УДК 681.324

Г.А. Кучук[1], А.А. Коваленко[2], А.А. Можаев[3]

[1]*Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков*
[2]*Харьковский национальный университет радиоэлектроники, Харьков*
[3]*Национальный технический университет "ХПИ", Харьков*

# ОЦЕНКА БЕЗОПАСНОСТИ МУЛЬТИСЕРВИСНОЙ СЕТИ

*В статье предложен новый подход к определению метрики безопасности, который объективно выявляет наиболее значимые факторы сетевых рисков, включая существующие уязвимости, историческую тенденцию уязвимости услуг с удаленным доступом, прогнозирование потенциальных уязвимостей для любой характерной сетевой услуги, а также оценку их серьезности и устойчивость политики безопасности к распространению атак в сети. Приведены эксперименты, базирующиеся на реальных данных об уязвимости мультисервисной сети.*

***Ключевые слова:*** *метрика, мультисервисная сеть, политика безопасности, уязвимость.*

## Введение

**Актуальность исследования.** Проведение оценки сетевой безопасности необходимо при организации защиты в любой сети. Такая оценка может оказать помощь специалистам в области безопасности в принятии оптимальных решений относительно разработки контрмер, при выборе между альтернативными архитектурами безопасности и систематическом модифицировании конфигураций безопасности. Однако, безопасность сети зависит от множества динамически изменяющихся факторов, таких как появление новых уязвимостей и угроз, структуры политик безопасности и изменений сетевого трафика. Выявление, квантификация и валидация этих факторов с использованием метрик безопасности является существенной проблемой в этой области.

При рассмотрении вопросов оценки уязвимости мультисервисной сети (МСС) необходимо оценивать уязвимость каждой из ее служб. Общая конфигурация системы безопасности сети определяет степень влияния брешей в безопасности каждой из служб на сеть. В данной статье предлагается новый подход для оценки политики безопасности сети, при котором можно количественно измерять степень уязвимости сети, основываясь на двух критических аспектах – угрозе успешной атаки и угрозе распространения такой атаки в сети (рис. 1). Модель такой системы оценки предполагает измерение уровня безопасности сетевых сервмсов на основе анализа уязвимости (наличия существующих уязвимостей, скрытая угроза основывается на истории предыдущих уязвимостей и на их прогнозировании в будущем) и прогнозирование степени безопасности сети. Модель должна учитывать степень незаконного проникновения или влияния успешных атак.

Предлагаемая метрика оценки даст возможность сравнения различных политик безопасности с целью определения более надежной. Также можно судить о влиянии изменения политики безопасности путем сравнением метрик безопасности до и после изменения. Это позволит сетям получать автоматическую оценку и укрепляться с помощью непрерывного мониторинга динамических изменений уязвимости сети и ее сервисов.

Существующие средства оценки безопасности сетей и проведенные исследования проверяют или анализируют заданную сеть на предмет разрешенных образцов трафика и существования уязвимо-

