УДК 004.056

И.В. Котенко, Е.В. Дойникова, А.А. Чечулин

ДИНАМИЧЕСКИЙ ПЕРЕРАСЧЕТ ПОКАЗАТЕЛЕЙ ЗАЩИЩЕННОСТИ НА ПРИМЕРЕ ОПРЕДЕЛЕНИЯ ПОТЕНЦИАЛА АТАКИ

Котенко И.В., Дойникова Е.В., Чечулин А.А. **Динамический перерасчет показателей защищенности на примере определения потенциала атаки.**
Аннотация. Анализ информационных рисков и вычисление показателей защищенности являются важными задачами для систем управления информацией и событиями безопасности (Security Information and Events Management, SIEM). Они позволяют определить текущую ситуацию в области защищенности и необходимые контрмеры. Данная статья рассматривает методику вычисления показателей защищенности во времени, близком к реальному, и демонстрирует ее применение на примере перерасчета потенциала атаки.
Ключевые слова: кибербезопасность, показатели защищенности, оценивание риска, графы атак, графы зависимостей сервисов.

Kotenko I.V., Doynikova E.V., Chechulin A.A. **Dynamical recalculation of the security metrics on the example of attack potentiality.**
Abstract. Analysis of security risks and calculation of security metrics is an important task for Security Information and Events Management (SIEM) systems. It allows recognizing the current security situation and necessary countermeasures. The paper considers a technique for calculation of the security metrics in the near real time and demonstrates it on the example of the recalculation of the attack potentiality.
Keywords: cyber security, security metrics, risk assessment, attack graphs.

1. Введение. В настоящее время растет интерес к SIEM-системам [1, 14, 19]. Такие системы способны быстро и четко обрабатывать информацию для эффективного реагирования на инциденты безопасности. Анализ информационных рисков и вычисление показателей защищенности является важной задачей для SIEM-систем. Он позволяет определить текущую ситуацию по защищенности, а также необходимость и вид реагирования.

Для адекватного отражения текущей ситуации по безопасности, при расчете показателей защищенности необходимо учитывать новую информацию, поступающую в реальном времени.

В рамках данной статьи была поставлена цель сделать процесс оценивания защищенности системы более гибким, т.е. предоставить возможность пересчета показателей в зависимости от заданных условий (таких как режим функционирования системы, наличие исторических данных об инцидентах, знания об атакующем, и т.п.).

Основной вклад статьи состоит в описании методики динамического пересчета потенциала атаки на примере тестовой компьютерной сети. Предложенная методика является частью компонента моделирования атак и оценивания защищенности (Attack Modelling and Security Evaluation component, AMSEC) [13, 16] SIEM-системы, разработанной в рамках проекта MASSIF (Management Security and information in Service Infrastructures) [19].

Статья организована следующим образом. Во втором разделе приведены релевантные работы в области графов атак и показателей защищенности. В третьем разделе кратко описывается предлагаемый подход к моделированию атак для оценивания защищенности и подход к перерасчету показателей на примере определения вероятности атаки. В четвертом разделе приведен пример расчетов для тестовой компьютерной сети. В заключении представлены основные результаты работы.

2. Релевантные работы. Описываемый в работе подход к моделированию атак основан на отображении сценариев атак в виде графов. Вопросы, посвященные построению и анализу графов и деревьев атак, рассмотрены в [6, 22, 25].

Показатели защищенности являются важным элементом систем оценивания защищенности, в том числе систем, основанных на графах атак. Они применяются при решении следующих важных задач: (1) определение текущей ситуации в области защищенности и (2) поддержка принятия решений в области выбора и оценивания возможных контрмер. Различные виды показателей рассмотрены в работах [2–5, 7–11, 17, 18, 20, 23, 24, 27, 28].

Одним из ключевых показателей при оценивании уровня защищенности компьютерной сети является показатель, характеризующий потенциал атаки. Методики его вычислений представлены в [10, 17, 24, 26, 28]. В [10] потенциал атаки определяется на основе динамических графов атак с учетом событий безопасности. В [17] предложен статический подход к качественному вычислению показателя на основе сложности шагов атаки в графе атак. В [24] обосновывается динамический подход к перерасчету показателя потенциала атаки на основе байесовских графов атак. В [26] рассмотрен пример расчета показателя на основе количества выполненных атакующим шагов и количества оставшихся до цели шагов. В [28] при расчете потенциала атаки учитываются как события безопасности, так и исторические данные об инцидентах безопасности.

