією з особливостей технологій LTE є те, що у вихідному каналі сигнали є ортогональними, а значить, взаємні радіоперешкоди між користувачами однієї соти відсутні – принаймні, за ідеальних умов радіозв'язку. Рівень перешкод, створюваний користувачам сусідніх сот, залежить від місця розташування випромінюючого мобільного терміналу, а точніше, від рівня загасання його сигналу на шляху до цих стільників. Загалом, чим ближче термінал до сусідньої соти, тим вище рівень створюваних ним перешкод в ній. Відповідно

термінали, що знаходяться на більш далекій відстані від сусідньої соти, можуть передавати сигнали більшої потужності, ніж термінали, розташовані поруч з нею.

Ортогональність сигналів у вихідному каналі LTE дозволяє мультиплексувати сигнали термінальних пристроїв різної потужності в цьому каналі в одній і тій же соті. Це означає, що замість компенсації сплесків рівня сигналу, що виникають внаслідок багатопроменевого поширення радіохвиль (шляхом зниження випромінюваної потужності), їх (сплески) можна використовувати для збільшення швидкості передачі даних за допомогою механізмів диспетчеризації та адаптації каналу зв'язку. Функція диспетчеризації залежно від стану каналу виділяє користувачам кращі ресурси. Багатоантенні технології зменшують завмирання сигналу, а механізми адаптації каналу задіють такі методи модуляції та кодування сигналу, які гарантують найкращу якість зв'язку в конкретних умовах. У вихідному каналі зв'язку механізм регулювання потужності дозволяє досягти високої якості сигналу і боротися з взаємними перешкодами.

В ході проведених досліджень було розроблено удосконалену систему регулювання випромінюваної потужності базових станцій мереж LTE. На відміну від існуючих методів регулювання потужності передавачів БС стільникових мереж зв'язку, удосконалений метод надає змогу підтримувати постійну швидкість передавання даних в стільниковій мережі, при цьому забезпечуючи допустиму імовірність бітової помилки та підтримуючи необхідне відношення сигнал/шум на приймальній стороні.

Це надає змогу отримувати користувачам стільникових мереж високу якість зв'язку, при цьому не збільшується негативний вплив електромагнітного випромінювання від БС. Крім того удосконалена система регулювання випромінюваної потужності надає можливість збільшити ємність мережі, розширити зону радіопокриття та знизити енергоспоживання.

УДК 621.391 (043.2)

Л.В. Беленчак
Національний авіаційний університет, м. Київ

НАДВИСОКОЧАСТОТНА ЛІНІЯ ЦИФРОВОГО ЗВ'ЯЗКУ (VDL) РЕЖИМУ 2

VHF Datalink (VDL) – це засіб передачі інформації між повітряними суднами і наземними станціями. В даний час, VDL-2 є основною версією VDL, і єдиним режимом, що підтримує Controller-Pilot Data Communications Link (CPDLC). Мережі VDL-2, мережі цифрового зв'язку високої швидкості і високої ємності забезпечують приблизно в 20 разів більшу ємність повідомлень, ніж зазвичай використовують сьогоднішні системи ACARS. Збільшені швидкість і ємність підтримують CPDLC, в якому визначені набори текстових інструкцій і повідомлень замінили звичайні обміни інформації. Ці набори інструкцій призначені для полегшення управління повітряним рухом при радіоперевантаженнях. В VDL-2 використовується модуляція D8PSK і метод управління множинним доступом з контролем несної (CSMA).

Цифровий канал передачі даних VDL-2 є одним з каналів мережі авіаційного електрозв'язку (ATN), що має в основі 7-рівневу модель взаємодії відкритих систем (OSI) ISO.

Канал VDL-2 виконує функції трьох нижчих рівнів моделі OSI.

Рівень 1 (фізичний) забезпечує управління частотою передачі, модуляцію і демодуляцію сигналу, а також функції сповіщення.

Рівень 2 (канальний) забезпечує надійну передачу пакетів даних і доступ до фізичного каналу, він розділяється на два підрівні і об'єкт управління. Підрівень управління доступом до середовища передачі (MAC) використовує метод множинного доступу з контролем несної (CSMA).

Рівень 3 (мережевий) забезпечує доступ до підмережі ATN і визначається ISO 8208. Цей протокол також відповідає за передачу пакетів в мережі, відновлення в випадку помилок, управління потоком даних, фрагментацію і зборку пакетів, а також управління зв'язками.

Основною рисою VDL-2 є значне підвищення пропускної здатності каналу і ефективності використання радіочастотного спектру. Ця перевага дозволила замінити існуючі системи або покращити їхню роботу завдяки використанню фізичного каналу VDL-2.

Для вирішення існуючих задач великий практичний інтерес складає розробка mesh-мережі. Здатність таких мереж ретранслювати повідомлення, використання різноманітних алгоритмів підтримки зв'язку і невеликий об'єм службових даних дозволить скласти мережу повного зв'язку (кожен з кожним), де кожен вузол може вести передачу даних з будь-яким ПС, використовуючи для цього інші вузли. Також це дозволить вирішити проблему втрати радіовидимості і зв'язку з диспетчером через особливості місцевості. Наприклад: здійснюється виліт літака з аеропорту, в цей же момент до аеропорту наближається інший літак для заходу на посадку. Припустимо, що через погану радіовидимість диспетчер не може зв'язатись з ПС, що заходить на посадку. За відсутності мережі це може призвести до зіткнення, якщо літак здійснює аварійну посадку. Якщо ж ми маємо повну мережу зв'язку, тоді диспетчер зможе одночасно помітити ПС і дати коректуючи команди для безпечного приземлення судна.

Для перевірки доцільності розробки mesh-надстройки для режиму VDL Mode 2 необхідно провести попередній аналіз структури. Для цього були проведені розрахунки необхідної дальності радіозв'язку і розрахунки ймовірності пропускної здатності мережі. Всі розрахунки враховують вплив умов середовища поширення радіосигналу.

Радіомережа є зв'язковою тоді, коли між будь-якою парою радіостанцій існує маршрут, котрий, в загальному випадку, може включати декілька ретрансляцій. Для оцінки зв'язковості використовуються наступні допущення:

– для зв'язності радіостанцій необхідна дальність радіозв'язку повинна бути не менше ніж R; система, яку аналізують пропонується як однорідна, тобто значення R для всіх радіостанцій однакове;

– територіальний розподіл радіостанцій є пуассонівським;

– при поширенні радіохвиль враховуються середні втрати поширення, повільні та швидкі завмирання;

– в якості антени використовується кругова антенна решітка.

Метою аналізу є оцінка такого значення дальності радіозв'язку R, яке за заданої густини радіостанцій системи передачі даних λ_S забезпечуватиме зв'язок радіостанцій з ймовірністю $P_{\text{CON}} \geq P_{\text{CON\_ТРЕБ}}$, де $P_{\text{CON\_ТРЕБ}}$ – необхідна ймовірність зв'язку радіостанцій.

Під зв'язком радіостанцій розуміють ситуацію, яка з визначеною вірогідністю P_{ISO} виключає наявність ізольованих радіостанцій в системі зв'язку. Ізольованою вважається така радіостанція, яка з визначе-

ною імовірністю P_{ISO} виявляється поза зоною радіопокриття інших радіостанцій. Зона радіопокриття визначається дальністю радіозв'язку R.

На графіках (рис. 1) представлена залежність дальності радіозв'язку від площі радіопокриття і кількості радіостанцій.

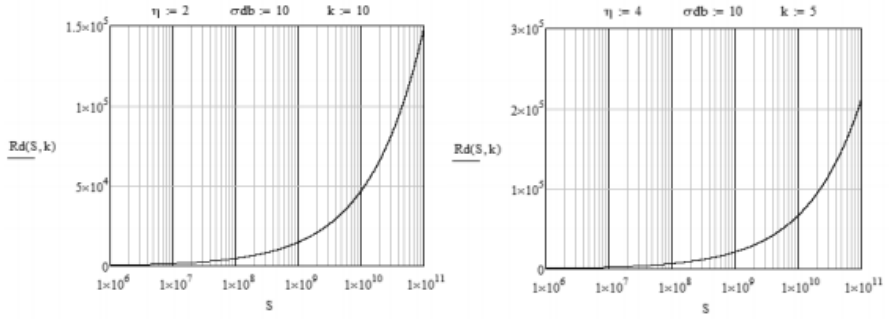

Рис. 1. Залежність дальності радіозв'язку від площі радіопокриття і кількості радіостанцій

Проаналізувавши графіки можна зробити висновок, що зі збільшенням показника середніх втрат поширення, необхідна дальність радіозв'язку R збільшується, а зі збільшенням числа вузлів мережі k, необхідна дальність зменшується.

