УДК 004.056

Е.В. Дойникова

ПОКАЗАТЕЛИ И МЕТОДИКИ ОЦЕНКИ ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ НА ОСНОВЕ ГРАФОВ АТАК И ГРАФОВ ЗАВИСИМОСТЕЙ СЕРВИСОВ

Дойникова Е.В. **Показатели и методики оценки защищенности компьютерных сетей на основе графов атак и графов зависимостей сервисов.**
Аннотация. В данной работе рассматриваются основные направления исследований в области показателей защищенности и вводится сформированная на их основе классификация показателей. Кроме того, предлагается многоуровневый подход к оценке защищенности, включающий систему показателей защищенности и методики их расчета, основанные на графах атак и зависимостях сервисов. Данный подход позволяет оценивать различные аспекты защищенности системы с учетом ее топологии, режима работы, исторических данных об инцидентах и другой информации.
Ключевые слова: показатели защищенности, методика оценки рисков, граф атак, граф зависимостей сервисов.

Doynikova E.V. **Security metrics and security assessment techniques for the computer networks on the base of the attack graphs.**
Abstract. The paper considers the last researches in the area of the security metrics. Classification of the known metrics is suggested. Multilevel approach to the security assessment is suggested. It is based on the attack graphs and service dependencies graphs. The approach allows evaluating different aspect of the system security considering its topology, operation mode, historical data about incidents and other information.
Keywords: security metrics, risk assessment technique, attack graph, service dependencies graph.

1. Введение. Процесс управления информационными рисками является важным аспектом функционирования современных сложных распределенных информационных систем. Для своевременного и эффективного реагирования на инциденты безопасности важно корректно и оперативно обрабатывать релевантную информацию. В связи с этим большое количество исследований ведется в области формирования систем управления информацией и событиями безопасности (Security Information and Events Management, SIEM) [1].

Одним из этапов функционирования таких систем является вычисление и анализ показателей защищенности. Вычисленные показатели защищенности применяются в процессе управления рисками при принятии решений по безопасности.

В статье рассматриваются методики оценки риска и система показателей защищенности, положенная в их основу. Предлагаемый подход был разработан для системы анализа защищенности, входящей в состав SIEM-системы, разрабатываемой в СПИИРАН в рамках проекта

MASSIF (Management Security and information in Service Infrastructures) [16]. Основными чертами предлагаемого в данной работе подхода являются анализ статической, динамической и исторической информации, связанной с безопасностью, применение для расчета показателей защищенности графов атак и зависимостей сервисов, использование протокола автоматизации управления данными безопасности (Security Content Automation Protocol, SCAP) и международных стандартов, входящих в его состав, для представления данных и оценки уязвимостей, учет современных исследований в области показателей защищенности.

На основе требований со стороны архитектуры системы анализа защищенности и режимов функционирования системы, выделяется несколько уровней оценки защищенности (топологический, графа атак, нарушителя, событий и системы), каждый из которых объединяет ряд показателей защищенности. Предлагаемые показатели позволяют оценивать топологию сети, характеристики нарушителя и атаки, а также интегральные свойства безопасности и характеристики, вычисленные на основе стоимостного анализа, а также анализа уязвимостей нулевого дня. Также в работе рассматривается несколько наиболее характерных методик расчета предлагаемых показателей: статическая методика экспресс оценки защищенности, методика, учитывающая события безопасности, происходящие в системе, и методика, основанная на использовании исторических данных.

Работа организована следующим образом. Во втором разделе рассмотрены основные направления исследований в области показателей защищенности и предложена их классификация. В третьем разделе описаны требования к предлагаемому подходу и представлена сформированная система показателей защищенности. В четвертом разделе дано краткое описание предлагаемых методик оценки рисков. В заключении приведены основные результаты исследования.

2. Релевантные работы. На основе существующих исследований в области показателей защищенности можно выделить следующие основные группы показателей: топологические характеристики, показатели нарушителя, характеристики атаки и реакции на атаку, интегральные показатели, стоимостные характеристики и показатели, применяемые при анализе уязвимостей нулевого дня.

Топологические характеристики рассматриваются, например, в [18] и [5].