Отличие подхода, предлагаемого в данной работе, состоит в выделении различных уровней расчета показателей в соответствии с процессом функционирования системы и использовании различных методик на разных уровнях. Такой подход позволяет иметь актуальную оценку показателей, соответствующую новой информации о ситуации по безопасности, поступающей во времени, близком к реальному. Работа методики рассмотрена на примере расчета потенциала атаки для тестовой компьютерной сети.

3. Среда оценивания защищенности и методика вычисления показателя потенциала атаки. Общий подход к моделированию атак и оцениванию защищенности, реализованный в AMSEC, основывается на моделировании поведения атакующего, генерации графов атак и зависимостей сервисов, вычислении различных показателей защищенности и предоставлении процедур всестороннего анализа рисков [12–17].

Общий процесс оценивания защищенности делится на три этапа: (1) сбор входной информации; (2) построение графов атак; (3) вычисление показателей защищенности. Первые два этапа были рассмотрены в работах [13–15]. Методика вычисления показателей, включая систему показателей защищенности, была подробно рассмотрена в [12]. В данной статье рассматриваются возможности методики, связанные с динамическим пересчетом показателей во времени, близком к реальному.

AMSEC имеет два режима функционирования: оф-лайн (статический) и он-лайн (динамический) [13– 15].

В статическом режиме входными данными для вычисления показателей являются топология сети, описание установленного программного обеспечения (ПО), данные об известных уязвимостях, а также сгенерированные графы атак и модели атакующих.

В динамическом режиме данными для пересчета показателей служат обработанные события и сигналы тревоги.

Чтобы продемонстрировать идею динамического пересчета показателей, остановимся на показателе *Потенциал Атаки*. Он относится к показателям уровня графа атак [1].

Потенциал Атаки может рассчитываться статически, на основе максимальной сложности доступа на различных шагах атаки [17]:

$$Potentiality(T) = \begin{cases} Высокая, AccessComplexity(T) = Низкая; \\ Низкая, AccessComplexity(T) = Высокая, \end{cases}$$

где T – набор атакующих действий; $AccessComplexity(T)$ – максимальная сложность доступа шагов атаки, вычисляемая на основе показателей “Общей системы оценивания уязвимостей” (Common Vulnerabilities Scoring System, CVSS) [21].

Потенциал Атаки также может оцениваться динамически, на основе количества реализованных шагов атаки и общего количества шагов до цели [26]: (*Количество реализованных шагов*)/(*Общее количество шагов атаки*).

В данной работе, для вычисления *Потенциала Атаки* была выбрана модификация подхода, предложенного в [24], так как в зависимости от имеющихся в наличии данных, он может использоваться как в статическом режиме, так и в режиме, близком к реальному времени, и дает более точную количественную оценку показателя.

Общая идея методики пересчета показателя в рамках предлагаемой методики представлена на рис. 1. При расчетах учитываются уровень навыков атакующего, вероятность успешного использования уязвимостей, вычисляемая на основе CVSS, и теорема Байеса:

- каждое состояние определяется как узел графа атак, с учетом его пред- и постусловий;
- исходному узлу атаки назначается вероятность, определяемая моделью атакующего (0.7 для Высокого *Уровня Навыков Атакующего*, 0.5 для Среднего *Уровня Навыков Атакующего*, 0.3 для Низкого *Уровня Навыков Атакующего*);

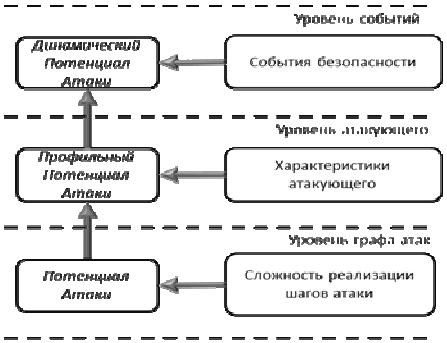

Рис. 1. Изменения показателя *Потенциал Атаки* в зависимости от учитываемых данных.

- вероятность перехода от одного узла к другому определяется сложностью доступа соответствующей уязвимости (если существует несколько уязвимостей, ведущих к данному состоянию –

вероятность определяется минимальной сложностью доступа): $\Pr(e_i) = CVSS\_AC$, где $CVSS\_AC$ - сложность доступа CVSS; e_i - используемая уязвимость;

- для каждого узла вычисляются локальные распределения вероятностей. На их основе вычисляются безусловные вероятности состояний по формуле совместного распределения вероятностей: для набора состояний $S = \{S_1, ..., S_n\}$, $\Pr(S_1, ..., S_n) = \prod_{i=1}^{n} \Pr(S_i \mid \mathrm{Pa}[S_i])$, где $\mathrm{Pa}[S_i]$ - набор всех предков S_i [30].