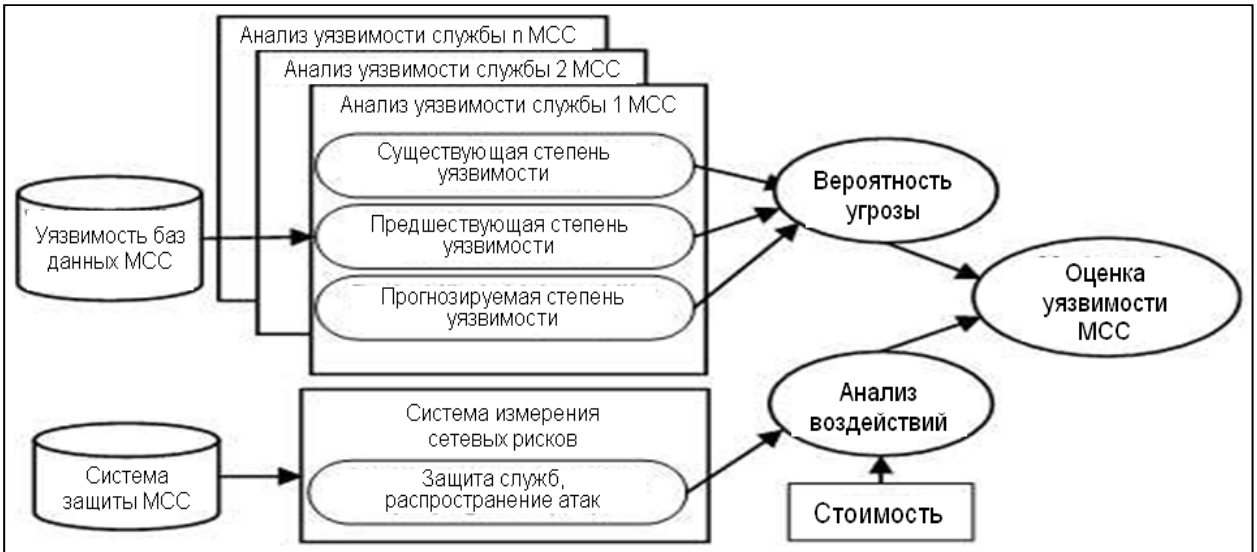



Рис. 1. Схема оценки сетевой безопасности

стей, однако не прогнозируют будущие состояния безопасности сети. Работы, в которых прогнозируются будущие уязвимости, только начинают появляться [1]. Предложенная модель прогнозирования является универсальной и может работать, используя только общедоступные данные.

**Анализ существующих подходов.** Организационные стандарты, необходимые при получении оценки безопасности мультисервисной сети, достаточно полно рассмотрены в [2]. В [3] аргументирована важность метрик безопасности. Оценка брандмауэров и их политик безопасности для подсетей корпоративных сетей (Virtual Private Network, VPN) проведена в ряде работ, например, [4 – 7]. Технология оценки рисков, базирующаяся на построении графа атак, рассмотрена в [8]. В [9] введены количественные оценки безопасности, базирующиеся на чувствительности системы к атакам (вводится понятие поверхности атак). В [10] предложена метрика безопасности, основанная на анализе самого слабого противника (т.е. наименьшем усилии, требуемом для успешной атаки). В [1] авторы представили результаты прогнозирования уязвимостей. В [11] предлагается подход к вычислению меры риска. В [12] проведено исследование подходов к измерению уязвимости сети. Однако все вышеперечисленные работы преимущественно пытаются обнаружить существующие риски и не затрагивают проблемы количественной оценки безопасности системы в ближайшем будущем (как структура политики безопасности и сетевого трафика может повлиять на безопасность).

Исходя из этого, **целью данной статьи** является разработка нового подхода к определению метрики безопасности мультисервисной сети, который объективно выявляет наиболее значимые факторы сетевых рисков как в настоящем времени, так и на некоторый последующий период, основываясь на предшествующей информации про функционирование сетевой системы защиты.

## 1. Теоретическая часть

### 1.1. Анализ рисков сетевого сервиса

При проведении анализа уязвимости с целью измерения степени риска сетевого сервиса необходимо определить меру существующей степени уязвимости (Existing Vulnerability Measure, EVM), меру предшествующей степени уязвимости (Existing Historical Measure, HVM) и меру прогнозируемой степени уязвимости (Existing Probabilistic Measure, PVM).

Существующая уязвимость важна для тех сетей, где системы обеспечения безопасности сетевых сервисов остались необновленными с точки зрения безопасности, либо для сетей, у которых не существует обновлений. После обнаружения уязвимости сети требуется время для внедрения исправляющего обновления, если это возможно. В этот период сеть и ее сервисы уязвимы к внешним атакам. EVM должна измерять такой риск для сетевых сервисов. EVM – мера серьезности существующей уязвимости в сети [12]. Для измерения EVM можно использовать существующее программное обеспечение, позволяющее сканировать сетевые уязвимости [12].