Ще одна відмінна особливість ДВЧ лінії передачі даних режиму 2 полягає в тому, що існує можливість не тільки контроля повідомлень на рівні цілісності, але й прямого виправлення помилок. Дана перевага забезпечує кодування кадра даних кодом Ріда-Соломона, що дозволяє не усі пошкоджені повідомлення передавати повторно, і, в кінцевому рахунку, збільшує ефективність використання радіоканала.

Завдання оцінки пропускної здатності радіостанцій самоорганізованої радіомережі вирішується використанням методики оцінки пропускної здатності імовірнісним способом. Методика враховує апріорну невизначеність територіального розподілу радіостанцій, умови поширення радіохвиль і імовірність передачі радіостанції. Отримані співвідношення дозволяють в явному виді визначити пропускну здатність радіостанцій мережі при використанні ненаправлених антен.

На графіках (рис. 2) представлені залежності пропускної здатності від імовірності передачі радіостанції та від кількості сусідів радіостанції, для випадку ненаправлених антен.

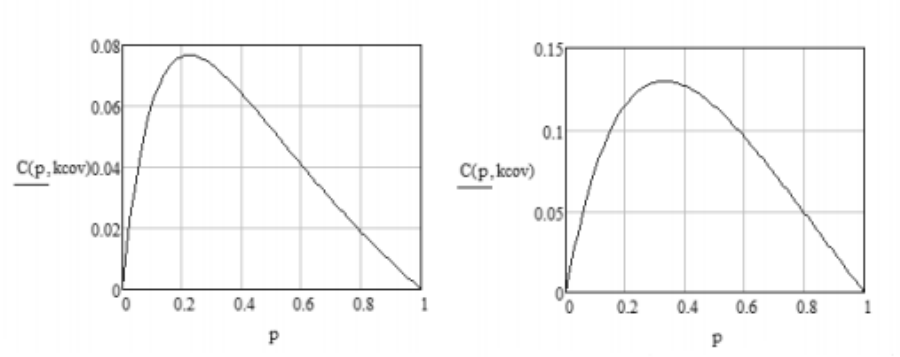

Рис. 2. Залежності пропускної здатності від імовірності передачі радіостанції та від кількості сусідів радіостанції

Аналіз графіків вказує на зменшення пропускної здатності при збільшенні сусідніх вузлів.

Представлена модель показує, що використання алгоритма самоорганізації дозволяє здійснювати видимість між всіма об'єктами мережі, а значить з використанням протоколів передачі даних здійснювати зв'язок між ними. Розрахунок зв'язку дозволяє дати оцінку стійкості взаємозв'язків між вузлами.

Отже, VDL-2 забезпечує сумісну з авіаційною телекомунікаційною мережею (ATN) лінію передачі даних «повітря-земля» і передбачає використання методів цифрового радіозв'язку. Номінальна швидкість передачі даних в 31,5 кбіт/с сумісна з характеристиками зв'язку при частотному розносі каналів в 25 кГц, що використовується при аналоговому надвисокочастотному зв'язку. VDL-2 дозволяє використовувати набори протоколів ATN для різноманітних експлуатаційних прикладних процесів, забезпечуючи, тим самим, значне підвищення ефективності використання високочастотного канала. Необхідно відмітити, що D8PSK (що використаний в VDL-2) був рекомендований ICAO, щоб уникнути амплітудних спотворень від різних схем модуляції в каналах «повітря-земля».

УДК 004.046 (043.2)

О.С. Паламарчук, Ю.В. Триус
Черкаський державний технологічний університет, м. Черкаси

ТИПОВА СТРУКТУРА ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЛЯ НЕБАНКІВСЬКИХ ФІНАНСОВИХ УСТАНОВ

Небанківські фінансові установи (НБФУ) є професійними учасниками ринку фінансових послуг, які, на відміну від банків, спеціалізуються на окремих фінансових послугах, забезпечуючи страхування, кредитування, спільне інвестування, управління активами, посередництво у купівлі-продажі фінансових інструментів, недержавне пенсійне забезпечення, гарантійні операції тощо. Основними відмінностями в діяльності НБФУ є: вузька спеціалізація; реалізація небанківських послуг (за наявності дозволу держави – окремих банківських послуг); відсутність безпосереднього впливу на формування пропозиції грошей на ринку; більший ризик порівняно з операціями банків [1].

Законом України «Про фінансові послуги та державне регулювання ринків фінансових послуг» визначено наступне: небанківські фінансові установи – юридична особа, яка відповідно до закону надає одну чи декілька фінансових послуг, а також інші послуги (операції), пов'язані з наданням фінансових послуг, у випадках, прямо визначених законом, та внесена до відповідного реєстру в установленому законом порядку. До НБФУ належать: *ломбарди*, *кредитні спілки* та *фінансово-кредитні установи* [1].

Наявність сучасних інформаційних систем (ІС) у НБФУ сприяє поширенню інформації про ці установи та їх послуги, що значно збільшує кількість потенційних клієнтів та партнерів. Одним із пріоритетних завдань будь-якої установи є розробка та інтеграція у її діяльність web-орієнтованих ІС, розвиток яких є одним із чинників, що впливають на діяльність НБФУ та на розвиток небанківського фінансового сектору в цілому.

Більшість ломбардів та кредитних спілок, які діють на ринку НБФУ України, мають свої web-ресурси. Проаналізувавши структуру та функціональне наповнення цих ресурсів, було виділено додаткові інформаційні, функціональні блоки та аналітичні модулі, що увійшли до web-орієнтованої ІС для НБФУ, яка розробляється в ЧДТУ.

Було розроблено типову структуру web-орієнтованої ІС для НБФУ, яка подана на рис. 1.

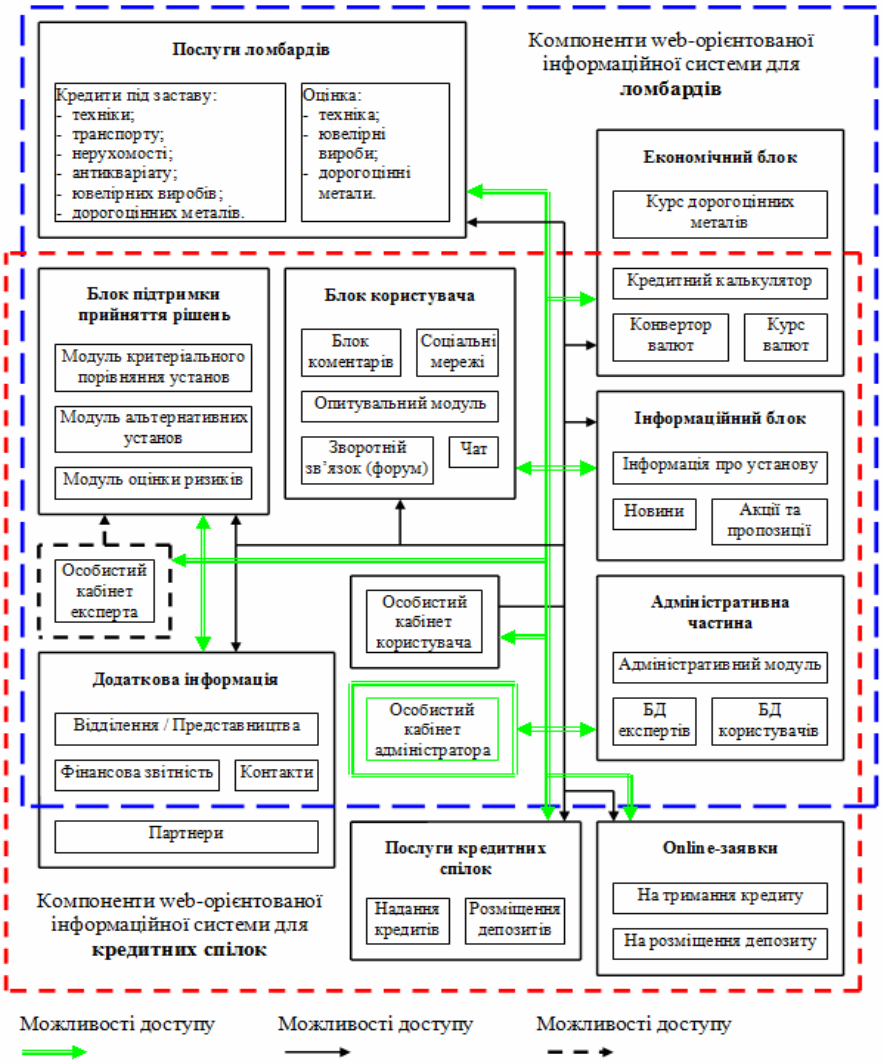

Рис. 1. Структура web-орієнтованої інформаційної системи для небанківських фінансових установ

Дана ІС розрахована на ломбарди та на кредитні спілки, оскільки вони мають практично однакову структуру за винятком деяких специфічних блоків та компонентів, притаманних тій чи іншій установі.