Эти шаги соответствуют уровню графа атак на рис. 1.

На следующем уровне, уровне атакующего, вводится показатель *Уровень Навыков Атакующего*. На основе данного показателя *Потенциал Атаки* пересчитывается, формируя новый показатель *Профильный Потенциал Атаки*. Новые данные на уровне событий, соответствующем он-лайн режиму работы AMSEC, также позволяют откорректировать показатели. Например, информация о реализованных атакующих действиях позволяет судить о навыках атакующего и пересчитать показатель *Уровень Навыков Атакующего*. Также информация, содержащаяся в событиях безопасности, позволяет пересчитывать вероятности реализации атакующих действий на основе теоремы Байеса (определяющей апостериорную вероятность события S_1 при условии, что S_2 произошло [24]):

$$\Pr(S_1 \mid S_2) = \Pr(S_2 \mid S_1) \times \Pr(S_1) / \Pr(S_2),$$

где $\Pr(S_1)$, $\Pr(S_2)$ - априорные безусловные вероятности событий S_1 и S_2.

Это дает возможность откорректировать показатель *Потенциала Атаки*, сформировав новый показатель *Динамического Потенциала Атаки* (уровень событий на рис. 1).

4. Тестовый пример. Рассмотрим изменение значения показателя *Потенциал Атаки* во времени на примере вычислений для тестовой компьютерной сети. На рис. 2 изображены взятые для примера пути атак и соответствующие уязвимости хостов сети: (1) Внешний пользователь с ноутбуком → Шлюз → Внешний маршрутизатор → Межсетевой экран → Внутренний маршрутизатор 1 → Хост-1 (CVE-2001-1572, CVE-2006-0038); (2) Внешний пользователь с ноутбуком → Шлюз → Внешний маршрутизатор → Межсетевой экран → Внутренний маршрутизатор 1 → Хост-1 → Хост-2 (CVE-2001-1572,CVE-2006-0038,CVE-

2013-0073); (3) Внешний пользователь с ноутбуком → Шлюз → Внешний маршрутизатор → Межсетевой экран → Внутренний маршрутизатор 1 → Хост-1 → Хост-3 (CVE-2001-1572,CVE-2006-0038,CVE-2013-0073).

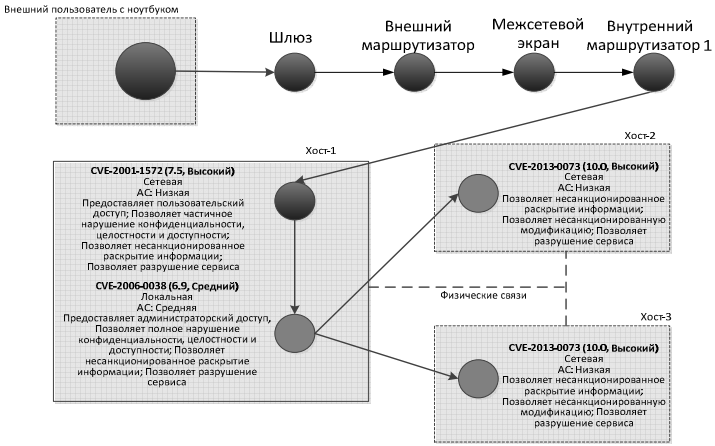

Рис. 2. Пример путей атаки.

Потенциал Атаки (на уровне графа атак) может быть определен следующим образом. На данном этапе не будем учитывать *Уровень Навыков Атакующего*, и определим исходную вероятность атаки как 1. Рассмотрим пути атаки (1) – (3), представленные выше на рис. 2.

Атакующий начинает с узла: Внешний пользователь с ноутбуком. Атакующий проходит Шлюз, Внешний маршрутизатор, Межсетевой экран и Внутренний маршрутизатор 1 (данный отрезок пути не рассматривается при вычислениях) до межсетевого экрана (Хост-1) и хоста Хост-2 или до хоста Хост-3 и может скомпрометировать их свойства безопасности (конфиденциальность, целостность, доступность).

Определим узлы, соответствующие использованию уязвимостей данных хостов следующим образом: A - CVE-2013-0073; B - CVE-2006-0038; C - CVE-2001-1572; D – Внешний пользователь с ноутбуком.