**Определение предшествующей степени уязвимости – HVM.** Данная мера должна отражать поведение уязвимости сети и ее сервисов в прошлом, используя отчеты относительно уязвимости сетевых сервисов и сети в целом. Рассматривая частоту и степень новизны уязвимостей, разобьем множество прошлых уязвимостей таким образом, чтобы сервисы с высокой частотой уязвимостей в недалеком прошлом имели большее значение HVM. Для этого множество уязвимостей U разделим на L классов уязвимостей

$$U = \bigcup_{\ell=1}^{L} U_\ell ,$$

где $U_1$, $U_2$, …, $U_L$ – подмножества, упорядоченные по убыванию степени уязвимости, представляющие риски с весовыми коэффициентами $\omega_1$, $\omega_2$, …, $\omega_L$ соответственно.

Каждому классу $j_\ell$ запротоколированных уязвимостей сервиса $S_i$ ($i=\overline{1,I}$, I – количество сервисов рассматриваемой МСС) введем коэффициенты $h_{ij_\ell}$ (коэффициент старения) и $k_{ij_\ell}$ (коэффициент частоты) с таким расчетом, чтобы уязвимости, обнаруженные давно, имели меньший вес, так как со временем они анализируются и исправляются. Применив функцию экспоненциального затухания для возраста уязвимости определим для каждого класса соответствующие весовые множители

$$H_{ij_\ell} = k_{ij_\ell} \cdot e^{-\beta h_{ij_\ell}}, \qquad (1)$$

где параметр $\beta$ управляет скоростью затухания множителя с течением времени. При вычислении значения HVM отдельного сервиса МСС просуммируем эти затухающие множители каждого класса и возьмем их взвешенную сумму, которую для получения аддитивной неотрицательной меры сдвинем на единицу и прологарифмируем, т.е.

$$\begin{aligned} HVM(S_i) &= \ln\left(1+\sum_{\ell=1}^{L}\omega_\ell \cdot \sum_{j_\ell=1}^{J_\ell} H_{ij_\ell}\right) = \\ &= \ln\left(1+\sum_{\ell=1}^{L}\omega_\ell \cdot \sum_{j_\ell=1}^{J_\ell} k_{ij_\ell} \cdot e^{-\beta h_{ij_\ell}}\right). \end{aligned} \qquad (2)$$

Для оценки комплексного значения HVM МСС S объединим значения HVM всех сетевых сервисов, взяв экспоненциальное среднее всех значений HVM отдельных сервисов МСС:

$$\begin{aligned} HVM(S) &= \ln\left(\sum_{i=1}^{I}\exp\left(HVM(S_i)\right)\right) = \\ &= \ln\left(\sum_{i=1}^{I}\left(1+\sum_{\ell=1}^{L}\omega_\ell \cdot \sum_{j_\ell=1}^{J_\ell} H_{ij_\ell}\right)\right). \end{aligned} \qquad (3)$$

**Определение вероятностной степени уязвимости – PVM.** Рассматриваемая мера должна объединять вероятность ожидаемой уязвимости и ее серьезность с целью получения информации о рисках сети в ближайшем будущем.

Используя историю уязвимостей можно подсчитать распределение вероятностей серьезности уязвимостей, влияющих на сетевой сервис. Используя данное распределение можно вычислить ожидаемую серьезность уязвимости в следующий период времени. Определим меру ожидаемого риска ($ER_i$) для i-го сервиса, как произведение вероятности по меньшей мере одной новой уязвимости, влияющей на сервис в следующий период времени, и ожидаемой серьезности уязвимостей. При заданном значении типа уязвимости $\ell$, можно сказать, что сервис имеет большую вероятность получения по меньшей мере одной новой уязвимости серьезности $\ell$ в следующий период времени.

Сначала построим список межинтервальных времен между предыдущими уязвимостями, влияющими на каждый из сервисов. Затем вычислим вероятность того, что межинтервальное время становится меньше заданного периода времени $T_i$, т.е. $P_{S_i}$ (вероятность того, что $d_{S_i}$ – количество дней до следующей уязвимости сервиса $S_i$), меньше $T_i$. Значение $T_i$, приводящее к большей точности, определяется экспериментально на основании используемой базы данных. Для вычисления ожидаемой серьезности, построим распределение вероятностей серьезности. Используя $\ell$ как случайную переменную, соответствующую степени серьезности рассматриваемого сервиса, $\ell(S_i)$, можно определить ожидаемый риск $ER_i$, для сервиса $S_i$:

$$ER(S_i) = P_{S_i} \times M\left[\ell(S_i)\right]. \qquad (4)$$

где $M\left[\ell(S_i)\right]$ – ожидаемое значение $\ell$ для услуги сервиса $S_{ii}$.

