УДК 004.056

В. И. Булдыжов, аспирант
Ин-т проблем моделирования в энергетике
им. Г. Е. Пухова НАН Украины
(Украина, 03164, Киев-164, ул. Генерала Наумова, 15,
тел. (044) 4249903, e-mail: vladimir.buldyzhov@gmail.com)

Электротехнические аналоги в оценке рисков информационной безопасности

Предложен новый подход к построению количественной оценки уровня риска безопасности информации. Обоснована возможность и корректность использования электротехнических аналогий для решения задач моделирования таких рисков.

Запропоновано новий підхід до побудови кількісного оцінювання рівня ризику безпеки інформації. Обґрунтовано можливість та коректність використання електротехнічних аналогій для розв'язання задач моделювання таких ризиків.

Ключевые слова: управление рисками, уязвимости нулевого дня, сопротивление атаке.

Компьютерные сети являются ключевым компонентом инфраструктуры информационных технологий, используемых в большинстве предприятий и организаций. Защита данных сетей от вредоносных вторжений имеет большое значение для экономики и государственной безопасности.

В подавляющем большинстве сетевых программных продуктов регулярно обнаруживаются уязвимости, используемые для организации атак, проводимых удаленными злоумышленниками. Такие уязвимости являются результатом халатности или осознанным браком, который допущен производителем, работающим в условиях конкуренции, когда требуется ускоренный выход продукта. Устранение брака производителем выполняется в виде специальных программных обновлений, «заплат», выпускаемых по мере обнаружения уязвимостей. Процесс обнаружения выполняется как производителем и пользователями продукта, так и злоумышленниками. От момента выпуска обновления до его установки проходит время, в течение которого системы подвергаются наибольшему риску вследствие вынужденного раскрытия информации об уязвимости.

Производитель программного обеспечения (ПО) не несет ответственности за последствия, к которым приводят атаки, обусловленные браком в его продукции. Поэтому ответственность приходится нести владель-

цам и пользователям информационных систем. Величина ответственности соответствует потенциальному ущербу от атаки, который соизмерим со стоимостью всех информационных активов предприятия или организации. Проблема заключаются в том, что заранее неизвестно, где будет обнаружена уязвимость, как быстро придет обновление и не принесет ли установка обновления больше вреда, чем пользы. Поэтому в настоящее время управление рисками безопасности корпоративной сети можно считать скорее искусством, чем наукой. Системные администраторы работают на основе интуиции и опыта, а не полагаются на объективные метрики, руководствуясь которыми можно принимать решения.

Описанный подход к безопасности производства, поддержки и использования сетевого ПО, к сожалению, наиболее распространенный в мире. Наилучшим способом решения данной проблемы является разработка изначально безопасного ПО, но он неприменим для большинства производителей по причине высокой стоимости и других ограничений. Поэтому, исходя из существующей ситуации, попытаемся выполнить поиск и применение объективных метрик, необходимых для управления рисками уязвимостей в имеющихся условиях.

Качественная система метрик защищенности сети должна учитывать последовательное регулярное измерение показателей, сбор информации должен быть не слишком ресурсоемким, показатели должны быть выражены численно, иметь единицы измерения и конкретный контекст. Эти проблемы можно решить, изучая взаимозависимости уязвимостей и измеряя безопасность именно тех путей, которыми проникают в сеть реальные злоумышленники. Анализируя все пути сетевых атак, можно получать показатели риска, позволяющие анализировать компромиссы между затратами и выгодами, а также принимать объективные решения по обработке рисков.

Анализ опубликованных работ. Графы атак позволяют моделировать способы сочетания нескольких уязвимостей для выполнения атаки и представляют собой состояния системы. При этом используются наборы связанных с безопасностью условий, например существование уязвимости в определенном узле сети или связи между узлами.

Граф атак описывает сценарии атак злоумышленника или действующего от его имени вредоносного ПО. В результате анализа графа можно получить следующее:

перечень возможных атак;

сравнение мер безопасности и достигнутого уровня защищенности;

перечень наиболее серьезных уязвимостей;

перечень необходимых мер по устранению уязвимостей.

Графы атак применяются при управлении инцидентами [1], анализе рисков [2] и мониторинге событий в сети (корреляции событий систем обнаружения атак) [3, 4].

Анализируя последние исследования в области графов атак, следует заметить, что в настоящее время разработаны различные типы узлов и дуг графов, такие как граф перечисления состояний, граф зависимостей, ориентированный на условия, и граф зависимостей эксплоитов [5, 6].