Ключовим елементом системи є *адміністративна частина*, яка складається з адміністративного модуля і баз даних користувачів системи та експертів, які можуть бути задіяні в аналітичних обрахунках та експертному оцінюванні діяльності НБФУ. Адміністратор системи має свій *особистий кабінет*, з якого він може керувати всіма компонентами ІС, розподіляти права та функції іншим користувачам. Розглянемо детальніше призначення кожного блоку і модуля цієї системи:

- *особистий кабінет користувача* – забезпечує доступ користувачів до модулів і блоків системи та можливості їх використання у відповідності з наданими правами та рівнями;
- *особистий кабінет експерта* – забезпечує доступ користувачів до модулів і блоків системи та можливості їх використання у відповідності з наданими правами та рівнями, зокрема *блоку підтримки прийняття рішень*;
- *блок підтримки прийняття рішень* (ППР) – складається з модуля критеріального порівняння НБФУ з БД, модуля для визначення альтернативних установ при прийнятті рішень, модуля оцінювання ризиків при проведенні бізнес-операцій НБФУ;
- *інформаційний блок* – призначений для внесення відомостей про установу, наповнення та оновлення новин, акційних пропозицій та бонусних програм (при їх наявності);
- *блок користувача* – призначений для слідкування за відгуками користувачів установи та системи, здійснення моніторингу відгуків та коментарів про установу в соціальних мережах, для спілкування з клієнтами та відповідей на питання, проведення опитування відвідувачів системи та користувачів (клієнтів) установи;
- *блок додаткової інформації* – призначений для внесення даних про нові відділення / представництва установ, їх контакти чи зміни існуючих даних (наприклад, адреси, телефону, e-mail тощо), додавання (завантаження) документів про фінансову звітність установи, про підсумки аудиторських перевірок, внесення даних про партнерів (кредитних спілок);
- *економічний блок* – призначений для налаштовування конвертора валют, кредитного калькулятора, приєднання модуля з курсами валют та дорогоцінних металів (для ломбардів), контролювання відповідності та правильності їх обрахування;

– *блок з послугами установи* – призначений для внесення відомостей про надання кредитів під заставу та здійснення оцінювання майна (для ломбардів); про надання кредитів та розміщення депозитів (для кредитних спілок);
– *блок для подання online-заявок* (для кредитних спілок) – призначений для прийняття заявки в електронному вигляді на отримання кредиту чи розміщення депозиту потенційного користувача (клієнта).

Користувач має визначені права та можливості доступу до кожного блоку системи. Деякі з них він може просто переглядати, а деякі – редагувати.

Адміністратор може призначати відповідальних осіб для керування деякими блоками (фахівців певної галузі).

Для створення web-орієнтованої ІС обрано такі програмні засоби:
– *Joomla!* – відкрита універсальна система керування вмістом (CMS) для створення web-орієнтованих систем;
– *Apache Denver* – програмна оболонка для створення та налагодження сайтів на локальному комп'ютері (локальний сервер);
– *PHP* – скриптова мова програмування для генерації HTML-сторінок на web-сервері;
– *MySQL* – система керування реляційними базами даних.

Отже, web-орієнтована ІС для НБФУ, що розробляється в ЧДТУ, призначена для надання повної, достовірної та доступної інформації про установу, проведення аналітичних обрахунків, для прийняття рішень як з боку НБФУ, так і з боку її клієнтів, здійснення бізнес-операцій та спілкування в реальному часі.

Список літератури

1. Паламарчук О.С. Розробка web-орієнтованої інформаційної системи для небанківських фінансових установ // Тези доповідей ІІ Міжнародної науково-практичної конференції «Інформаційні технології в науці, освіті і техніці» (ІТОНТ-2014): Черкаси, 24-26 квітня 2014 р. – У 2-х томах. – Черкаси: Черкаський державний технологічний університет, 2014. – Т 1. – С. 167-169.

УДК 004.732 (043.2)

І.В. Кохан
Національний авіаційний університет, м. Київ

МУЛЬТИСЕРВІСНА МЕРЕЖА ПІДПРИЄМСТВА

Сучасні потреби клієнтів у нових послугах є відправною точкою у визначенні стратегії розвитку мережевої інфраструктури. Попит на нові послуги – пакетної телефонії, передачі даних, відеоконференцзв'язку, голосової та універсальної пошти, теленавчання, VPN, а також додаткові інформаційні сервіси – розвивається у всьому світі стрімкими темпами. Мультисервісні мережі на підприємстві забезпечують можливість надання користувачам більш широкого спектра якісних послуг при ефективному використанні передавальних ресурсів мережі й універсальному способі обробки навантаження, що генеруються різними застосуваннями.

Усе більше організацій і підприємств приходять до висновку про необхідність створення мультисервісної мережі, що дозволяє використовувати увесь потенціал інформаційних технологій, значно підвищити їх ефективність і швидкість роботи. Такі зміни в структурі трафіку ускладнюють, а іноді і взагалі виключають, застосування аналітичного моделювання для створюваних алгоритмів і процесів. Альтернативним рішенням може служити імітаційне моделювання, яке дозволяє створювати моделі і умови роботи мережі найбільш наближені до реальності. Проблема проектування мультисервісних мереж є актуальною, внаслідок неможливості застосування старих підходів і відомих методик.

Задача проекту була в тому, щоб побудувати мультисервісну мережу підприємства використовуючи проводову і безпроводову мережу передачі даних. В даному завданні основною проблемою було підібрати комутаційне обладнання, яке б витримувало навантаження та функціонувало без жодних проблем і збоїв.

Проаналізувавши ринок інформаційних технологій вибір був зупинений на таких виробниках обладнання:

- для захисту мережі – WatchGuard;
- для комутаційної мережі – Hewlett-Packard;
- для бездротової мережі Ubiquiti UniFi та Linksys;
- для серверної частини також Hewlett-Packard.

Дані виробники є досить відомими і надійними компаніями, які вже давно стали світовими лідерами на ринку інформаційних технологій.

При побудові мережі було використано два інтернет канали, які ідуть через мережний захисний екран WatchGuard в два коммутатори Hewlett-Packard 1810-24 та Hewlett-Packard 2620-48 PoE+. Комутатор Hewlett-Packard 1810-24 повністю розрахований на серверну частину мережі. До нього було підключено шість серверів та одне мережне сховище даних. В свою чергу коммутатор Hewlett-Packard 2620-48 PoE+ використовується для комутації робочих станцій та оргтехніки.

В розрахунковій частині проекту були розраховані затримки та черги на Hewlett-Packard 2620-48 PoE+, розрахунок ймовірності збоїв та розрахунок надійності серверів. Також була побудована безпроводова мережа на обладнані Ubiquiti UniFi та Linksys. Програмно-апаратний комплекс Ubiquiti UniFi дозволяє побудувати безшовну Wi-Fi мережу, що складається з великої кількості безпроводових точок. Можливість підключити до одної майстер-точки, підключеної по кабелю, до 4-х точок по Wi-Fi. Завдяки цій можливості не довелося до кожної Wi-Fi точки підключати мережевий кабель. Було побудовано власну безпроводову мережу таким чином, щоб Wi-Fi мережа покривала повністю все приміщення.

З активним розвитком мультисервісних мереж стає важливим питання про їх кваліфіковану розробку. Адже від грамотного створення проекту мережі залежить ефективність її подальшого функціонування. У проекті в результаті проведеної роботи була спроектована мультисервісна мережу для офісу. Мережа було побудована двома способами: як проводовим так і безпроводовим, що повністю задовольнило всіх користувачів. Зробивши розрахунки черг і ймовірностей збоїв стає зрозумілим, що вибране обладнання повністю підходить для побудови офісів малого розміру.

