6. *Молдовян Н. А., Рыжков А. В.* Способ коммутативного шифрования на основе вероятностного кодирования // Вопросы защиты информации. 2013. № 3. С. 3—10.

7. *Демьянчук А. А., Молдовян Н. А., Рыжков А. В.* Выбор „идеальных“ параметров в схеме двухшаговой аутентификации и коммутативном шифре // Изв. СПбГЭТУ „ЛЭТИ“. 2013. № 8. С. 15—18.

8. *Berezin A. N., Moldovyan N. A., Shcherbakov V. A.* Cryptoschemes based on difficulty of simultaneous solving two different difficult problems // Computer Science Journal of Moldova. 2013. Vol. 21, N 2(62). P. 280—290.

Сведения об авторах

Антон Владимирович Муравьев — аспирант; СПИИРАН, научно-исследовательский отдел проблем информационной безопасности; E-mail: muravev.anton@gmail.com

Андрей Николаевич Березин — аспирант; Санкт-Петербургский государственный электротехнический университет „ЛЭТИ“ им. В. И. Ульянова, кафедра автоматизированных систем обработки информации и управления; E-mail: a.n.berezin.ru@gmail.com

Дмитрий Николаевич Молдовян — СПИИРАН, научно-исследовательский отдел проблем информационной безопасности; научный сотрудник; E-mail: mdn.spectr@mail.ru

Рекомендована СПИИРАН

Поступила в редакцию
10.06.14 г.

УДК 004.056

Е. В. Дойникова, И. В. Котенко

АНАЛИЗ ТЕКУЩЕЙ СИТУАЦИИ И ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЙ ПО БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ СЕТИ НА ОСНОВЕ СИСТЕМЫ ПОКАЗАТЕЛЕЙ ЗАЩИЩЕННОСТИ

Рассматривается подход к отслеживанию текущей ситуации по защищенности компьютерной сети и поддержке принятия решений по реагированию на инциденты, нарушающие информационную безопасность. Подход основан на использовании предлагаемой системы показателей защищенности и разработанных алгоритмов их расчета.

Ключевые слова: *оценивание защищенности, показатели защищенности, графы атак, графы зависимостей сервисов, события информационной безопасности.*

Введение. Сложность архитектуры современных компьютерных сетей и проводимых против них атак, а также многообразие событий, нарушающих информационную безопасность, обусловливает необходимость автоматизированной поддержки принятия решений по реагированию на инциденты (information security incident). Основой для принятия решений по реагированию могут служить показатели защищенности, корректно отражающие текущую ситуацию по безопасности компьютерной сети.

В настоящей статье предлагается система показателей защищенности, приводится ряд известных и модифицированных алгоритмов расчета отдельных и интегральных показателей и рассматривается общий подход к анализу ситуации и принятию решений по безопасности на основе предложенной системы показателей.

Релевантные работы. На данный момент существует большое количество исследований в области применения показателей защищенности для анализа безопасности компьютерных сетей. Однако в большинстве работ анализируются отдельные показатели и не учитываются разные типы информации по безопасности. Так, в работах [1, 2] рассматриваются показатели, рассчитываемые на основе информации о составе и характеристиках объектов ком-

пьютерной сети, например характеристиках хостов сети (критичность хоста или ценность для бизнеса, незащищенность хоста и т.п.), характеристиках сети с позиции приложений (количество приложений, процент критичных приложений и т.п.) и характеристиках сети, учитывающих информацию об уязвимостях (количество систем без известных критичных уязвимостей, количество известных уязвимостей и т.п.).

Показатели, рассчитываемые на основе графов атак, рассматриваются в работах [3, 4]. Данные показатели (такие, как уровень навыков атакующего, атрибуты атакующего, потенциал/вероятность атаки) позволяют получить дополнительную информацию о возможных шагах атакующего в сети с учетом уязвимостей системы. Показатели, рассчитываемые на основе графов зависимостей сервисов, позволяют отследить распространение ущерба в сети (см. работы [4, 5]). В работах [6, 7] рассматриваются показатели, отражающие возможность атак нулевого дня (вероятностная мера уязвимости, k-безопасность нулевого дня).