Попытки стандартизации уязвимостей увенчались созданием систем типа SSE-CMM [5]. Вклад в развитие измерений уязвимостей внесли документы NIST, в которых предложено следующее:

реализация метрик безопасности процесса [8];

принципы установления безопасности базового уровня [9];

выполнение измерений по информационной безопасности [10];

руководство по управлению рисками для систем информационных технологий [11].

Следует также упомянуть системы стандартизации количественных оценок уязвимостей, в частности CVSS [12], хотя в них рассмотрены отдельные уязвимости без учета взаимозависимости атак на целевую систему.

Сначала графы атак строились вручную, несколько позже были разработаны различные методы автоматизации. Основная проблема при синтезе графов атак —масштабируемость метода на большие сети.

В первых работах по анализу графов атак применялась проверка моделей для перечисления последовательностей атак, связывающих начальное и целевое состояния [13, 14]. Явное перечисление состояний атак обусловливает экспоненциальное возрастание сложности алгоритмов, используемых в данном подходе, при увеличении размера сети. При практическом допущении монотонности атаки сложность графа атак является полиномиальной, а не экспоненциальной [15, 16]. В дальнейшем сложность графов была еще более понижена и в худшем случае стала $O(n^2)$ [17].

Дальнейшее совершенствование методов происходило путем группирования сетей в домены защиты, внутри которых между хостами существует неограниченный доступ [18]. В этом случае сложность сводится к линейной внутри каждого домена защиты и квадратичной в зависимости от числа доменов защиты (которых, как правило, гораздо меньше, чем хостов). Такие графы атак для десятков тысяч хостов (сотни доменов) были синтезированы в течение одной минуты, за исключением визуального представления графа [17]. Подробное описание такого подхода к графам атак приведено в работах [18—20].

Кроме повышения сложности графов атак были предложены методические основы для выражения моделей сетевых атак [21—23]. Возмож-

ности для отображения многоступенчатой атаки стали появляться в некоторых коммерческих продуктах [24, 25], однако в них не показаны все возможные пути атак одновременно, что необходимо для эффективной оценки рисков. Обзор исследований графов атак рассматриваемого этапа развития методологии приведен в работе [26].

Были предприняты попытки измерения рисков сетевой безопасности посредством объединения графов атак с отдельными метриками уязвимостей. В [27] предложено преобразование графов атак и отдельных оценок уязвимостей в байесовские сети для вычисления кумулятивной вероятности. В [28] подтверждается существование циклов в графах атак и поясняется, как вероятность атаки связана с данными циклами. Предложены также методы измерения сопротивления атаке [28] и методы слабейшего успешного нарушителя [29]. В работе [31] описаны методы получения метрик корпоративной сети безопасности, а в [32] для определения риска безопасности ПО использовано понятие «измерение поверхности атаки».

Оценка рисков неизвестных уязвимостей. Перечисленные выше работы посвящены в основном применению графов атак к оценке состояния защищаемой системы и процессу управления известными уязвимостями. В частности, не учитывается величина возможного ущерба от реализации атаки, связанная со стоимостью защищаемых активов. Существенной нерешенной проблемой представляется управление неизвестными уязвимостями, их прогнозирование, а также управление рисками, связанными с данными уязвимостями, включая монетизацию данных рисков.

Под неизвестными уязвимостями системы (в частности, под уязвимостями нулевого дня (zero day vulnerabilities)) подразумевается наиболее опасная стадия существования уязвимостей, когда они известны злоумышленникам, но неизвестны защищаемой системе. Такие уязвимости и способ их использования становится известным злоумышленникам чаще всего в результате обратного инжиниринга выпускаемых производителями ПО обновлений («заплаток»). При этом данные обновления по разным причинам еще не установлены в защищаемой системе.

Целью выбранного направления работы является разработка метода управления рисками (включая их количественную оценку), связанными с неизвестными уязвимостями, на основе графов атак. Задачей настоящей работы является развитие понятия сопротивления атаке, разработка способа его расчета, а также процесса обработки неизвестных уязвимостей и связанных с ними рисков.

Определение. Назовем графом атак направленный граф G ($V \cup S$, require $\cup$ provides), где $V \cup S$ — множество вершин; require $\cup$ provides — множество дуг; V — множество уязвимостей; S — множество состояний системы (пред- и постусловий); require $\subseteq V \times \mathrm{S}$ — конъюнктивное отношение (для использования уязвимости необходимы все состояния как преду-

словия); provides $\subseteq S \times V$ — дизъюнктивное отношение (для получения определенного состояния постусловия достаточно использования любой уязвимости).