В [18] выделяются такие показатели, как *Критичность хоста* (ущерб для бизнеса от потери хоста), *Незащищенность* (определяется достижимостью хоста и простотой использования его уязвимостей),

Ценность для бизнеса (то же, что и *Критичность*), *Риск* (определяется на основе *Незащищенности* и *Ценности для бизнеса*) и *Нисходящий риск* (кумулятивный риск, проходящий через все хосты, атакуемые с данного хоста). В [5] также рассматриваются топологические характеристики с точки зрения приложений — *Количество приложений*, *Процент критичных приложений*, а также топологические характеристики, учитывающие информацию об уязвимостях — *Процент систем без известных критичных уязвимостей*, *Среднее время на устранение уязвимости*, *Количество известных уязвимостей*, и топологические характеристики, учитывающие информацию об атаках, — *Критичность уязвимости* и *Сложность доступа* уязвимости, позволяющие вычислить *Вероятность атаки*.

К характеристикам нарушителя относится *Уровень навыков нарушителя*, являющийся индикатором возможности нарушителя провести сценарий атаки и достигнуть целей безопасности. Данный показатель может вычисляться статически, как в [10], или динамически, как в [21]. В [6] рассматривается вычисление уровня риска на основе поведения нарушителя. В ряде других работ, например в [4], рассматриваются также атрибуты нарушителя (имя, инструменты, географическое положение, мотивы и т.п).

К характеристикам атаки относится *Потенциал атаки* (показывает, как близко находится нарушитель к своей цели). В [22] для определения *Потенциала атаки* используется показатель *Уровень уверенности* — уровень уверенности в том, что атака осуществляется в настоящий момент. В [24] используется *Показатель уверенности в компрометации*. В [3, 9, 11] вычисляется другой показатель — *Ущерб от атаки*. Он может определяться как на основе относительной важности активов, так и на основе статической или динамической стоимости активов. В работах [9, 11, 24] рассматриваются показатели, связанные с контрмерами, такие как *Эффективность реагирования*, *Выигрыш при реагировании* и *Побочные потери при реагировании*.

К интегральным характеристикам относятся, например, следующие показатели: *Поверхность атаки* (определяется на основе показателя – *Отношение потенциала разрушений к затратам*) [15] и *Уровень риска* [6, 8, 14, 22].

К характеристикам, связанным со стоимостным анализом, относятся такие показатели как *Ожидаемые годовые потери* и *Общий выигрыш* (определяется как разница между выигрышем от снижения годовых потерь и соответствующими затратами) [7], а также *Возврат инвестиций от реагирования на атаку* [11].

К характеристикам, используемым при анализе уязвимостей нулевого дня, относятся такие показатели как *Вероятностная мера уязвимости* [3], показывающая насколько вероятно возникновение уязвимости нулевого дня определенной критичности для сервиса за определенный период времени, и показатель, определяющий устойчивость сети к уязвимостям нулевого дня — *k-безопасность нулевого дня* [22].

На основе рассмотренных выше работ была сформирована классификация показателей защищенности, приведенная на рис. 1. Эта классификация была положена в основу формирования системы показателей защищенности и методик их расчета, предлагаемых в данной работе.

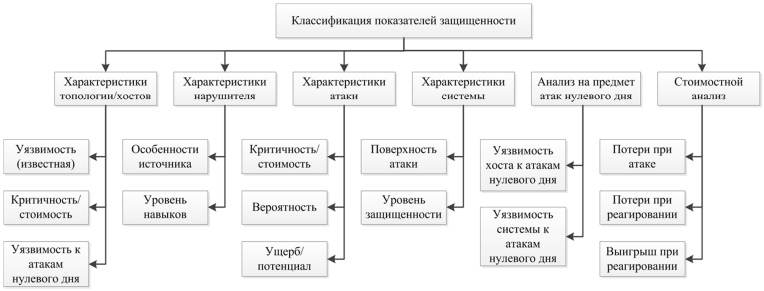

Рис. 1. Классификация показателей защищенности.