Для оценивания общего уровня защищенности системы в работах [3, 8] предлагается использовать показатель „уровень риска“, а в работе [9] рассматривается показатель „поверхность атаки“.

Проблемы принятия решений обсуждаются в работах [4, 5, 10], где выделяются показатели, отражающие потери и выигрыш при внедрении ответных мер или отказе от реагирования (например, ожидаемые годовые потери, эффективность реагирования, затраты на реагирование и т.п.).

Ряд работ посвящен созданию различных систем показателей, например, показатели могут быть разделены на первичные и вторичные в зависимости от порядка вычислений [11] или разделены по областям функционирования (управление инцидентами или управление уязвимостями) [1]. В работе [12] выделены восемь категорий показателей в зависимости от типа значения (например, количественное или порядковое).

Подход, рассматриваемый в настоящей статье, базируется на показателях защищенности, предложенных в указанных работах, и подходе к моделированию графа атак, изложенном в работах [13—15]. Основным отличием предлагаемого подхода от других является объединение показателей в комплексную систему, предназначенную для эффективной поддержки принятия решений по реагированию на инциденты, нарушающие информационную безопасность.

Система показателей защищенности. При разработке системы показателей защищенности, алгоритмов их расчета и подхода к оцениванию защищенности сети и поддержке принятия решений учитывался ряд требований, в том числе стандартные требования к показателям, приведенные в работе [16] (такие, как значимость, ценность, объективность, воспроизводимость и т.п.). Основными функциональными требованиями к показателям являются:

— возможность выявления наиболее уязвимых мест системы;

— оценивание потенциала атаки и уровня возможного ущерба в случае ее успешной реализации;

— определение профиля атакующего, его целей и возможностей по реализации атак;

— оценивание выигрыша при реагировании на инциденты;

— учет событий, происходящих в системе, для корректного отображения текущей ситуации.

Подход к оцениванию защищенности и поддержке принятия решений по реагированию на инциденты также должен удовлетворять основным функциональным требованиям, а именно, при реализации подхода должны быть обеспечены:

— всеобъемлющая оценка рисков и помощь администратору по безопасности в принятии решения по реагированию с учетом временных и стоимостных ограничений;

— учет требований стандартов и протоколов в области информационной безопасности.

Основные нефункциональные требования к алгоритмам расчета показателей — оперативность (получение результата за минимальное время) и обоснованность (соответствие результатов оценки реальному состоянию компьютерной сети).

На основе указанных требований была разработана система показателей защищенности, включающая показатели нескольких групп (уровней). В соответствии с информацией, используемой для вычисления показателей, выделены показатели топологического уровня, уровня графа атак, уровня атакующего, уровня событий и интегрального (системного) уровня. На *интегральном уровне* показатели предыдущих уровней используются для определения степени риска и выработки рекомендаций.

Показатели *топологического уровня* основываются на данных о составе и характеристиках сети и позволяют выделить наиболее критичные и уязвимые места системы. К ним относятся: *уязвимость хоста*, *слабость хоста*, *внутренняя критичность*, *внешняя критичность*, *процент систем без известных критичных уязвимостей*, *уязвимость хоста к атакам нулевого дня*, *ценность хоста для бизнеса*. Для учета распространения ущерба в сети через зависимости сервисов на данном уровне строится граф зависимостей сервисов на основе подхода, предложенного в работе [5]. Это позволяет более точно рассчитать критичность хостов сети.

Интегральный показатель риска на данном уровне определяется показателями критичности и уязвимости хостов, которые, однако, не учитывают возможные маршруты атак в сети, т.е. доступность хоста для нарушителя.