Для определения сетевого значения PVM рассчитаем экспоненциальное среднее всех значений HVM отдельных сервисов МСС:

$$PVM(S) = \ln\sum_{i=1}^{I}\exp\left(ER(S_i)\right). \qquad (5)$$

Предположим, что случайная величина $\ell(S_i)$ имеет экспоненциальное распределение со средним межинтервальным временем для сервиса $S_i$, равным $\lambda_i$. Тогда

$$P_{S_i} = P\left(d_{S_i} \le T\right) = F_{d_{S_i}}(T) = 1 - e^{-\lambda_i T}. \qquad (6)$$

Можно рассчитать $P_{S_i}$, используя эмпирическое распределение случайной величины $\ell(S_i)$. Если $f_i(\ell)$ – число уязвимостей, при которых значение $\ell$ оказывается в межинтервальных временах сервиса $S_i$, то

$$P_{S_i} = P\left(d_{S_i} \le T\right) = F_{d_{S_i}}(T) = \sum_{\ell_i | d_{S_i} \le T} f_i(x) \Bigg/ \sum_{\ell_i=1}^{L_i} f_i(x), \qquad (7)$$

### 1.2. Анализ рисков сетевой политики безопасности

Сетевая политика безопасности определяет границы возможного проникновения МСС во внешнюю среду. Степень, с которой политика безопасности позволяет атаке распространяться в сети, представлена метрикой распространения атак (AP). Это позволяет оценить сложность (для атакующего) распространения атаки по сети, используя уязвимо-

сти услуг и уязвимости политик безопасности. Данная мера дополняет предыдущие меры при формировании комплексной метрики, позволяющей анализировать специфические области с целью улучшения безопасности сети, в которой могут взаимодействовать различные политики безопасности.

Определим МСС, состоящую из N узлов и защищенную k брандмауэрами, следующими множествами: $D=\{d\in N\}$ – множество узлов МСС, доступных внешним воздействиям; $S_n=\left\{i\middle|i\in\overline{1,I}\right\}$ – множество сервисов, поддерживаемых узлом n; $P=\{p_i\}$ – множество нормированных комплексных мер уязвимости EVM и HVM служб МСС, $p_i$ – убывающая в диапазоне от 0 до 1 функция сервиса i.

Для оценки защищенности сервиса от атак определим меру $\mu(i)$, которая оценивает защищенность от атак для данной услуги i, используя значения $HVM(S_i)$ и $EVM(S_i)$:

$$\mu(i)=-\ln(p_i). \qquad (8)$$

Значение меры $\mu(i)$ находится в диапазоне $[0,\infty)$ и используется для измерения простоты, с которой атакующий может распространить атаку от одного узла к другому используя услугу i. Таким образом, если узел $n_1$ может подключаться к узлу $n_2$, используя исключительно услугу i, то $\mu(i)$ является мерой защищенности узла $n_2$ к атаке, исходящей из узла $n_1$. Полагая, что мера комплексной уязвимости независима для различных услуг, можно вычислить меру комплексной уязвимости $\mu(n_1,n_2)$, т.е. оценить комплексную уязвимость к атакам как:

$$\mu(n_1,n_2)=-\ln\left(p_{n_1,n_2}\right)\times PL, \qquad (9)$$

где PL – характеристика уровня защиты (для защиты с использованием брандмауэра этот уровень равен 1, а для защит IDS его значение колеблется между 0 и 1).

Далее отобразим полученные результаты в качестве весов дуг ориентированного графа связей сервисов $G_S$. Для расчета распространения атаки в пределах досягаемости от пораженного узла $n_d\in D$ построим минимальное связующее дерево $G_{n_d}$ с корнем в вершине $n_d$ в сегменте возможного распространения атаки графа $G_S$, . Влияние взлома услуги $\left(SBE_{n_d}\right)$ на вес дерева $G_{n_d}$ может быть вычислено следующим образом:

$$SBE_{n_d}=\sum_{n_\xi\in G_{n_d}}\left(\prod_{n_v\in(n_d,n_\xi)}p_{n_d,n_v}\right)\times Cost_{n_\xi}, \qquad (10)$$

где $Cost_{n_\xi}$ – стоимость повреждения узла $n_\xi$.