3. Предлагаемая система показателей защищенности. Рассматриваемая в данной работе система показателей была разработана для подхода к оценке защищенности, который включает следующие этапы: (1) формирование графа атак и зависимостей сервисов на основе данных о топологии сети, (2) учет навыков и позиции нарушителя и формирование профильных графов атак, (3) анализ происходящих в системе событий для отслеживания текущей ситуации по безопасности, (4) вычисление показателей защищенности на основе этих данных [12, 13].

Для представления данных по безопасности предлагается использовать протокол SCAP [2]. Протокол включает ряд спецификаций, предназначенных для стандартизации управления данными по безопасности. В рамках рассматриваемой системы анализа защищенности используются следующие стандарты, входящие в состав SCAP: «Общее перечисление конфигураций» (Common Configuration Enumeration, CCE) для определения топологии сети, «Общее перечисление платформ» (Common Platform Enumeration, CPE), «Общие уязвимости и де-

факты» (Common Vulnerabilities and Exposures, CVE) и «Общая система оценки уязвимостей» (Common Vulnerabilities Scoring System, CVSS) для определения характеристик хостов — используются для генерации графа атак и оценивания уязвимостей.

Кроме топологии сети и характеристик хостов, входными данными являются зависимости сервисов (используются для определения распространения ущерба), модель нарушителя, события, происходящие в системе, слабые места системы, которые определяются на основе стандарта «Общее перечисление слабых мест» (Common Weaknesses Enumeration, CWE), и т.п.

К выходным данным, получаемым в результате работы системы анализа защищенности, относятся: графы атак, вычисленные показатели защищенности и реагирования, набор рекомендуемых контрмер. В рамках данной статьи рассматривается только вторая группа выходных данных (а именно, показатели защищенности).

Входные и выходные данные для предлагаемой системы оценки защищенности представлены на рис. 2.

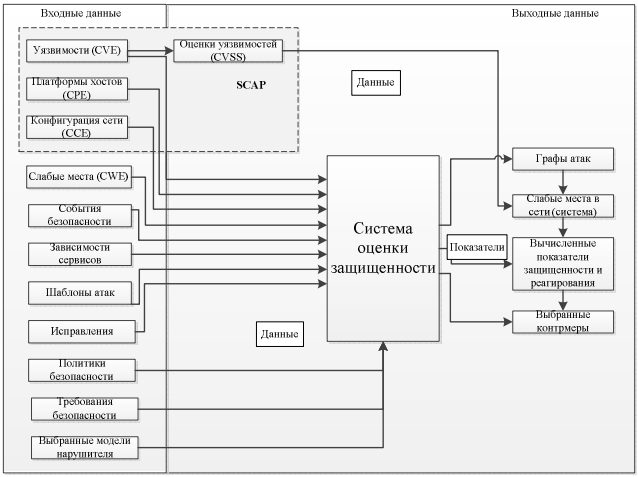

Рис. 2. Входные и выходные данные системы оценки защищенности.

При разработке показателей, помимо существующих исследований в данной области, и архитектуры предлагаемой системы оценки защищенности, учитывались возможные режимы работы системы: реального времени и статический (offline). Первый накладывает ограничения на время вычислений, что приводит к необходимости их упрощения. Однако он позволяет учитывать текущую ситуацию по безопасности (со-

бытия, конфигурацию системы и т.п.) и более точно определять направление развития атаки.

Второй не имеет временных ограничений. В этом случае могут использоваться исторические данные, и полностью строиться и анализироваться общий граф атак и зависимости сервисов. Такой режим позволяет осуществлять более полную оценку.

На основе приведенных выше аспектов, можно выделить следующие уровни предлагаемой системы оценки защищенности с соответствующими показателями: топологический уровень, уровень графа атак, уровень нарушителя, уровень событий и уровень системы.

Показатели топологического уровня определяются администратором на основе топологии системы. Предлагается использовать следующие показатели: уязвимость хоста, критичность хоста, уязвимость хоста к атакам нулевого дня.

На уровне графа атак при генерации показателей защищенности учитывается информация из графа атак. Предлагается использовать показатели вероятности атаки и ущерба от атаки.

На уровне нарушителя вводится зависимость от профиля нарушителя (включая его местоположение и навыки), что позволяет сформировать профильный граф атак [6], включающий только те атаки, которые может реализовать данный нарушитель.