Для синтеза графа атак применим модифицированный инструментарий MULVAL [33]. На вход данного ПО подаются факты и правила на языке Datalog (подмножество Пролога), в частности следующие условия и правила:

известные уязвимости (с использованием CVSS, OVAL, Nessus и др.);

конфигурации хостов (сервисы и ПО, работающие на хостах);

конфигурация сети (преобразованные правила маршрутизаторов и брандмауэров);

пользователи в сети (права пользователей хостов);

взаимодействие (модель отношений компонентов, правила Datalog, определяющие возможность выполнения кода, доступа к файлам и др.);

политика доступа (кому и к чему разрешен определенный доступ), т.е. могут быть заданы конфигурации сети для проверки соответствия политике безопасности (в данном случае не используются).

На выходе получаем текстовое представление графа атак, которое формируется в процессе обработки правил и фактов Datalog (рис. 1).

В работе [28] предложено использовать метрику сопротивления атаке. Графическое представление рассматриваемого графа атак аналогично электрической цепи, в которой сопротивление мер безопасности аналогично электрическому сопротивлению резисторов (рис. 2). По обратной аналогии граф атак можно назвать цепью защиты актива. На рис. 2 окружностями обозначены условия в виде фактов Datalog, которые могут быть получены посредством расчета трасс атак, темными кружками — примитивные факты, а прямоугольниками — правила деривации Datalog, обозначающие использование эксплоитов, т.е. компрометацию сетевых мер безопасности. При этом факт 0 — конечная цель атакующего.

Назовем ресурсоемкостью атаки U возможные затраты злоумышленника (в общем случае — источника угрозы [11]) на проведение атаки. Допустим (например, в предельном случае нулевой прибыли), что ресурсоемкость атаки равна стоимости актива. В частном случае атаки грубой силы на алгоритм шифрования время взлома шифра уменьшается при увеличении затрат агента угрозы. Это приводит к пропорциональному снижению стойкости шифра, следовательно, к увеличению частоты нарушений:

$$I = U / R, \tag{1}$$

где R — собственная характеристика криптостойкости алгоритма шифрования, представляющая собой, фактически величину сопротивления меры безопасности атаке.

```
<0>I --execCode (attacker, workStation, root)
    <r0>Rule5: Trojan horse installation
    I<1>I --accessFile(attacker,workStation,write,/usr/local/share)
        <r1>Rule14: NFS semantics
            []-nfsMounted(workStation,/usr/local/share,fileServer,/export,read)
          <2>II --accessFile(attacker,fileServer.write,/export)
            <r2a>Rule10: execCode implies file access
                []-fileSystemACL(fileServer,root,write,/export)
              <3>I --execCode(attacker,fileServer,root)
                <r3>Rule3: remote exploit of a server program
                    []-networkServiceInfo(fileServer,mountd,rpc,100005,root)
                    []-vulExists(fileServer,CVE-2003-0252,mountd,
                        remoteExploit,privEscalation)
               <4>I --netAccess(attacker,fileServer,rpc,100005)
                <r4>Rule6: multi-hop access
                    [] -hacl (webServer, fileServer, rpc, 100005)
                 <5>I --execCode(attacker,webServer,apache)
                    <r5>Rule3: remote exploit of a server program
                        [] -networkServiceInfo(webServer,httpd,tcp,80,apache)
                        [] -vulExists(webServer,CAN-2002-0392,httpd,
                                remoteExploit,privEscalation)
                      <6>I --netAccess(attacker,webServer,tcp,80)
                        <r6>Rule7: direct network access
                            [] -hacl (internet, webServer,tcp,80)
                            [] -located(attacker,internet)
            <r2b>Rule15: NFS shell
                [] -hacl (webServer, fileServer, rpc, 100003)
                []-nfsExportInfo(fileServer,/export,write,webServer)
                I --execCode(attacker,webServer,apache)==> <5>
```