Тогда метрика распространения атак в сети определяется как

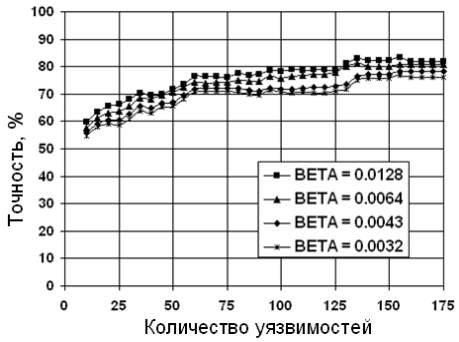
$$MP(S)=\sum_{n_d\in D}P(n_d)\cdot SBE_{n_d}=$$

$$=\sum_{n_d\in D}P(n_d)\cdot\left(\sum_{n_\xi\in G_{n_d}}\left(\prod_{n_v\in(n_d,n_\xi)}p_{n_d,n_v}\right)\times Cost_{n_\xi}\right), \qquad (11)$$

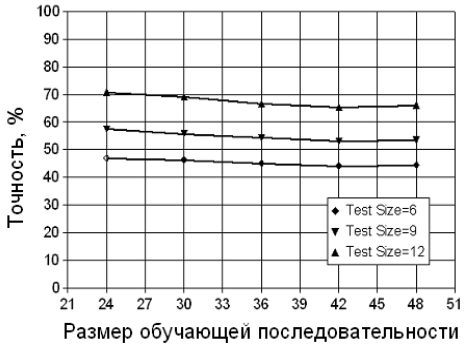
где $P(n_d)$ – вероятность наличия уязвимости в узле $n_d$. Данная метрика позволяет получить ожидаемую стоимость как результат распространения атаки в сети.

## 2. Анализ результатов экспериментов

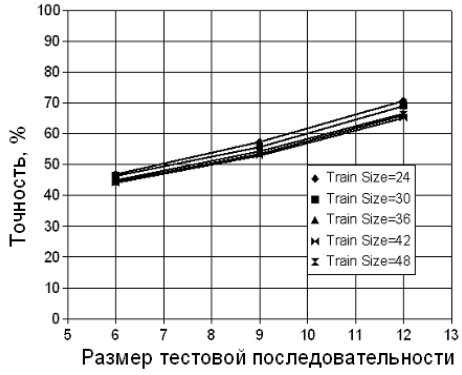
Для экспериментов использовались данные баз данных уязвимостей в стандарте CVE (Common Vulnerabilities and Exposures), приведенные Национальным институтом науки и технологий (США, [13]). Текущая степень уязвимости основывалась на оценке CVSS [14] в диапазоне от 1 до 10. (рис. 2).




а




б




в

Рис. 2. Анализ точности HVM: а – для различных значений β; б – для различных длительностей обучающей выборки; в – для различных длительностей тестовой выборки

На рис. 2 показаны результаты проверки точности HVM для различных значений управляющего параметра $\beta$ (рис. 2, а) и проверки точности определения ожидаемого риска для различных значений обучающей выборки (рис. 2, б, в).

Проверки точности HVM для различных значений управляющего параметра $\beta$ показала, что при увеличении базового числа анализируемых предшествующих уязвимостей точность определения увеличивается, а влияние управляющего параметра уменьшается. Максимальная точность составила 83.33%.

При анализе оценки ожидаемого риска (ER) данные разделялись на тестовую и обучающую последовательности, вычислялось необходимое количество обучающих последовательностей, а точность определялась тестовыми последовательностями данных. Распределение .случайной величины $\ell(S_i)$ предполагалось близким к экспоненциальному (оценка эмпирического распределения проводилась методом наименьших квадратов с уровнем значимости $\alpha = 0{,}05$. Значение T изменялось от 15 до 90 дней с шагом $\Delta T = 15$.