УДК 621.396.1 (043.2)

Ю.І. Стецюра
Національний авіаційний університет, м. Київ

ОПТИМІЗАЦІЯ СТРУКТУРИ МЕРЕЖ 4 ПОКОЛІННЯ (LTE)

У зв’язку з розвитком технологій, а також з появою нових більш вдосконалених мобільних пристроїв, які надають користувачам біль-

ше можливостей, з'являється необхідність у наявності високошвидкісного бездротового інтернет з'єднання. Завдяки цьому з'являється попит на більш швидкісний зв'язок. Так, завдяки цьому сучасні оператори мобільного зв'язку починають впроваджувати у свої мережі нові технології, які здатні надати абонентам необхідну швидкість з'єднання і якість зв'язку. Однією з таких технологій є LTE. Це нове покоління мобільного зв'язку, яке характеризується більш високими швидкостями передачі даних. Такі мережі мають унікальну архітектуру, завдяки якій і досягаються істотно вищі показники не тільки швидкості, але і якості зв'язку.

Основною перевагою LTE є те, що вона будується на базі існуючого обладнання з порівняно легкою інтеграцією GSM і WCDMA, тому мережа LTE підтримує існуючі абонентські пристрої 2G і 3G. Цього позбавлені мережі WiMAX, які, так само як мережі LTE, відносяться до четвертого покоління.

Останні роки оператори мобільного зв'язку в усьому світі фіксують різке зростання обсягів переданих даних, яке багато в чому зумовлено популярністю смартфонів і планшетних комп'ютерів, що забезпечують зручний доступ до всіх нових додатків і сервісів мережі Інтернет. Аналіз ринку телекомунікацій показує, що трафік передачі даних в мобільних мережах з 2010 р. по 2014 р. зріс майже в 30 разів.

З впровадженням мереж 4 покоління спостерігається значне зростання швидкості та спектральної ефективності, проте він все рівно відстає від росту об'ємів трафіку. Таким чином, щоб підвищити ефективність та якість передачі даних необхідно підвищити просторову ефективність використання наявного частотного ресурсу. Іншими словами, збільшити щільність установки базових станцій, які будуть використовувати частоти.

Авторами було розроблено метод розвантаження мереж LTE за рахунок оптимізації структури, використання технології малих сот та переносу частини трафіку в мережу Wi-Fi на основі Hotspot 2.0.

У 2010 р. компанія Cisco сформувала Next Generation Hotspot Task Group. Мета полягала в тому, щоб об'єднати індустрію навколо загального комплексу стандарту Wi-Fi Alliance (WFA), який має назву Hotspot 2.0. На основі цієї сертифікації був розроблений метод, який допоможе забезпечити аутентифікацію та роумінг сумісності для операторів і постачальників обладнання. Він поєднує 3 основні блоки: стандарт IEEE 802.11u, Wi-Fi Protected Access 2 (WPA 2) і аутентифікацію на основі протоколу EAP (Extensible Authentication Protocol).

Таким чином, метод розвантаження способом інтеграції мережі LTE з мережею Wi-Fi на основі Hotspot 2.0 дає можливість збільшити ємність у густозаселених районах та місцях скупчення людей, розширити зону покриття LTE, а також дозволяє використати переваги кожної з технологій відповідно до потреб операторів та користувачів. В передачі обслуговування такого типу, одиночні потоки трафіку направляються через одну технологію доступу, в той час як інші потоки направляються через іншу.

УДК 004.822.514 (043.2)

О.І. Козлов
Національний авіаційний університет, м. Київ

СИСТЕМА ВІДДАЛЕНОГО КЕРУВАННЯ ТА ОПТИМІЗАЦІЇ КОНТЕНТУ ВЕБ-СТОРІНОК САЙТІВ

Останнє десятиліття стало періодом стрімкого розвитку Інтернет-технологій в Україні. Зараз неможливо уявити велику компанію, яка б не мала Web-представництва, або, хоча б, візитної картки у вигляді сайту в мережі Інтернет. Ріст і розвиток послуг Інтернет провайдерів, а також підвищення комп'ютерної освіченості несуть за собою необхідність Web-представництва, яке перетворилось з проекту «на імідж» в проект, передусім, успішної реклами, яка розрахована на вузькоспеціалізовану цільову аудиторію. А у випадку використання Web-ресурсу в якості Інтернет-магазину функціональне значення підвищується ще більше. У зв'язку з цим створення Web-представництва стає актуальною задачею.

На шляху розробників виникає ряд проблем. По-перше, проектування і розробка сайтів – довготривалі та трудомісткі. Для замовника часовий фактор може виявитись ключовим при виборі компанії розробників. Якщо компанія не виконує в терміни поставлене завдання, вона несе збитки, що ставить під загрозу перспективи її подальшого розвитку та існування. Ціна кінцевого продукту та його якість також мають не мале значення для замовника. По-друге, управління сайтом без допомоги зручної системи адміністрування для людини, що не знайома з HTML-розміткою – неможливе. Стандартні засоби розробки сайтів (основані на базі мови HTML) не дозволяють належним чином справлятися з поставленими завданнями. Виходом з цієї ситуації є використання систем управління контентом (CMS – Content Management

System). Система управління контентом – це програмне забезпечення та інструкції по його використанню в цілях створення та редагування вмісту і структури сайту.

Основна мета використання системи управління контентом – дозволити будь-якій людині, яка не розбирається у тонкощах програмування, вносити зміни на Web-ресурсі, знизити вартість розробки і подальшої підтримки сайтів, скоротити сроки проектування, розробки та впровадження сайтів, підвищити якість роботи сайтів, а також значно підвищити швидкість оновлення інформації. Проте в використанні CMS також є свої недоліки: для невеликих проектів використання складних систем може бути не виправданим, оскільки великий функціонал може виявитися зайвим, але при цьому буде створювати додаткове навантаження на сервер. Також проблемою багатьох CMS є безпека даних, оскільки якщо знайти недолік в системі, то можна отримати доступ до будь-якого сайту, розробленому на цій CMS.

В процесі проектування і розробки системи були вирішені всі поставлені задачі. Проведена класифікація існуючих сайтів і систем управління контентом. Вивчено методи і механізми проектування і розробки систем управління контентом. На основі отриманих знань було вибрано метод проектування та засоби розробки системи.

Система дала можливість позбавитися від рутинної роботи, якою займались менеджери по контенту. Зникла необхідність у «ручному» перетворенні інформації на зрозумілу браузерам мову гіпертекстової розмітки (HTML). Використання системи скоротило часові та матеріальні витрати на розробку проектів. Зросла ефективність взаємодії користувачів мережі Інтернет та WEB-додатків, розроблених на даній системі. Також були проведенні роботи з оптимізації сайту, для кращої індексації в пошукових системах. Що надалі приведе більше відвідувачів на ресурс.

На даний момент в Україні не так багато гарних компаній надають якісні послуги з розробки сайтів і їх просування у пошукових системах. Більшість «фахівців» розробляють неякісні сайти та використовують заборонені способи просування, для того щоб ресурс якомога швидше потрапив у топові позиції пошукових систем, вводячи в оману замовника. Через деякий час такі сайти потрапляють під фільтри пошуковиків та випадають з індексу на тривалий період. У зв’язку з цим власник ресурсу втрачає відвідувачів, а, відповідно, і кошти.

УДК 621.39 (043.2)

І.В. Семенюк
Національний авіаційний університет, м. Київ

ВПРОВАДЖЕННЯ МЕРЕЖІ МОБІЛЬНОГО ЗВ'ЯЗКУ ЧЕТВЕРТОГО ПОКОЛІННЯ СТАНДАРТУ LTE В УКРАЇНІ

Розвиток мобільного зв'язку, нові покоління та стандарти дають користувачеві все більше можливостей. Ще кілька років тому ми мали змогу користуватися мобільними терміналами стандарту GSM, які були обмежені мовним каналом і передачею коротких повідомлень. Пізніше на базі GSM розроблено GPRS та EDGE для доступу в інтернет на малій швидкості. На сьогоднішній день в Україні користувачам доступний швидкісний мобільний інтернет за технологіями третього та четвертого покоління EV-DO CDMA та WiMAX. Виникає потреба в розгортанні високошвидкісної мережі мобільного зв'язку, так як число користувачів мобільним інтернетом постійно зростає.

Стандарт LTE (Long Term Evolution) дає змогу знизити вартість передачі даних, збільшити швидкість більше 100 Мбіт/с, збільшити спектр послуг та гнучкість мережі з використанням існуючих систем мобільного зв'язку, дозволяє транслювати потокове відео високої роздільної здатності за стандартом DVB-H.

Щодо використання радіоресурсу, LTE працює в діапазоні частот від 700 МГц до 2700 МГц, які в свою чергу поділені на 40 діапазонів. Розділення каналів – дуплексне часове (TDD) або частотне (FDD). Радіус покриття базової станції до 30 км. Ємність обслуговуваних абонентів базової станції більше 200 користувачів при смузі 5 МГц. Затримка пакетів даних не перевищує 30 мс. Стандарт підтримує типи модуляції: 64QAM, QPSK, 16QAM.