Рис. 1. Древовидное представление графа атак на выходе MULVAL

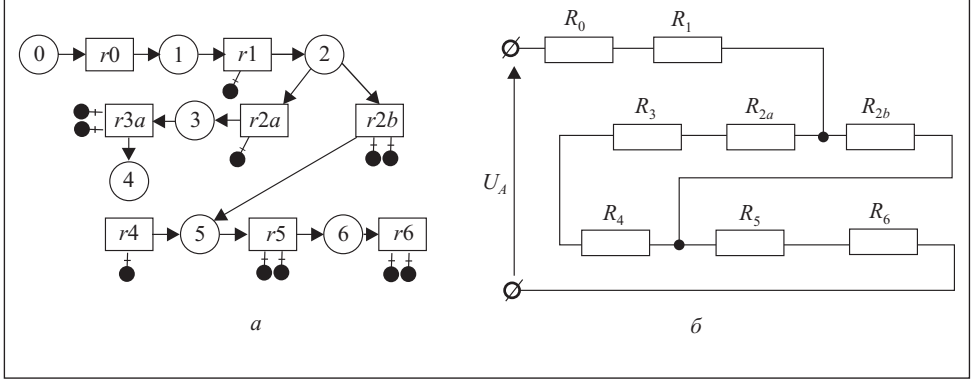

Рис. 2. Граф атак (*а*) и аналогичная электрическая цепь (*б*)

Зависимость (1) аналогична закону Ома для активного сопротивления. При некоторых допущениях можно обобщить зависимость (1), перейдя от нарушений вида «компрометация шифра» к нарушениям вида «компрометация системы». С помощью синтезированного графа (см. рис. 1), с учетом метрик CVSS величины уязвимостей [12], можно получить систему линейных уравнений по законам Кирхгофа и найти эквивалентное сопротивление цепи $R_э$. Получение и решение этих уравнений поддается автоматизации.

Рассмотрим зависимость величины вероятности нарушения информационной безопасности с частотой нарушений f. При $f < 1/t$, т.е. при инцидентах, возникающих со средней частотой f, вероятность возникновения инцидента за время t подчиняется экспоненциальному распределению:

$$Q(t) = 1 - e^{-ft}. \tag{2}$$

При редких инцидентах, $f \approx Q$, риск за время t можно представить в виде

$$\mathrm{Risk}_t = QU_A \approx f\,U_A, \tag{3}$$

где $0 < f < 1/t$; U_A — стоимость актива. Используя (1), получаем

$$\mathrm{Risk}_t = U_A^2 / R_э. \tag{4}$$

Таким образом, получена возможность оперативной количественной оценки рисков, связанных с уязвимостями. При этом величина риска в графе атаки аналогична величине мощности, выделяемой в электрической цепи, также являющейся разновидностью графа.

Процесс управления неизвестными уязвимостями и рисками, связанными с ними, состоит из двух этапов, включающих следующие операции.

Э т а п I. Управление уязвимостями и формирование их базы знаний:

1. Импорт в систему текущей базы данных известных уязвимостей (CVSS, OVAL).

2. Импорт в систему текущей конфигурации сети.

3. Оценка текущих величин сопротивления мер безопасности R.

4. Синтез и анализ текущего графа атак; управление текущими уязвимостями.

5. Сохранение текущих результатов в базе данных уязвимостей и сопротивлений.

Э т а п II. Оценка рисков неизвестных уязвимостей:

1. Оценка величин сопротивления мер безопасности R:

а) анализ динамики обнаружения уязвимостей в ПО; оценка R в зависимости от типов и версий ПО, его разработчиков и местоположений ПО в сети;

б) экспертная оценка R и коррекция ошибки оценки относительного сопротивления, связанной с субъективностью восприятия защищенности и сопротивления.

2. Синтез графа вероятных атак для неизвестных уязвимостей (zero-day); оценка $R_э$.

3. Нахождение трасс вероятных атак; подстановка величин стоимости активов в сети и нахождение величин рисков, соответствующих вероятным трассам атак.

Э т а п III. Обработка рисков неизвестных уязвимостей:

1. Определение вариантов мер увеличения $R_э$ или уменьшения U_A (например, страхование, переоценка или перенос активов).

2. Оценка планируемого остаточного риска по каждой из данных мер.

3. Оценка затрат на владение (внедрение и эксплуатацию) данными мерами.

4. Выбор оптимального варианта обработки рисков посредством минимизации суммы затрат на владение мерами безопасности и величин рисков.

Выводы

Преимущество предложенного подхода к монетизации метрики сопротивления атакам на неизвестные уязвимости и к обработке их рисков состоит в выражении плохо прогнозируемой величины вероятности атаки через величину сопротивления мер безопасности, относящуюся к конкретной мере безопасности, поэтому более пригодную для оценки и ранжирования. Ранжирование («калибровка») сопротивлений типовых мер безопасности является пока нерешенной проблемой, требующей дальнейших исследований.

Development of attack resistance estimation method is proposed aimed at quantitative estimation of risk level of unknown vulnerabilities and at development of the process of such risks managing.