Уровень событий актуален в случае работы системы оценки защищенности в реальном времени. Он позволяет отслеживать развитие атаки и профиль нарушителя согласно поступающим событиям. При появлении новых событий можно корректировать текущее местоположение нарушителя (хост и права доступа) на графе атак и возможные пути атаки (включая наиболее вероятные), и получать таким образом более точное представление о развитии атаки.

И, наконец, на уровне системы определяется общий уровень защищенности системы и поверхность атаки. Подход к вычислению данных показателей зависит от учитываемых параметров и отличается для всех вышестоящих уровней.

На рис. 3 приведены перечисленные уровни и их связь с соответствующими показателями защищенности.

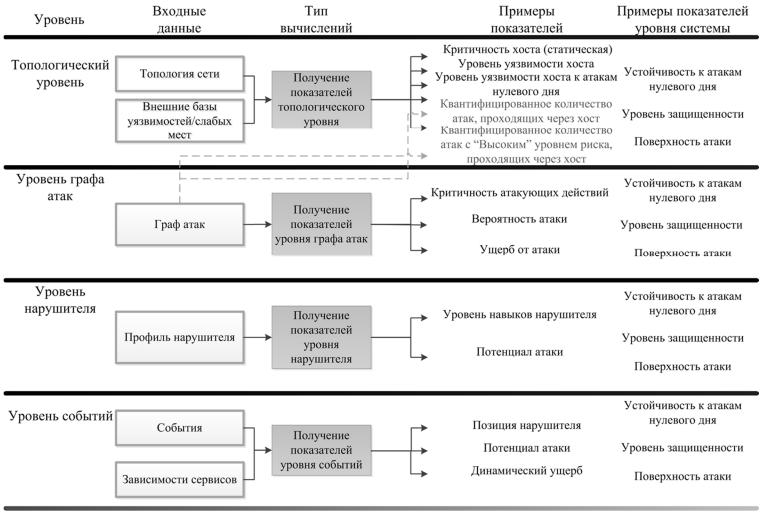

Рис. 3. Показатели защищенности и уровни оценки.

4. Предлагаемые методики оценки риска. На основе аспектов, приведенных в третьем разделе, было выделено три методики оценки риска

1) статическая методика экспресс оценки уровня защищенности;
2) основанная на поведении динамическая методика;
3) методика, основанная на исторических данных.

Первая методика — статическая методика экспресс оценки — объединяет качественный и количественный подходы к оценке рисков и позволяет определить общий уровень защищенности системы. Риск определяется как результат вероятности угрозы и последствий ее реализации для системы. В данном подходе предлагается использовать CVSS (для определения критичности атакующих действий) и методику FRAP (Facilitated Risk Analysis Process) [19].

Методика включает определение уровней критичности хостов и атакующих действий, вычисление ущерба от реализации атакующих действий, на их основе находится ущерб от реализации угроз и сложность их реализации, затем вычисляется уровень риска для всех угроз, и на его основе — общий уровень защищенности системы. На рис. 4 представлены основные этапы методики и соответствующие показатели защищенности.

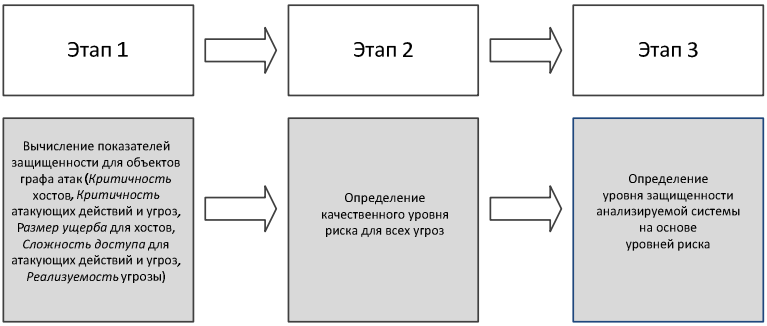

Рис. 4. Основные этапы методики экспресс оценки уровня защищенности.