В архітектурі стандарту мережева взаємодія відбувається між базовою станцією (eNB) і блоком керування мобільністю (MME), який включає в себе мережевий шлюз GW.

Сама мережа LTE складається з мережі радіодоступа E-UTRAN і базової мережі SAE.

E-UTRAN Складається з базових станцій eNB. Кожна базова станція має інтерфейс S1 з базовою мережею SAE.

Функції базових станцій: керування радіоресурсами, шифрування даних, маршрутизація пакетів до обслуговуючого шлюзу.

Базова мережа SAE ще так звана EPC (Evolved Packet Core) скла-

дається з логічних елементів MME та UPE. MME керує мобільністю абонентського пристрою та керує базовими станціями з допомогоу протоколів C-plane.

Базова мережа SAE має стик з протоколом IP, тому обмін пакетами між абонентами на відстані відбувається виходом в транспортну мережу. Також доступ до базової мережі може здійснюватися через мережі мобільного зв'язку другого і третього покоління, також мережі Wi-Fi, WiMAX та дротові IP технології.

В Україні в основному розвинена 2G мережа, зв'язок третього покоління має достатнє покриття в більшості населених пунктів.

Технологія LTE являється високошвидкісною, багатофункціональною, гнучкою в взаємодії з іншими технологіями. Тому доцільно розвивати і в подальшому оптимізувати мережі четвертого покоління в Україні.

Для розгорнення мережі не потрібно будувати абсолютно нову базову станцію. Так як у кожного мобільного оператора України стандарту GSM покриття становить більше 80% , зацікавлений в розвитку LTE оператор GSM стандарту може модернізувати свої базові станції.

На разі економічно вигіднішим є рішення SingleRAN від Huawei. SingleRAN (єдина мережа радіодоступа) – мінімізована базова станція, яка об'єднала в собі кілька стандартів мобільного зв'язку. Компанія Huawei розробила SingleRAN на 3 стандарта – GSM, UMTS, LTE, це зручно для проектування мереж і плавного переходу на четверте покоління. Компактні рішення не займають великого простору на базових станціях, споживають менше електроенергії.

Використовують антени панельного типу з кросс-поляризацією сигналу. Для стандартів GSM та 3G також використовують такі антени, відмінність від LTE в тому, що в GSM та 3G працюють дві поляризації на прийом і одна на передачу. Пілот (антена) стандарту LTE також може працювати в такому режимі, але технологія MIMO реалізує прийом-передачу з задіяними двома або чотирма поляризаціями сигналу одночасно.

В даний момент в Україні існують складнощі з ліцензуванням і виділенням робочого діапазону для роботи LTE. Радіоресурс занадто стислий, і всі представлені діапазони вже зайняті. На прикладі:

– 790–862 МГц – повітряна радіонавігація, CDMA 800;
– 880–915 МГц / 925–960 МГц – GSM-900;
– 1710–1785 МГц / 1805–1880 МГц – GSM-1800;

– 2400 МГц – WiMAX;
– 2690 МГц – WiMAX.

Нижній діапазон має переваги в покритті і в кращому проходженню сигналу, верхній має перевагу в ширині каналу, а отже більша ємність обслуговуваних абонентів.

Для вирішення питань щодо забезпечення робочих частот для LTE необхідно виконати ряд реформ, які передбачають звільнення необхідних частот, ліцензування, розрахунок необхідного максимально-ефективного робочого діапазону.

Доцільно в етапі розвитку використовувати робочій діапазон 2500–2690 МГц, потім при достатньому розвитку переходити на частоти GSM стандарту в випадку успішного розвитку, таким чином замінити застаріле покоління 2G на нове покоління мобільного зв'язку 4G.

Список літератури

1. Тихвинский В.О., Терентьев С.В. Сети мобильной святи LTE. Технологии и архитектура. – Москва, Эко-Трендз, 2010 г. – 248 с.

2. Гельгор А.Р., Попов Е.А. Технология LTE мобильной передачи данных. – Санкт-Петербург, 2011 г. – 150 с.

3. Приходько А.С. Проблемы частотного радиопокрытия и частотной совместимости при использовании технологи LTE на существующих сетях GSM.

4. Тихвинский В.О. Технологические принципы глобальной совместимости сетей LTE с мобильными сетями других стандартов. – Москва, 2010 г.

УДК 621.396.4 (043.2)

Д.І. Бахтіяров
Національний авіаційний університет, м. Київ

КРИПТОГРАФІЧНИЙ ЗАХИСТ СИГНАЛУ КЕРУВАННЯ БЕЗПІЛОТНИМ ЛІТАЛЬНИМ АПАРАТОМ

Тема дослідження відноситься безпосередньо до каналу зв'язку системи управління місцем розташування і курсом безпілотного літального апарату (БПЛА) і може бути використаною при проектуванні БПЛА. Після проведеного аналізу систем захисту каналів управляння БПЛА було встановлено, що вони мають низку недоліків. Тому метою дослідження є аналіз технічного завдання по створенню криптографічного захисту сигналу керування БПЛА.

Система криптографічного захисту передбачає виконання наступних функцій:

– криптографічне перетворення інформації має відповідати ГОСТ 28147-89;

– генерацію та формування випадкової послідовності;

– неможливість зчитування змісту ключових даних зовнішнім програмним забезпеченням;

– вирівнювання статистичних характеристик, побудованих на базі рекурентної лінії зворотного зв'язку з поліномом та реалізованого програмно у спеціальному програмному забезпеченні модулів управління пунктом керування та БПЛА.

Також система захисту повинна працювати в наступних режимах:

– самоконтроль;

– контроль;

– шифрування;

– адміністрування.

Пристрій повинен відповідати спеціальним вимогам із захисту інформації від витоку каналами ПЕМВН, а саме:

– забезпечувати можливість його використання у складі комплексів криптографічного захисту конфіденційної інформації та не погіршувати їх спеціальних якостей;

– модулі повинні бути виконані як автономні пристрої в металевому корпусі, у якому повинні розміщуватись апаратні компоненти.

Програмне забезпечення керування каналом управління повинно відповідати наступним вимогам:

– інтерфейс користувача повинен бути виконаний у графічному (віконному) вигляді;

– інтерфейс програмного забезпечення повинен бути виконаний українською, російською та англійською мовами;

– усі процедури, тривалість виконання яких перевищує 3 секунди, повинні супроводжуватися відображенням оператору відповідного повідомлення;

– порядок дій оператора при виконанні усіх критичних операцій, які пов'язані із знищенням інформації або зміною паролів доступу до модулів, повинен забезпечувати виконання таких операції лише за умов їх обов'язкового підтвердження;

– пароль доступу до облікового запису оператора повинен містити 8 символів; символами паролю можуть бути будь-які символи латинського, російського або українського алфавіту, а також десяткові цифри;

– драйвер обладнання та програмне забезпечення каналу управління повинні відповідати усім вимогам сумісності з операційною системою Windows XP/7/8.1.

Таким чином, проведений аналіз технічного завдання по створенню системи криптографічного захисту сигналів керування безпілотними літальними апаратами показав те, що дане технічне завдання є необхідним і достатнім для створення системи криптографічного захисту каналу керування БПЛА на базі ГОСТ 28147-89.

УДК 004.056.53 (043.2)

В.В. Рассказчікова
Національний авіаційний університет, м. Київ

КОМПЛЕКСНІ ЗАХОДИ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ПРОВЕДЕННІ КОНФЕРЕНЦІЇ

В час швидкого розвитку інформаційних технологій, комерційні, державні, військові та інші установи зіштовхуються з серйозною проблемою – несанкціонованим вилученням, прослуховуванням та знищенням важливої інформації.

Метою несанкціонованого збору інформації в даний час є, перш за все комерційний інтерес. Як правило, інформація різнохарактерна і ступінь її конфіденційності залежить від особи чи групи осіб, кому вона належить, а також сфери їх діяльності. Викрадення конфіденційної інформації може здійснюватися простим підключенням до телефонних і комп'ютерних мереж, перехопленням радіоповідомлень, входом в персональний комп'ютер, установкою радіомікрофонів, використанням лазерної техніки для зчитування коливань помилок, зчитування і розшифровки випромінювання комп'ютерів та іншої техніки. Широко використовуються диктофони з акустоматом – приладом , що автоматично вмикає магнітофон при виникненні звуку голосу. Також використовуються мікрофони далекої дії.

Метою проекту є створення системи інженерно-технічного захисту залу для переговорів комерційного підприємства.