1. *Stephenson P.* Using formal methods for forensic analysis of intrusion events – a preliminary examination. [Электронный ресурс] — Режим доступа: http://www.imfgroup.com/Document Library.html.
2. *Amenaza.* A Quick Tour of Attack Tree Based Risk Analysis Using. [Электронный ресурс] — Режим доступа:http://www.amenaza.com.
3. *Cuppens F.* Alert Correlation in a Cooperative Intrusion Detection Framework // Proc. of the 2002 IEEE Symposium on Security and Privacy, 2002. [Электронный ресурс] — Режим доступа: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.8332&rep=rep1&type=pdf.
4. *Camtepe S., Yener B.* A Formal Method for Attack Modeling and Detection. [Электронный ресурс] — Режим доступа: http://cs.rpi.edu/research/pdf/06-01.pdf.

5. *Danforth M.* Models for Threat Assessment in Networks. [Электронный ресурс] — Режим доступа: http://www.cs.ucdavis.edu/research/tech-reports/2006/CSE-2006-13.pdf.
6. *Jajodia S., Noel S.* Managing Attack Graph Complexity Through Visual Hierarchical Aggregation // In 1st Intern. Workshop on Visualization and Data Mining for Computer Security, Washington, DC, 2004. — P. 109—118.
7. The Systems Security Engineering Capability Maturity Model. [Электронный ресурс] — Режим доступа: http://www.ssecmm.org/index.html.
8. *Swanson M., Bartol N., Sabato J. et al.* Security Metrics Guide for Information Technology Systems. Special Publication 800-55.— National Institute of Standards and Technology. July, 2003. [Электронный ресурс] — Режим доступа: http://www.rootsecure.net/content/downloads/pdf/nist_security_metrics_guide.pdf.
9. *Stoneburner G., Hayden C., Feringa A.* Engineering Principles for Information Technology Security. Special Publication 800-27 (Rev A).— National Institute of Standards and Technology. June, 2004. [Электронный ресурс] — Режим доступа: http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf.
10. *Chew E., Swanson M., Stine K. et al.* NIST Special Publication 800-55. Revision 1.Performance Measurement Guide for Information Security. July, 2008. [Электронный ресурс] — Режим доступа: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.
11. *Stoneburner G., Goguen A., Feringa A.* NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems. March, 2001. [Электронный ресурс] — Режим доступа: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.
12. *Mell P., Scarforne K., Romanosky S.* A Complete Guide to the Common Vulnerability Scoring System (CVSS). Version 2.0. [Электронный ресурс] — Режим доступа: http://www.first.org/cvss/cvss-guide.html.
13. *Ritchey R., Ammann P.* Using Model Checking to Analyze Network Vulnerabilities // Proc. IEEE Symposium on Security and Privacy.— 2000. [Электронный ресурс] — Режим доступа: http://www.cs.washington.edu/research/projects/poirot3/Oakland/sp/PAPERS/0007_17.PDF.
14. *Sheyner O., Haines J., Jha S. et al.* Automated Generation and Analysis of Attack Graphs// Ibid.— 2002. [Электронный ресурс] — Режим доступа: http://wiki.cac.washington.edu/download/attachments/10000785/Automated+Generation+and+Analysis+of+Attack+Graphs.pdf.
15. *Ammann P., Wijesekera D., Kaushik S.* Scalable, Graph-Based Network Vulnerability Analysis//Proc. Conf. on Computer and Communications Security.— 2002. [Электронный ресурс] — Режим доступа: http://mason.gmu.edu/~skaushik/index_files/p160-ammann.pdf.
16. *Lippmann R., Ingols K., Scott C. et al.* Validating and Restoring Defense in Depth Using Attack Graphs // MILCOM Military Communications Conference, 2006. [Электронный ресурс] — Режим доступа: http://www.ll.mit.edu/mission/communications/ist/publications/ 061023_Lippmann.pdf.
17. *Noel S., Jajodia J.* Understanding Complex Network Attack Graphs through Clustered Adjacency Matrices//Proc. 21st Annual Computer Security Applications Conf., 2005. [Электронный ресурс] — Режим доступа: http://www.acsac.org/2005/papers/87.pdf.
18. *Noel S., Jajodia S.* Managing Attack Graph Complexity through Visual Hierarchical Aggregation// Proc. ACM CCS Workshop on Visualization and Data Mining for Computer Security, 2004. [Электронный ресурс] — Режим доступа: http://csis.gmu.edu/noel/pubs/2004_VizSec.pdf.
19. *Noel S., Jajodia S.* Advanced Vulnerability Analysis and Intrusion Detection through Predictive Attack Graphs//Critical Issues in C4I, Armed Forces Communications and Electronics Association (AFCEA) Solutions Series, 2009. [Электронный ресурс] — Режим доступа: http://csis.gmu.edu/noel/pubs/2009_c4i.pdf.
20. *Noel S., Jajodia S.* Proactive Intrusion Prevention and Response via Attack Graphs// Practical Intrusion Detection. Ed. by Ryan Trost. — Addison-Wesley Professional (in preparation). [Электронный ресурс] — Режим доступа: http://csis.gmu.edu/noel/pubs/ 2008_IDS_chapter.pdf.