На *уровне графа атак* вводится дополнительная информация о связях уязвимостей в сети и строятся возможные маршруты атак, объединенные в граф [13—15]. На данном уровне определяются такие показатели, как: *критичность атакующих действий*, *потенциал атаки*, *ущерб от атаки*, *потенциал атаки с учетом нулевого дня*, *стоимостный ущерб от атаки*, *затраты на реагирование*. Для определения вероятностей атаки граф атак преобразуется в граф уязвимостей, вершины которого определяют соответствующие уязвимости, а дуги — переходы между ними. При этом для уменьшения объема вычислений уязвимости делятся на группы в соответствии с индексами Общей системы оценивания уязвимостей (Common Vulnerability Scoring System — CVSS): вектор доступа, сложность доступа и аутентификация [17]. При успешной реализации уязвимости, относящейся к какой-либо группе, атакующий может нанести ущерб хосту или расширить свои права доступа к системе. Вероятность успешной реализации уязвимостей группы определяется как произведение значений указанных индексов CVSS. Для учета успешной реализации уязвимостей, необходимых для достижения предусловий реализации текущей уязвимости, используется формула определения совместной вероятности. Таким образом, при определении интегрального показателя риска на данном уровне, кроме критичности хоста, учитывается вероятность успешной реализации атаки на хост.

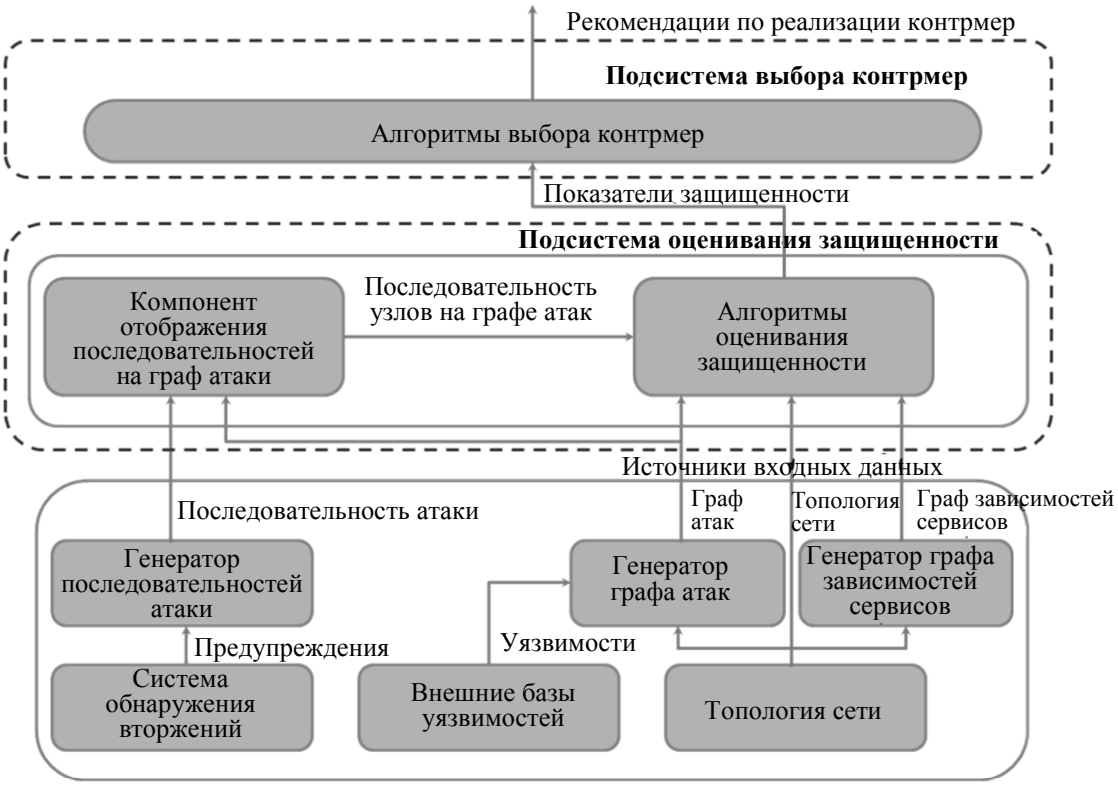
На *уровне атакующего* вводится информация, связанная с различными моделями, характеризующими атакующего, в том числе положение атакующего в системе (внутренний или внешний), уровень навыков атакующего (высокий, средний или низкий) и цель атакующего. На данном уровне определяются следующие показатели: *уровень навыков атакующего*, *профильный потенциал атаки*, *профильный потенциал атаки с учетом нулевого дня*, *профильный стоимостный ущерб от атаки*, *профильные затраты на реагирование*. Данный уровень позволяет при определении интегрального показателя риска учитывать заданные модели.