Головним завданням проекту є:

• аналіз існуючої системи інженерно-технічного захисту залу для переговорів комерційного підприємства;

• проектування системи інженерно-технічного захисту залу для переговорів комерційного підприємства.

У першу чергу необхідно визначити канали витоку інформації і засоби їх контролю, а, при необхідності, і перекриття. Найважливішим інструментом у цьому є аудит інформаційної безпеки. Аудит дозволить виявити канали витоку, оцінити їх критичність і ймовірність витоку по них. Аналіз даних, зібраних під час аудиту, дасть можливість вибору засобів контролю каналів, виходячи з бізнес-моделі підприємства і типів каналів. Однак існують контрзаходи проти кожного засобу розкрадання інформації – шифратори, засоби виявлення підслуховуючого обладнання та створення йому перешкод, засоби блокування небажаних випромінювань. Однак такі пристрої доступні за коштами лише великим фірмам або агентствам промислового шпигунства. Але забувати про них не слід. Особливого захисту потребують комп'ютерні засоби, що містять практично всю інформацію сучасного підприємства. Справжньою загрозою власників комп'ютерів стали комп'ютерні віруси.

За результатами роботи запропоновано комплекс організаційно-технічних заходів щодо запобігання витоку інформації, а саме, комплекс заходів: щодо запобігання перехоплення радіо і електричних сигналів, щодо запобігання проникнення зловмисника, по захисту мовної інформації від підслуховування і перелік програмно-апаратних засобів.

Розроблено варіант системи захисту інформації на розглянутому об'єкті інформатизації.

УДК 004.056.5 (043.2)

А.О. Бусел
Національний авіаційний університет, м. Київ

МОДЕЛЬ ОЦІНКИ ЦІННОСТІ ОТРИМАНОЇ ІНФОРМАЦІЇ У СИСТЕМІ КОНКУРЕНТНОЇ РОЗВІДКИ

З кожним днем спостерігається значне підвищенням важливості інформації в усіх сферах людського життя. Дослідження та аналіз економічних процесів на засадах інформаційного підходу дозволяє значно оптимізувати і покращувати розвиток бізнесу. В умовах сучасного зовнішнього середовища одним із способів якісного підвищення конкурентоспроможності підприємства є раціональне управління інформаційними ресурсами. У сучасних бізнес-процесах інформація трактується як один із найважливіших ресурсів, ефективне викорис-

тання якого сприяє досягненню цілей та вирішення задач підприємства. Стрімкий розвиток бізнесу у наш час сприяє активному розвитку конкурентної розвідки, яка займається процесами збору, нагромадження, структурування та аналізу інформації про внутрішнє та зовнішнє середовища компаній-конкурентів.

Успіх конкурентної розвідки залежить основним чином від властивостей здобутої інформації, – її достовірності, повноти, актуальності, адекватності, релевантності, об'єктивності чи суб'єктивності тощо. Сукупність цих та інших факторів показує на скільки здобута інформація може бути цінною для замовника. І, зрозуміло, що чим цінніша інформація, тим ефективнішим буде її використання для підприємства. Тому визначення цінності інформації, здобутої у процесі конкурентної розвідки є завданням актуальним.

Конкурентна розвідка є необхідним процесом для нормального розвитку бізнесу. У зв'язку з цим оцінка цінності інформації, здобутої у її процесі являється безумовно необхідним фактором. І чим швидше та якісніше дана оцінка буде здійснюватися, тим більша вірогідність підвищення ефективності процесу конкурентної розвідки і, як наслідок, можливе швидше та оптимальніше реагування на певні зміни у бізнесі, підвищення конкурентоспроможності підприємства.

Створена модель оцінки визначає цінність інформації на основі сукупності результатів послідовного аналізу таких критеріїв, як релевантність, після чого питання стоїть у доступності, і далі – актуальність. При необхідності також додаються результати аналізу на об'єктивність/суб'єктивність, повнота/неповнота, зрозумілість/незрозумілість тощо.

Модель оцінки цінності отриманої інформації дозволяє здійснювати структурування, аналіз, визначення ефективності, тощо для здобутої інформації у процесі конкурентної розвідки. Новизною є вперше запропонована модель оцінки інформації за критерієм цінності, який базується на аналізі таких нечітких критеріїв, як достовірність, актуальність тощо. Модель оцінки цінності інформації дає можливість спростити та удосконалити процеси структурування, систематизації та аналізу отриманої інформації, визначати її цінність у грошовому та іншому еквівалентах, також дозволяє спрогнозувати ефективність/неефективність її використання для розвитку підприємства.

УДК 654.01 (043.2)

А.В. Мокроусов
Національний авіаційний університет, м. Київ

МОДЕЛЮВАННЯ ПОБУДОВИ КОНТАКТ-ЦЕНТРУ НА БАЗІ АПАРАТНИХ ТА ПРОГРАМНИХ ЗАСОБІВ AVAYA

Технічний розвиток контакт-центрів та етапів розвитку організаційних форм телефонного обслуговування наведений у табл. 1.

Таблиця 1

Етапи розвитку організаційних форм телефонного обслуговування

	Телефонні комутатори (50-ті рр. XX ст.)	Центри телефонного зв'язку (90-ті рр. XX ст.)	Комунікаційні центри (після 2000 р.)
Контакт з клієнтом	Передача телефонних звернень по інстанціям	Телефонний діалог з клієнтом	Багатомедійна комунікація з клієнтом
Організаційна форма	Працює паралельно з основним відділом	Працює в комбінації з основним відділом або самостійно	Окремий комунікаційний центр
Цілі	Обслуговування за допомогою телефонних контактів	Створення лояльної клієнтури, завоювання нових клієнтів	Орієнтування на партнерство, створення лояльних партнерів
Якість обслуговування	Низька	Середні та високі рівні обслуговування	Виключно високий рівень обслуговування
Задачі	Передача по інстанціям інформації та довідок	Термінові інформаційні лінії, довідки про договори, управління рекламаціями, терміновий та допоміжний сервіс	Термінові інформаційні лінії, підписання договорів, управління рекламаціями, урегулювання проблем матеріального збитку

Було поставлено за мету організувати центр обслуговування викликів (ЦОВ) на дві локації з навантаженням в 1000 агентів з використанням надійного обладнання для забезпечення обробки 1500 одночасних викликів. Опираючись на власний досвід та рецензії багатьох великих компаній, вибір було зупинено на обладнанні від Avaya, адже саме для створення сучасного Call-центру, використовують рішення світових лідерів: рішення Avaya Communications та системи запису Nice Systems.

Виходячи з дослідження ринку та пропозицій різних вендорів телекомунікаційних рішень вирішено використовувати наступне ПЗ та обладнання:

- IP-PBX AVAYA Communication Manager на базі серверів S8700 та шлюзів G650;
- Avaya Call Management System;
- система запису Nice Perform;
- Avaya Interactive Response (AIR);
- Avaya Interaction Center (AIC).

Найпростіша з можливих схем організації телефонного зв'язку на основі Avaya Communication Manager виглядає таким чином (зображена на рис. 1):

- Avaya Interactive Response (AIR) – надає можливість відповіді звукової інформації, тобто – IVR;
- System Access Terminal (SAT) – дозволяє здійснювати віддалене підключення та управління;
- Basic Call Management System (BCMS) – збирає та надає інформацію про продуктивність ЦОВ;
- ASAI – дозволяє інтеграцію між комп'ютерами та системою, що працює на СМ;
- Call Detail Recording (CDR) – збирає, зберігає, фільтрує та надає записи всіх дзвінків, які були прийняті системою;
- Call Accounting System (CAS) - використання запису викликів для створення білінгової звітності для визначення задоволеності абонента;
- Call Management System (CMS) – збирає інформацію та генерує звіти по телемаркетингу ЦОВ;
- AUDIX workstation – дозволяє адмініструвати голосову пошту.