21. *Cuppens F., Ortalo R.* LAMBDA: A Language to Model a Database for Detection of Attacks// Proc. on Recent Advances in Intrusion Detection, 2000.— Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs. [Электронный ресурс] — Режим доступа: http://www.springerlink.com/content/4yru642m1f354fdv/.
22. *Templeton, Levitt K.* A Requires/Provides Model for Computer Attacks// Proc. New Security Paradigms Workshop, 2000. [Электронный ресурс] — Режим доступа: http://seclab.cs.ucdavis.edu/ papers/NP2000-rev.pdf.
23. *Ritchey R., O'Berry B., Noel S.* Representing TCP/IP Connectivity for Topological Analysis of Network Security//Proc. 18th Annual Computer Security Applications Conf., 2002.
24. Skybox Security. [Электронный ресурс] — Режим доступа: http://www.skyboxsecurity.com/.
25. RedSeal Systems. [Электронный ресурс] — Режим доступа: http://www.redseal.net/.
26. *Lippmann R., Ingols K.* An Annotated Review of Past Papers on Attack Graphs.— Lincoln Laboratory Technical Report ESC-TR-2005-054.— 2005.
27. *Frigault M., Wang L., Singhal A., Jajodia S.* Measuring Network Security Using Dynamic Bayesian Network//2008 ACM Workshop on Quality of Protection. October 2008. [Электронный ресурс] — Режим доступа: http://csrc.nist.gov/staff/Singhal/qop2008_DBN_paper.pdf.
28. *Wang L., Singhal A., Jajodia S.* Measuring the Overall Security of Network Configurations using Attack Graphs// Proc. 21st IFIP WG 11.3 Working Conference on Data and Applications Security.— Springer-Verlag, 2007.
29. *Pamula J., Jajodia S., Ammann P., Swarup V.* A Weakest-Adversary Security Metric for Network Configuration Security Analysis//Proc. 2nd ACM Workshop on Quality of Protection, ACM Press, 2006. [Электронный ресурс] — Режим доступа: http://dl.acm.org/citation.cfm?id=1179502.
30. *Wang L., Islam T., Long T. et al.* An Attack Graph Based Probabilistic Security Metrics// Proc. 22nd IFIP WG 11.3 Working Conference on Data and Application Security (DBSEC 2008).— London, 2008. [Электронный ресурс] — Режим доступа: http://www.nist.gov/itl/csd/singhal-anoop.cfm.
31. *Singhal A., Xou S.* Techniques for Enterprise Network Security Metrics// Proc. 2009 Cyber Security and Information Intelligence Research Workshop.— Oakridge National Labs, 2009. [Электронный ресурс] — Режим доступа: http://www.csiir.ornl.gov/csiirw/09/CSIIRW09-Proceedings/Abstracts/Singhal_abstract.pdf.
32. *Manadhata P., Wing J., Flynn M., McQueen M.* Measuring the attack surface of two FTP daemons//Proc. 2nd ACM Workshop on Quality of Protection, 2006. [Электронный ресурс] — Режим доступа: http://www.cs.cmu.edu/~pratyus/qop.pdf.
33. *Ou X., Govindavajhala S., Appel A.W.* MulVAL: A logic-based network security analyzer // The 14th USENIX Security Symposium, Baltimore, MD, USA, 2005. [Электронный ресурс] — Режим доступа: http://www.cis.ksu.Edu/~xou/publications/mulval_sec05.pdf.

Поступила 09.10.12

БУЛДЫЖОВ Владимир Иванович, аспирант Ин-та проблем моделирования в энергетике им. Г. Е. Пухова НАН Украины. В 2000 г. окончил Украинский государственный морской технический университет (г. Николаев). Область научных исследований — управление информационной безопасностью и рисками.