Основной особенностью методики, основанной на поведении системы, является тот факт, что она ориентирована на работу в реальном времени.

В рамках данной методики вычисляются как показатели уровня системы, так и дополнительные показатели защищенности, не участвующие в определении интегральных показателей, но полезные для понимания текущей ситуации. К дополнительным показателям можно отнести *Уязвимость хоста*, *Слабость хоста*, *Уязвимость хоста к атакам нулевого дня*, *Процент систем без известных критичных уязвимостей*, *Поверхность атаки*. *Уязвимость хоста* определяется на основе известных уязвимостей хоста и базовой оценки CVSS по следующей формуле:

$$Vulnerability(h_k) = \sum_{i=1}^{n} Critical\_BaseScore(v_i),$$

где

h_k — k-й хост системы (k — номер хоста в системе [1..m]),

$$\begin{cases} Critical\_BaseScore(v_i) = BaseScore(v_i), & \text{если } BaseScore(v_i) \geq 7.0 \\ Critical\_BaseScore(v_i) = 0, & \text{иначе} \end{cases},$$

$BaseScore(v_i)$ — базовая оценка CVSS для уязвимости v_i,

i — количество уязвимостей на хосте, может принимать значения в интервале [1..n].

Для получения значения уязвимости хоста относительно других хостов системы, данное значение нормируется по следующей формуле:

$$N\_Vulnerability(h_k) = \frac{\sum_{i=1}^{n} BaseScore(v_i)}{\max_k Vulnerability(h_k)} \cdot 100\%.$$

Слабость хоста определяется на основе стандартов “Общее перечисление слабых мест” (Common Weakness Enumeration, CWE) и “Общая система оценки слабых мест” (Common Weaknesses Scoring System, CWSS) по следующей формуле:

$$Weakness(h_k) = \sum_{i=1}^{n} Critical\_CWSS\_Score(w_i),$$

где

h_k — k-й хост системы (k — номер хоста в системе [1..m]),

$$\begin{cases} Critical\_CWSS\_Score(w_i) = CWSS\_Score(w_i), & \text{если } CWSS\_Score(w_i) \geq 60.0 \\ Critical\_CWSS\_Score(w_i) = 0, & \text{иначе} \end{cases},$$

$CWSS\_Score(w_i)$ — оценка CWSS для слабого места w_i,
i — количество слабых мест на хосте, может принимать значения в интервале [1..n].

Для получения значения слабости хоста относительно других хостов системы, данное значение нормируется по следующей формуле:

$$N\_Weakness(h_k) = \frac{\sum_{i=1}^{n} CWSS\_Score(w_i)}{\max_k Weakness(h_k)} \cdot 100\%.$$

Для вычисления *Уязвимости хоста к атакам нулевого дня* предлагается использовать следующую формулу (основанную на предположении, что чем слабее хост, тем выше вероятность наличия на нем неизвестных уязвимостей):

$$Z\_Vulnerability(h_k) = N\_Weakness(h_k).$$

Уязвимость системы к атакам нулевого дня можно определить следующим образом:

$$Z\_Vulnerability = \frac{\sum_{\mathrm{k}} Z\_Vulnerability(h_k)}{\mathrm{k}}.$$

Поверхность атаки определим как все возможные пути развития атаки, исходя из текущего положения нарушителя на графе атак и его навыков.

И, наконец, *Процент систем без известных критичных уязвимостей* (под критичными понимаются уязвимости для которых базовая оценка CVSS «Высокая») определим следующим образом:

$$\frac{\text{Количество хостов без известных критичных уязвимостей}}{\text{Общее количество хостов}} \cdot 100\%.$$

На рис. 5 представлены основные модули системы оценки защищенности, ответственные за предложенную методику, входные данные и связи между ними.