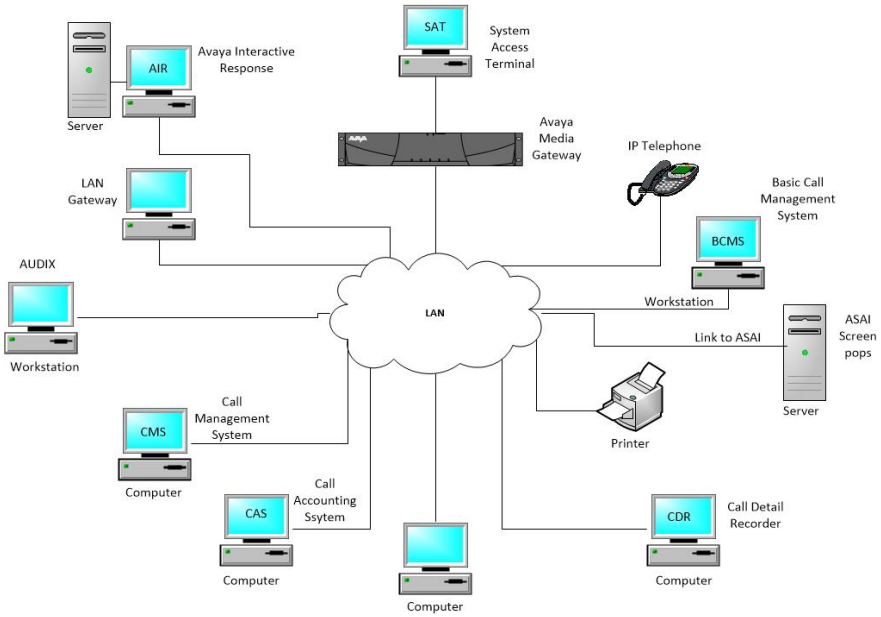

Рис. 1. Схема організації телефонного зв'язку на основі Avaya Communication Manager

Переваги та недоліки такої інфраструктури.

Переваги:

- простота інфраструктури;
- низька вартість побудови;
- легкість адміністрування.

Недоліки:

- відсутність системи резервування;
- непрацездатність системи при виході з ладу будь-якої апаратної частини VoIP-обладнання.

Враховуючи вище вказані недоліки можливо покращити схему організації зв'язку шляхом введення механізмів резервування. В такому разі кожен сайт має доступ до мережі PSTN (Public Switched Telephone Network) за допомогою технології TDM (Time Division Multiplexing). Активним та головним при такій моделі є сервер S8700, що працює в активному режимі в головному офісі. У іншому офісі медіасервер S8700 працює у режимах Stand-by. А сервери CMS збирають

інформацію відразу зі всіх локацій/офісів. Та всі ці офіси об'єднані між собою мережею WAN.

Ще покращити дану схему можна розглянувши варіант цієї ж інфраструктури, але при умові недоступності мережі WAN та автономності кожної з локацій.

З економічної точки зору вартість даного проекту становить близько 3 млн. доларів США.

В порівнянні з більш примітивною інфраструктурою, така побудова мережі буде складнішою в своєму обслуговуванні та дорожчою по вартості. Проте саме завдяки використанню такої технології побудови інфраструктури отримуємо відмовостійку систему, яка не дозволить понести збитки через форс-мажорні обставини.

УДК 621.396.42 (043.2)

М.С. Высочиненко
ГУ «Киевский колледж связи», г. Киев

СТАТИСТИЧЕСКИЕ ХАРАКТЕРИСТИКИ ПРОЦЕССА ЗАПРОСОВ К СТАНЦИЯМ БЕСПРОВОДНОЙ СЕТИ НА ОСНОВЕ МЕТОДОВ ПОЛЛИНГА

Беспроводные сети предназначены для обмена большими объемами данных между пользователями. Однако с ростом числа пользователей, а, следовательно, объемов данных возникает проблема оптимизации скорости обработки запросов и выдачи запрашиваемых данных. Наиболее перспективный путь решения этой задачи – применение статистических методов, в частности, методов теории массового обслуживания.

Для оценки эффективности функционирования сетей хранения данных как систем массового обслуживания предлагается применять стохастические модели поллинга или упорядоченного опроса [1, 2]. Порядок опроса очередей определяется правилом выбора сервером следующей очереди. Наиболее распространенные виды порядка опроса [2, 3]:

– циклический – установлена последовательность прохода очередей;

– периодический – опрос осуществляется на основе таблицы поллинга;

– случайный;
– приоритетный.

В работе [5] отмечается, что с практической точки зрения значительный интерес представляют системы с адаптивным механизмом поллинга, в которых при опросе очередей учитывается состояние очереди, то есть если очередь была пуста в данном цикле опроса, то на следующем цикле опроса эта очередь будет пропущена. Однако такой подход можно применять только в системах поллинга, в которых поток заявок представляет собой стационарный эргодический процесс [3, 4]. Следовательно, необходимо учитывать нестационарности текущей величины конкретной очереди. Поэтому на практике целесообразно применять механизм поллинга с обратной связью и адаптацией не только к текущему размеру очереди, но и к скорости роста (убывания) очереди.

Модель системы поллинга для сети хранения описывается следующим образом.

Система имеет один обслуживающий прибор и N ($N \geq 2$) очередей. Каждый из N буферов имеет ограниченный объем памяти в L ячеек. Заявки поступают в общем нестационарном входном потоке. В i-ю очередь поступает нестационарный поток заявок с функцией распределения $f_i(t)$ и мгновенной интенсивностью $\lambda_i(t)$. Максимальное число заявок на интервале наблюдения T_S равно M_i, причем $L > M_i$, $i = \overline{1, N}$. При опросе i-го элемента сети хранения обслуживается $f_i(n) \leq M_i$ заявок. Считаем, что времена обслуживания τ_{si} заявок в очереди независимы и одинаково распределены с функцией распределения $w_i(t)$, которая является непрерывной и дифференцируемой, с математическим ожиданием $m_i = \int_0^\infty t dw_i(t)$ и вторым начальным моментом $\sigma_i^2 = \int_0^\infty t^2 dw_i(t)$. Интеграл понимается в смысле Стилтьеса. Предполагается, что потоки заявок и длительности обслуживания заявок представляют собой взаимно независимые процессы.

Сервер посещает очереди, следуя выбранному порядку опроса и обслуживая их в соответствии с выбранной дисциплиной. Время под-

ключения к очереди τ_{qi} – случайная величина с плотностью распределения $v_{qi}(t)$, математическим ожиданием m_{qi} и вторым начальным моментом σ_{qi}^2.

По результатам имитационного моделирования процессов опроса установлено, что выбор наиболее приемлемого порядка опроса зависит как от объема запрашиваемого пакета данных, так и от распределения данных по отдельным элементам хранилища данных.

Список литературы

1. Вишневский В.М. Системы поллинга: теория и применение в широкополосных беспроводных сетях / В.М. Вишневский, О.В. Семенова. – М.: Техносфера, 2007. – 312 с.

2. Высочиненко М.С., Халимон Н.Ф. Управление запросами к станциям беспроводной сети. – Восьма міжнародна науково-технічна конференція і шоста студентська науково-технічна конференція «Проблеми телекомунікацій» – НТУУ «Київський політехнічний інститут», Інститут телекомунікаційних систем, 22–25 квітня 2014 року.

3. Borovkov A., Schassberger R. Ergodicity of a polling network // Stoch. Proc. Appl., 1994. – v. 50. – pp. 253–262.

4. Фосс С.Г., Чернова Н.И. Теоремы сравнения и эргодические свойства систем поллинга // Проблемы передачи информации, т. 32, вып. 4, 1996. – С. 46–71.

5. Синюгина Ю.В. О времени ожидания в системе с ограниченным шлюзовым обслуживанием и адаптивными отдыхами // Проблемы физики, математики и техники, № 4 (13), 2012. – С. 61–65.

УДК 621.391 (043.2)

Ж.О. Шевчук, А.Ю. Спірідонов, І.О. Мачалін
Національний авіаційний університет, м. Київ

БЕЗПЕКА МЕРЕЖ НАСТУПНОГО ПОКОЛІННЯ NGN

Одним з важливих відкритих питань щодо NGN на сьогодні є підвищений ризик, пов’язаний з переведенням всієї телекомунікаційної індустрії на такий достатньо уразливий протокол, як IP. При цьому значні ризики можуть бути не тільки у операторів зв’язку, а й у всіх інших користувачів. Саме тому слід приділяти найбільше уваги саме безпеці NGN. Таким чином, в NGN для забезпечення безпеки застосовуються протоколи IPSec, TLS, SSL.

SSL (Secure Sockets Layer) протокол забезпечує конфіденційність обміну даними між клієнтом і сервером, причому для шифрування використовується асиметричний алгоритм з відкритим ключем. Коли помилка виявлена, той, хто її виявив, посилає про це повідомлення своєму партнерові. Непереборні помилки вимагають від сервера і клієнта розриву з'єднання. TLS (Transport Layer Security) надає можливості автентифікації і безпечної передачі даних через Інтернет з використанням криптографічних засобів. Часто відбувається лише автентифікація сервера, а клієнт залишається неавтентифікованим. Для взаємної автентифікації кожна з сторін мусить підтримувати інфраструктуру відкритого ключа (PKI), яка дозволяє захистити клієнт-серверні додатки від перехоплення, редагування повідомлень або ж створення підроблених. Основна проблема SSL/TLS – зниження продуктивності. Ця процедура потребує значних витрат процесорного часу на виконання складних криптографічних операцій з довгими ключами. Однак після встановлення з'єднання витрати на шифрування скорочуються.