На *уровне событий* при вычислении показателей учитывается информация о событиях в сети (атакованном хосте и привилегиях, полученных атакующим). Показателями данного уровня являются: *позиция атакующего*, *динамический уровень навыков атакующего*, *вероятностный уровень навыков атакующего*, *динамический потенциал атаки*, *динамический потенциал атаки с учетом нулевого дня*, *динамический стоимостный ущерб от атаки*, *динамические затраты на реагирование*. Данный уровень относится к динамическому режиму функционирования системы и позволяет отражать текущую ситуацию по защищенности

в виде профиля атаки и профиля атакующего. Профиль атаки содержит информацию о текущей позиции атаки на графе атак (в соответствии с поступившими нарушающими безопасность событиями), о наиболее вероятных предыдущих шагах атаки (определяемых на основе теоремы Байеса об апостериорных вероятностях), о наиболее вероятных будущих шагах атаки и цели атакующего. Профиль атакующего содержит информацию о проводимой атаке и наиболее вероятном уровне навыков атакующего. Таким образом, данный уровень позволяет при определении интегрального показателя риска учитывать информацию о развитии проходящей в сети атаки.

Принятие решений по реагированию основывается на учете возможных контрмер для каждой уязвимости графа и решении оптимизационной задачи с использованием предложенных показателей (т.е. минимизации таких показателей, как ущерб и затраты на реагирование при большом показателе вероятности атаки).

Архитектура системы оценивания защищенности и поддержки принятия решений. Предложенные алгоритмы были реализованы в рамках архитектуры, представленной на рисунке.



Система включает две основные подсистемы: 1) подсистему оценивания защищенности и 2) подсистему выбора контрмер. 2-я подсистема генерирует рекомендации по реализации контрмер на основе показателей, полученных от подсистемы оценивания защищенности. 1-я подсистема содержит набор алгоритмов оценивания защищенности и компонент отображения последовательностей событий на граф атак. Подсистема оценивания защищенности получает входные данные от генератора графа атак, генератора графа зависимостей сервисов и генератора последовательностей атак.

Заключение. Представленный подход к отслеживанию текущей ситуации по защищенности компьютерной сети и поддержке принятия решений по выработке контрмер основан на системе показателей защищенности. Описаны основные показатели, соответствующие разным уровням системы, и алгоритмы их расчета. На основе предложенного подхода разработан прототип системы оценивания защищенности и поддержки принятия решений, позволяющий

отследить ситуацию по безопасности в информационной системе и выбрать оптимальный набор контрмер с использованием системы показателей.

Статья подготовлена по результатам работы, выполняемой при финансовой поддержке Российского фонда фундаментальных исследований (гранты 13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417, 14-37-50735), программы фундаментальных исследований ОНИТ РАН (контракт № 2.2), проекта ENGENSEC программы Европейского сообщества TEMPUS и государственных контрактов № 14.604.21.0033, 14.604.21.0137, 14.604.21.0147 и 14.616.21.0028.