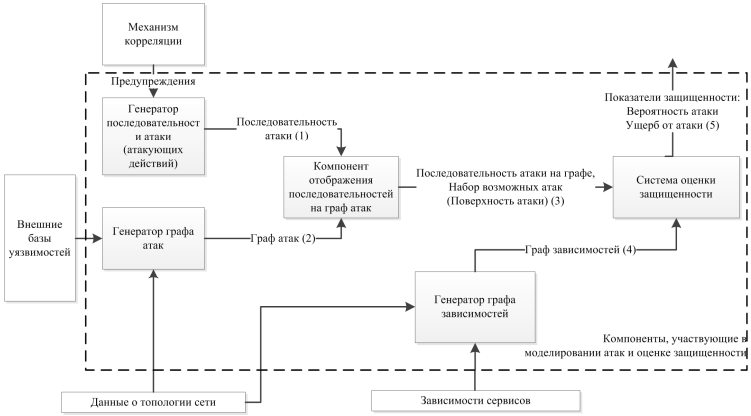

Рис. 5. Входные данные и основные модули системы оценки защищенности.

Основными этапами данной методики являются

1) генератор последовательности атаки строит последовательность атаки на основе предупреждений от механизма корреляции;
2) генератор графа атак формирует граф возможных атак на основе данных об известных уязвимостях и топологии системы;
3) компонент отображения последовательностей на граф атак отображает последовательность атаки (сгенерированной на этапе 1) на граф атак (сгенерированный на этапе 2) для определения реализуемой последовательности и позиции нарушителя на графе атак;
4) генератор графа зависимостей строит граф зависимостей сервисов на основе данных о зависимостях сервисов в анализируемой сети;
5) система оценки защищенности вычисляет набор показателей защищенности на основе графа атак, определенной позиции нарушителя, набора реализованных шагов и графа зависимостей сервисов.

В самом общем виде методика расчета интегрального показателя *Уровень риска* выглядит следующим образом. *Уровень* риска атаки определяется как произведение вероятности успешной реализации ата-

ки на ущерб в случае успешной реализации атаки. Вероятность успешной реализации атаки определяется исходя из навыков нарушителя (определяются на основе уровня сложности реализованных атакующих действий), надежности информации о событиях безопасности (свойство системы обнаружения вторжений), критичности атаки (определяется на основе базовой оценки CVSS) и потенциала атаки (определяется как отношение уже реализованных шагов атаки к общему количеству шагов в атаке). Ущерб в случае успешной реализации атаки включает собственный ущерб (определяется на основе CVSS) и распространенный ущерб (определяется с использованием зависимостей сервисов). Полученный в результате уровень риска используется для принятия решения о необходимости реагирования.

Методика, основанная на исторических данных, отличается от методики, основанной на поведении системы тем, что при вычислении вероятности атаки используются данные о предыдущих инцидентах.

5. Заключение. В настоящей работе рассмотрены основные исследования в области показателей защищенности и выделены классы показателей. На основе предложенной классификации, а также особенностей архитектуры системы анализа защищенности и режимов функционирования анализируемой системы сформирована система показателей защищенности. Предложены методики расчета показателей, предполагаемые для реализации в рамках системы оценки защищенности.

В настоящее время в рамках общей системы оценки защищенности выполняется реализация предложенных методик. Направления будущих исследований связаны с уточнением и расширением предложенных показателей и методик, тестированием системы оценки защищенности на реальных примерах и анализом эффективности оценки защищенности.

Литература

1. *Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А.* Технологии управления информацией и событиями безопасности для защиты компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. 2012, № 2. С.57–68.
2. *Котенко И.В., Дойникова Е.В.* Анализ протокола автоматизации управления данными безопасности SCAP // Защита информации. Инсайд, 2012, № 2, С.56-63.
3. *Ahmed M.S., Al-Shaer E., Khan L.* A novel quantitative approach for measuring network security // Proceedings of the 27th Conference on Computer Communications (INFOCOM'08). 2008. P. 1957–1965.
4. *Blakely B.A.* Cyberprints Identifying cyber attackers by feature analysis. Doctoral Dissertation: Iowa State University. 2012.
5. The Center for Internet Security, The CIS Security Metrics, 2009.