Протокол IPsec, на відміну від протоколів SSL та TLS, може використовуватися для захисту будь-яких протоколів, що базуються на TCP та UDP. IPsec може використовуватися для забезпечення безпеки між двома IP-вузлами, між двома шлюзами безпеки або між IP-вузлом і шлюзом безпеки. Протокол є «надбудовою» над IP-протоколом, і може забезпечувати цілісність та/або конфіденційність даних переданих по мережі. Можливе також для IP-телефонії застосування підключення віддалених користувачів через віртуальні приватні мережі (VPN). Зміст перехоплених пакетів, що відправлені по шифрованим VPN тунелям зрозумілий тільки для власника ключа шифрування.

Безумовною перевагою таких засобів захисту є мобільність користувача, та абсолютну гарантію безпеки, нажаль, не зможе забезпечити ні один комплекс засобів. На практиці слід розглядати всю інфраструктуру мережі, проводити глибокий аналіз належного і раціонального рівня захисту. Необхідно враховувати не тільки необхідність забезпечення безпеки внутрішніх переговорів, але і виходи на всі зовнішні канали зв'язку (мобільний зв'язок, телефонні мережі загального користування).

ЗМІСТ

Кот А.С., Миночкин Д.А.
Адаптивный алгоритм передачи обслуживания на основе оценки подвижности терминалов в сотовых системах связи..... 3

Миночкин Д.А., Кушниренко И.А.
Моделирование спутниковых MIMO каналов..... 7

Булах М.Г.
Модифицированный алгоритм мультипликативного инвертирования в двоичном поле..... 11

Голубничий О.Г., Конахович Г.Ф.
Аналіз нормативних рекомендацій щодо захисту наскрізного зв'язку «повітря–земля» у мережі ATN..... 13

Афанасьєв А.М.
Аналіз впровадження мереж стандарту LTE в світі..... 17

Соколовский С.В.
Эффективная идентификация абонентов с использованием булевых функций..... 20

Малік Т.Я.
Проектування мультисервісної мережі підприємства за допомогою САПР..... 22

Дубров О.В.
Підвищення ефективності впровадження мережі мобільного зв'язку 4G..... 24

Андрощук О.В.
Механізми реалізації послуг захисту інформації при передачі даних..... 25

Марченко О.В.
Аналіз концепції архітектури систем Cloud Monitoring..... 27

Вікулов П.О., Павлов В.Г.
Захист користувачів хмарних технологій..... 29

Шрамко М.О., Ткаліч О.П.
Безпроводова мережа для доступу до баз даних..... 31

Негрішний О.Ю.
Методи побудови захищених каналів керування повітряним рухом..... 32

Пластун Д.Г.
Порівняльний аналіз схем адміністрування мережею WCDMA..... 34

Димерлій А.О.
Розробка та проектування мережі LTE для Чернігівської області..... 35

Савченко А.В.
Проектування мережі Long Term Evolution в Київській області..... 36

Харечко І.С.
Методика побудови моделі загроз інформації..... 38

Половий О.М.
Алгоритм параметричної ідентифікації баз нечітких знань..... 40

Шеремет Є.Ю.
Дослідження сервісної частини IP-телефонії
на базі технології Asterisk..... 42

Ковалевський Д.В.
Оптимізація захищеного каналу управління повітряним рухом..... 43

Грицюк Л.Л.
Офісна віртуальна АТС..... 44

Рибальченко Є.В.
Підвищення продуктивності вузлового обладнання
шляхом використання механізмів прогнозування потоків трафіку..... 46

Агеєнко С.В.
Проектування мережі захищеного телефонного зв'язку..... 50

Терентьєва І.Є.
Аналіз надійносних характеристик обладнання
мереж широкосмугового радіодоступу UMTS/WCDMA..... 52

Демченко В.С.
Сенсорні мережі для оптимізації затрат на тепло та світло..... 54

Волков В.С.
Використання алгоритму мурашиних колоній
для ідентифікації баз нечітких знань..... 55

Колотуша С.В.
Техніко-економічні характеристики
розвитку телекомунікаційних підприємств..... 58

Рак Р.І.
Оптимізація процесу передачі обслуговування
в мережах LTE за допомогою інтерференційної координації..... 61

Лавриненко А.Ю., Давлетьянц А.И.
Сжатие и фильтрация речевых сигналов
в телекоммуникационных системах..... 65

Харламов І.В.
Оптимізація параметрів аналого-цифрового перетворення сигналу..... 69

Якименко І.В., Одарченко Р.С.
Рішення віртуалізації для центрів обробки даних..... 71

Тимошенко О.С., Ткаліч О.П.
Інтеграція мереж передачі IP-трафіку
з системами відеоспостереження об'єктів..... 73

Кочубей А.Б.
Захист хосту від хибного маршруту з використанням протокола
ICMP з метою створення в мережі Internet хибного маршрутизатора.. 74

Василенко Ю.В.
Метод структурної ідентифікації баз нечітких знань..... 77

Коренюк М.О.
Надання послуг Інтернет з використанням широкосмугових
бездротових систем на базі обладнання MikroTik..... 79

Спиридонов А.Ю., Шевчук Ж.А., Одарченко Р.С.
Многоуровневый анализ сбоев в работе сети..... 80

Смолянюк І.М.
Високошвидкісна мережа Інтернет..... 81

Вегер О.А.
Локальна мережа підприємства..... 83

Шемет Д.В.
Методи створення захищеного радіоканалу
керування безпілотними літальними апаратами..... 84

Іванченко І.В.
Розробка удосконаленої системи керування
рівнем випромінюваної потужності базових станцій мереж LTE..... 85

Беленчак Л.В.
Надвисокочастотна лінія цифрового зв'язку (VDL) режиму 2..... 87

Паламарчук О.С., Триус Ю.В.
Типова структура інформаційної системи
для небанківських фінансових установ..... 91

Кохан І.В.
Мультисервісна мережа підприємства..... 95

Стецюра Ю.І.
Оптимізація структури мереж 4 покоління (LTE)..... 96

Козлов О.І.
Система віддаленого керування та оптимізації
контенту веб-сторінок сайтів..... 98

Семенюк І.В.
Впровадження мережі мобільного зв'язку
четвертого покоління стандарту LTE в Україні.....100

Бахтіяров Д.І.
Криптографічний захист сигналу керування
безпілотним літальним апаратом.....102

Рассказчікова В.В.
Комплексні заходи захисту інформації при проведенні конференції.....104

Бусел А.О.
Модель оцінки цінності отриманої інформації
у системі конкурентної розвідки.....105

Мокроусов А.В.
Моделювання побудови контакт-центру
на базі апаратних та програмних засобів AVAYA.....107

Высочиненко М.С.
Статистические характеристики процесса запросов
к станциям беспроводной сети на основе методов поллинга.....110

Шевчук Ж.О., Спірідонов А.Ю., Мачалін І.О.
Безпека мереж наступного покоління NGN.....112

НАУКОВЕ ВИДАННЯ

ТЕЗИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

2 – 5 ЧЕРВНЯ 2014 Р.

М. КИЇВ

ГОЛОВНИЙ РЕДАКТОР КОНАХОВИЧ Г.Ф.

КОМП'ЮТЕРНА ВЕРСТКА ГОЛУБНИЧИЙ О.Г.

КОНТАКТНИЙ E-MAIL: a.holubnychyi@nau.edu.ua

ВІДПОВІДАЛЬНІСТЬ
ЗА ЗМІСТ ТА ФОРМУ ВИКЛАДЕННЯ НАУКОВИХ РЕЗУЛЬТАТІВ
НЕСУТЬ АВТОРИ МАТЕРІАЛІВ ТЕЗ.

© НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ, 2014

ЕЛЕКТРОННА ВЕРСІЯ ТЕЗ КОНФЕРЕНЦІЇ ЗРОБЛЕНА СПЕЦІАЛЬНО ДЛЯ РОЗМІЩЕННЯ НА САЙТІ
НАЦІОНАЛЬНОГО АВІАЦІЙНОГО УНІВЕРСИТЕТУ
http://nau.edu.ua/

ЗМІСТ ЕЛЕКТРОННОЇ ВЕРСІЇ ТЕЗ КОНФЕРЕНЦІЇ
ВІДПОВІДАЄ ЇХ ОФІЦІЙНІЙ ДРУКОВАНІЙ ВЕРСІЇ.