СПИСОК ЛИТЕРАТУРЫ

1. The Center for Internet Security. The CIS Security Metrics, v.1.0.0, 2009 [Электронный ресурс]: <https://buildsecurityin.us-cert.gov/sites/default/files/CIS_Security_Metrics_v1.0.0.pdf>, 11.2014.
2. *Mayer A*. Operational Security Risk Metrics: Definitions, Calculations, Visualizations // Metricon 2.0. CTO RedSeal Systems, 2007.
3. *Dantu R., Kolan P., Cangussu J.* Network risk management using attacker profiling // Security and Communication Networks. 2009. Vol. 2, N 1. P. 83—96.
4. *Kanoun W., Cuppens-Boulahia N., Cuppens F., Araujo J.* Automated reaction based on risk analysis and attackers skills in intrusion detection systems // Proc. of the 3rd Intern. Conf. on Risks and Security of Internet and Systems (CRiSIS'08). Toezer, Tunisia, 2008. P. 117—124.
5. *Kheir N., Cuppens-Boulahia N., Cuppens F., Debar H.* A service dependency model for cost-sensitive intrusion response // Proc. of the 15th European Symp. on Research in Computer Security (ESORICS'10). Athens, Greece, 2010. P. 626—642.
6. *Ahmed M. S., Al-Shaer E., Khan L.* A novel quantitative approach for measuring network security // Proc. of the 27th Conf. on Computer Communications (INFOCOM'08). Phoenix, Arizona, 2008. P. 1957—1965.
7. *Wang L., Singhal A., Jajodia S., Noel S.* k-zero day safety: measuring the security risk of networks against unknown attacks // Proc. of the 15th European Conf. on Research in Computer Security. Berlin, Heidelberg: Springer-Verlag, 2010. P. 573—587.
8. *Kotenko I., Saenko I., Polubelova O., Doynikova E.* The ontology of metrics for security evaluation and decision support in SIEM systems // IEEE 2nd Intern. Workshop on Recent Advances in Security Information and Event Management (RaSIEM 2013); In conjunction with ARES 2013. Regensburg, Germany, 2013. P. 638—645.
9. *Manadhata P. K., Wing J. M.* An attack surface metric // IEEE Transact. on Software Engineering, 2010. P. 371—386.
10. *Jahnke M., Thul C., Martini P.* Graph-based metrics for intrusion response measures in computer networks // IEEE Workshop on Network Security. 2007. P. 1035—1042.
11. *Idika N. C.* Characterizing and Aggregating Attack Graph-Based Security Metric: PhD Thesis, Purdue University, 2010. P. 1—131.
12. *Axelrod C. W.* Accounting for value and uncertainty in security metrics // Information Systems Control J. 2008. Vol. 6. P. 1—6.
13. *Kotenko I., Stepashkin M.* Network security evaluation based on simulation of malefactor's behavior // Proc. of the Intern. Conf. on Security and Cryptography (SECRYPT'06). Setubal, Portugal, 2006. P. 339—344.
14. *Котенко И. В., Степашкин М. В., Богданов В. С.* Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников // Проблемы информационной безопасности. Компьютерные системы. 2006. № 2. С. 7—24.
15. *Kotenko I., Chechulin A.* Computer attack modeling and security evaluation based on attack graphs // IEEE 7th Intern. Conf. on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2013). Berlin, Germany, 12—14 Sept., 2013. P. 614—619.
16. *Barabanov R.* Information security metrics. State of the art // DSV Report Ser. 2011. N 11—007, March.
17. Common Vulnerability Scoring System (CVSS) [Электронный ресурс]: <http: // www.first.org / cvss>, 09.2010.

Сведения об авторах

Елена Владимировна Дойникова — аспирант; СПИИРАН, лаборатория проблем компьютерной безопасности; E-mail: doynikova@comsec.spb.ru

Игорь Витальевич Котенко — д-р техн. наук, профессор; СПИИРАН, лаборатория проблем компьютерной безопасности; E-mail: ivkote@comsec.spb.ru

Рекомендована СПИИРАН

Поступила в редакцию
10.06.14 г.