6. *Dantu R., Kolan P., Cangussu J.* Network risk management using attacker profiling // Security and Communication Networks, 2009. Vol.2, No.1. P. 83–96.
7. *Hoo K.J.S.* How much is enough? A risk-management approach to computer security. PhD thesis, Stanford University, CA, 2000.
8. ISO/IEC 27005:2008, Information technology — Security techniques — Information security risk management.
9. *Jahnke M., Thul C., Martini P.* Graph-based metrics for intrusion response measures in computer networks // Proceedings of the 3rd IEEE Workshop on Network Security, held in conjunction with 32th IEEE Conference on Local Computer Networks. Dublin, 2007.
10. *Kanoun W., Cuppens-Boulahia N., Cuppens F., Araujo J.* Automated reaction based on risk analysis and attackers skills in intrusion detection systems // Proceedings of the third International Conference on Risks and Security of Internet and Systems (CRiSIS'08). Toezer, Tunisia, 2008. P. 117–124.
11. *Kheir N., Cuppens-Boulahia N., Cuppens F., Debar H.* A service dependency model for cost-sensitive intrusion response // Proceedings of the 15th European Symposium on Research in Computer Security (ESORICS'10), 2010. P. 626–642.
12. *Kotenko I., Chechulin A.* Attack Modeling and Security Evaluation in SIEM Systems // International Transactions on Systems Science and Applications, SIWN Press. 2013. ISSN 1751-1461.
13. *Kotenko I., Chechulin A.* Common Framework for Attack Modeling and Security Evaluation in SIEM Systems // 2012 IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing. Besançon, France, November 20-23, 2012. Los Alamitos, California. IEEE Computer Society. 2012. P. 94–101.
14. *Kotenko I., Stepashkin M.* Attack graph based evaluation of network security // Proceedings of the 10th IFIP Conference on Communications and Multimedia Security (CMS'2006). Heraklion, Greece, 2006. P. 216–227.
15. *Manadhata P.K., Wing J.M.* An attack surface metric // IEEE Transactions on Software Engineering, 2010. P. 371–386.
16. MASSIF FP7 Project. MAnagement of Security information and events in Service Infrastructures. http://www.massif-project.eu.
17. *Mayer A.* Operational Security Risk Metrics: Definitions, Calculations, Visualizations // Metricon 2.0. CTO RedSeal Systems, 2007.
18. *Mell P., Scarfone K., Romanosky S.* A Complete Guide to the Common Vulnerability Scoring System Version 2.0, 2007.
19. *Peltier T.R.* How to complete a risk assessment in 5 days or less // Auerbach publications, 2008. P. 1–55.
20. *Olsson T.* Assessing security risk to a network using a statistical model of attacker community competence // Proceedings of the 11th international conference on Information and Communications Security, 2009. P. 308–324.
21. *Poolsappasit N., Dewri R., Ray I.* Dynamic security risk management using Bayesian attack graphs // IEEE Transactions on Dependable and Security Computing, 2012. Vol.9, No.1. P.61–74.
22. *Stakhanova N., Basu S., Wong J.* A cost-sensitive model for preemptive intrusion response systems // Proceedings of the 21st International Conference on Advanced Networking and Applications, Washington, DC, USA, IEEE Computer Society, 2007. P. 428–435.
23. *Wang L., Singhal A., Jajodia S., Noel S.* k-zero day safety: measuring the security risk of networks against unknown attacks // Proceedings of the 15th European conference on Research in computer security, Springer-Verlag Berlin, Heidelberg, 2010. P. 573–587.

24. *Wu Y.-S., Foo B., Mao Y.-C., Bagchi S., Spafford E.H.* Automated adaptive intrusion containment in systems of interacting services // Computer Networks: The International Journal of Computer and Telecommunications Networking, 2007. Vol.51. P. 1334–1360.

Дойникова Елена Владимировна — асп. лаборатории проблем компьютерной безопасности СПИИРАН. Область научных интересов: методы оценки рисков компьютерных сетей. Число научных публикаций — 17. elenadoynikova@mail.ru, http://comsec.spb.ru/doynikova; 14-я линия В.О., д.39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328-2642, факс +7(812)328-4450. Научный руководитель — И.В. Котенко.

Doynikova Elena Vladimirovna — Ph.D. student of Laboratory of computer security problems of the Saint-Petersburg institute for information and automation of Russian Academy of Sciences (SPIIRAS). Research interests: information security risk assessment techniques. Number of scientific publication — 17. elenadoynikova@mail.ru, http://comsec.spb.ru/doynikova; 14th Liniya, 39, Saint-Petersburg, 199178, RF; tel. +7(812)328-2642, fax +7(812)328-4450. Scientific adviser — I.V. Kotenko.