Для тестовой последовательности данных для 12 месяцев, наблюдаемая максимальная точность составила 78.62% при 95% доверительном интервале [72:37; 84:87] для обучающей последовательности данных размером 42 месяца и интервалом прогнозирования в 90 дней. Согласно полученным результатам, точность ожидаемого риска в некоторой степени коррелируется с размером обучающей последовательности данных и строго коррелируется с размером тестовой последовательности данных.

Для оценки осуществимости вычисления метрика распространения атак в сети при различных условиях предложенный алгоритм был реализован в среде MATLAB для различных размеров сети и различных значений связности сети. Результаты моделирования приведены на рис. 3.

Для каждого размера сети генерировались несколько случайных сетей с одинаковым значением коэффициента связности сети. Время выполнения было вычислено для нескольких узлов в пределах каждого эксперимента. Как видно из рисунка, квадратичный рост времени выполнения к связности сети незначительно зависит от коэффициента связности сети при рассмотренных реализациях.

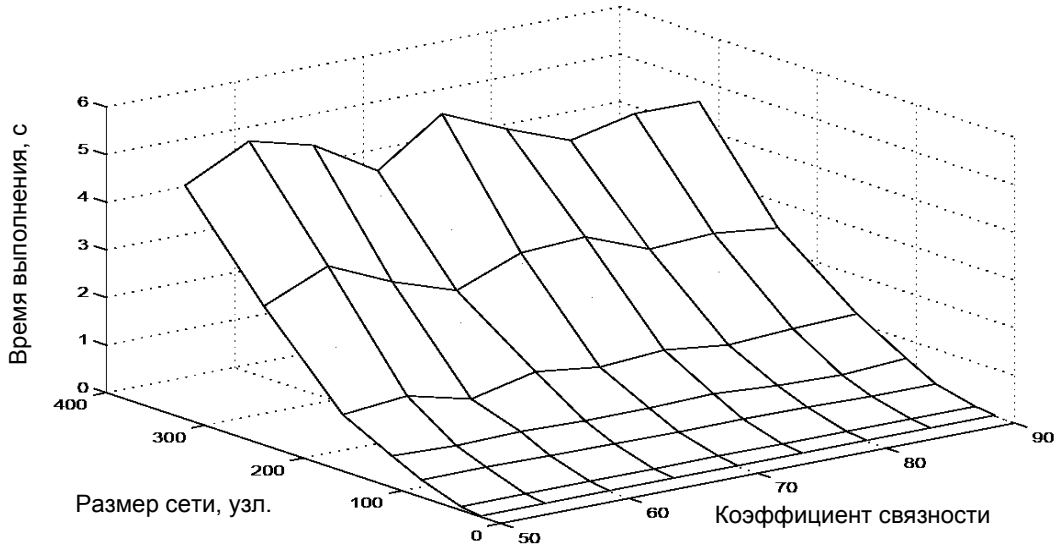



Рис. 3. Среднее время выполнения для различных размеров сети и коэффициентов связности

## Выводы

Предложенная универсальная метрика оценки политики безопасности МСС позволяет провести оценку степени защиты конкретной политики безопасности, а также разработать предложения по усилению безопасности сети. Предложенный подход к количественной оценке сетевой безопасности основан на идентификации, формализации и валидации ряда факторов, которые в значительной мере влияют на безопасность сети.

Проведенные эксперименты подтвердили гипотезу о том, что если у сервиса имеется историческая предрасположенность к уязвимости, то с большой вероятностью такая услуга снова подвергнется уязвимости в ближайшем будущем. Такие метрики полезны не только для администраторов сети с целью оценки изменений в политике безопасности и принятия своевременных решений, а также для введения адаптивных систем безопасности, что и является направлением дальнейших исследований

## Список литературы

*1. Rogers R. Network Security Evaluation Using the NSA IEM / R. Rogers, E. Fuller, G. Miles, M. Hoagberg, T. Schack, T. Dykstra,B. Cunningham // Syngress Publishing, Inc., first edition, August 2005.*