Поддержка исследований. В публикации представлены результаты исследований, поддержанных Министерством образования и науки Российской Федерации (государственный контракт 11.519.11.4008), грантами РФФИ, программой фундаментальных исследований ОНИТ РАН и проектами Седьмой рамочной программы Европейского Союза SecFutur и MASSIF.

Рекомендовано лабораторией проблем компьютерной безопасности, заведующий лабораторией Котенко И.В., д. т. н., проф.
Статья поступила в редакцию 02.03.2013.

РЕФЕРАТ

Дойникова Е.В. **Показатели и методики оценки защищенности компьютерных сетей на основе графов атак и графов зависимостей сервисов.**

В статье рассматриваются основные направления исследований в области показателей защищенности. Предложена классификация существующих показателей, включающая топологические характеристики (такие как *Критичность хоста*, *Процент систем без известных критичных уязвимостей* и т.п.), характеристики нарушителя (такие как *Уровень навыков нарушителя*), характеристики атаки (например, *Потенциал атаки*), интегральные характеристики (*Поверхность атаки* и *Уровень риска*), а также характеристики, связанные со стоимостным анализом и характеристики, используемые при анализе уязвимостей нулевого дня. Эта классификация была положена в основу формирования системы показателей защищенности и методик их расчета, предлагаемых в данной работе.

Помимо существующих исследований, при разработке системы показателей защищенности учитывались особенности архитектуры предлагаемой системы оценки защищенности и возможные режимы работы системы. С точки зрения архитектуры, система обладает следующими особенностями: использование для анализа защищенности графа атак и зависимостей сервисов, применение протокола SCAP и входящих в его состав стандартов для представления данных, анализ происходящих в системе событий безопасности. С точки зрения функционирования системы выделяются режим реального времени и статический режим. Первый накладывает ограничения на время вычислений, однако он позволяет учитывать текущую ситуацию по безопасности (события, конфигурацию системы и т.п.). Второй не имеет временных ограничений и позволяет применять более трудоемкие вычисления и использовать исторические данные.

На основе рассмотренных аспектов предложено выделение пяти уровней системы оценки защищенности с соответствующими показателями: топологический уровень, уровень нарушителя, уровень атаки, уровень событий и уровень системы.

Выделено три методики оценки риска: статическая методика экспресс оценки уровня защищенности, основанная на поведении динамическая методика, методика, основанная на исторических данных. Приведено краткое описание данных методик.

SUMMARY

Doynikova E.V. **Security metrics and security assessment techniques for the computer networks on the base of the attack graphs.**

The paper considers the last researches in the area of the security metrics. Classification of the known metrics is suggested. It includes: topological characteristics (i.e. *Host criticality*, *Percent of systems without known severe vulnerabilities*), attacker characteristics (i.e. *Attacker skill level*), attack characteristics (for example, *Attack potentiality*), integral characteristics (*Attack surface* and *Risk level*), and characteristics related with cost-sensitive analysis and characteristics that are used in analysis of the zero-day vulnerabilities. The classification was used in generation of system of security metrics and appropriate calculation techniques.

Besides, in process of generation of system of security metrics architecture of the proposed system for the security assessment and performance modes of this system were considered. From the architecture point of view there are the next features of the security assessment system: usage of the attack graph and service dependencies graph, application of the SCAP protocol and included standards to the data representation, analysis of the security events in the system. From the performance point of view the next modes are outlined: on-line mode and off-line mode. For the on-line mode time limitations and consideration of system events are typical. It allows to monitor current security situation (security events, system configuration etc.). For the off-line the absence of time limitations is typical. This allows performing more complex and accurate computations.

On the base of the considered aspects five levels of the security assessment system with appropriate security metrics were outlined: topological level, malefactor level, attack level, events level and system level.

Three risk assessment techniques were proposed and described: cstatic express risk assessment technique, performance-based (dynamic) technique and technique based on the historical data.