*2. Alhazmi O.H. Prediction capabilities of vulnerability discovery models / O.H. Alhazmi, Y.K. Malaiya // Proc. Reliability and Maintainability Symposium. – January 2006. – P. 86-91.*

*3. Ammann P. Scalable, graph-based network vulnerability analysis / P. Ammann, D. Wijesekera // 9th ACM conference on Computer and communications security, 2002.– P. 217-224.*

*4. Abedin M. Vulnerability analysis for evaluating quality of protection of security policies / M. Abedin, S. Nessa, E. Al-Shaer, L. Khan // 2nd ACM CCS Workshop on Quality of Protection, Alexandria, Virginia, October 2006.*

*5. Kamara S. Analysis of vulnerabilities in internet firewalls / S. Kamara, S. Fahmy, E. Schultz, F. Kerschbaum, and M. Frantzen // Computers and Security, 22(3):214232, April 2003.*

*6. Al-Shaer E. Conflict classification and analysis of distributed firewall policies / E. Al-Shaer, H. Hamed, R. Boutaba, M. Hasan // IEEE Journal on Selected Areas in Communications (JSAC), 23(10), October 2005.*

*7. Atzeni A. Why to adopt a security metric? A little survey / A. Atzeni, A. Lioy // QoP-2005: Quality of Protection workshop, September 2005.*

*8. Hamed H. Modeling and verification of ipsec and vpn security policies / H. Hamed, E. Al-Shaer, W. Marrero // IEEE ICNP'2005, November 2005.*

*9. Manadhata P. An attack surface metric / P. Manadhata, J. Wing // First Workshop on Security Metrics, Vancouver, BC, August 2006.*

*10. Sahinoglu M. Security meter: A practical decision-tree model to quantify risk / M. Sahinoglu // IEEE Security and Privacy, June 2005.*

*11. National institute of science and technology (nist). [Электронный ресурс]. – Режим доступа к ресурсу: кhttp://nvd.nist.gov.*

*12. Al-Shaer E. Discovery of policy anomalies in distributed firewalls /E. Al-Shae, H. Hamed // Proc. of IEEE INFOCOM'04, March 2004.*

*13. Pamula J. A weakest-adversary security metric for network configuration security analysis / J. Pamula, P. Ammann, S. Jajodia, V. Swarup // ACM 2nd Workshop on Quality of Protection 2006, Alexandria, VA, October 2006.*

*14. Schiffman M. A complete guide to the common vulnerability scoring system (cvss) [Электронный ресурс]/ M. Schiffman. – Режим доступа к статье: http://www.first.org/cvss/cvss-guide.html, June 2005.*

*Поступила в редколлегию 5.11.2009*

**Рецензент:** д-р техн. наук, проф. В.А. Краснобаев, Харьковский национальный технический университет сельского хозяйства им. П. Василенко, Харьков.

## ОЦІНКА БЕЗПЕКИ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ

Г.А. Кучук, А.А. Коваленко, О.О. Можаєв

*У статті запропонований новий підхід до визначення метрики безпеки, який об'єктивно виявляє найбільш значущі чинники мережевих ризиків, включаючи існуючі вразливості, історичну тенденцію вразливості послуг з віддаленим доступом, прогнозування потенційних уязвимостей для будь-якої характерної мережевої послуги, а також оцінку їх серйозності і стійкість політики безпеки до розповсюдження атак в мережі. Приведені експерименти, що базуються на реальних даних про вразливість мультисервісної мережі.*

***Ключові слова:*** *метрика, мультисервісна мережа, політика безпеки, вразливість.*

## ESTIMATION OF SAFETY MULTISERVICE NETWORK

G.A. Kuchuk, A.A. Kovalenko, A.A. Mogaev

*In the article the new going is offered near determination of birth-certificate of safety, which exposes the most meaningful factors of network risks objectively, including existing vulnerability, historical tendency of vulnerability of services with remote access, prognostication of potential уязвимостей for any characteristic network favour, and also estimation of their seriousness and stability of policy of safety to distribution of attacks in a network. Experiments, being based on the real information about vulnerability of multiservice network, are resulted.*

***Keywords:*** *birth-certificate, multiservice network, policy of safety, vulnerability.*