Определим вероятности успешного использования уязвимостей атакующим (согласно формулам, приведенным в разделе 3): $e_A = 0,71$; $e_B = 0,61$; $e_C = 0,71$.

На основе априорной вероятности атаки и вероятностей успешного использования уязвимостей определим локальные распределения условных вероятностей:

узел D: $\Pr(\mathrm{D}) = 1$ (учитывая, что вероятность того, что атакующий начнет атаку, равна 1), $\Pr(\neg \mathrm{D}) = 0$;

узел C: для $D = 1$ - $\Pr(C) = 0,71$ (т.к. вероятность успешного использования уязвимости $e_C = 0,71$), $\Pr(\neg C) = 0,29$; для $D = 0$ - $\Pr(C) = 0$, $\Pr(\neg C) = 1$;

узел B: для $C = 1$ - $\Pr(B) = 0,61$ (т.к. вероятность успешного использования уязвимости $e_B = 0,61$), $\Pr(\neg B) = 0,39$; для $C = 0$ - $\Pr(B) = 0$, $\Pr(\neg B) = 1$;

узел A: для $B = 1$ - $\Pr(A) = 0,71$ (т.к. вероятность успешного использования уязвимости $e_A = 0,71$), $\Pr(\neg A) = 0,29$; для $B = 0$ - $\Pr(A) = 0$, $\Pr(\neg A) = 1$.

Далее определим безусловные вероятности для каждого узла. Для узла D есть только одно успешное состояние: $\Pr(\mathrm{D}) = 1$. Для узла C необходимо учесть успех на узле D: $\Pr(C) = 1 \cdot 0,71 = 0,71$. Для узла B необходимо учесть успех на узле C: $\Pr(B) = 0,71 \cdot 0,61 = 0,4331$. Для узла A необходимо учесть успех на узле B: $\Pr(A) = 0,4331 \cdot 0,71 = 0,3075.$ Таким образом, *Потенциал Атаки* компрометации узла Хост-1 равен $\Pr(\mathrm{B}) = 0,4331$. *Потенциал Атаки* компрометации узла Хост-2 равен *Потенциалу Атаки* компрометации узла Хост-3 и равен $\Pr(A) = 0,3075$.

Теперь рассмотрим влияние на *Потенциал Атаки* показателя *Уровень Навыков Атакующего*. Определим *Уровень Навыков Атакующего* как средний (что соответствует количественному значению 0,5). Т.о. исходная вероятность атаки на узел D: $\Pr(\mathrm{D}) = 0,5$.

Остальные оценки изменятся следующим образом: для узла D - $\Pr(\mathrm{D}) = 0,5$; для узла C - $\Pr(C) = 0,5 \cdot 0,71 = 0,355$; для узла B - $\Pr(B) = 0,355 \cdot 0,61 = 0,2166$; для узла A - $\Pr(A) = 0,2166 \cdot 0,71 = 0,1538.$ Таким образом, очевидно, что снижение

Уровня Навыков Атакующего ведет к снижению вероятности атаки на узел A.

Профильный Потенциал Атаки для узла Хост-1 равен $\Pr(B) = 0,2166$. *Профильный Потенциал Атаки* для узла Хост-2 равен *Профильному Потенциалу Атаки* для узла Хост-3 и равен $\Pr(A) = 0,1538$.

На следующем этапе экспериментов проводится обработка событий безопасности. AMSEC анализирует события безопасности и вычисляет вероятности возможных будущих и предыдущих действий атакующего. Простое отображение события безопасности, которое может анализироваться AMSEC, содержит три поля: хост источника, хост назначения и тип атаки. Пример события безопасности:

192.168.1.212 192.168.1.2 SCAN nmap TCP {tcp}.

Это событие содержит информацию об обнаружении процесса сканирования портов (разведывательная стадия атаки). Прокси-сервер 192.168.1.2 был просканирован инструментом Nmap с пользовательского хоста во внешней сети 192.168.0.1/8. Если в отчете по событиям безопасности нет информации о других атакующих действиях, AMSEC делает вывод, что с высокой степенью вероятности в сети обнаружен внешний атакующий.

Предположим, что поступило событие безопасности об успешной компрометации узла B. Пересчитаем *Потенциал Атаки* на основе теоремы Байеса, чтобы получить *Динамический Потенциал Атаки* на уровне событий. Определим апостериорную вероятность для узла C, с учетом того, что B произошло. Априорные безусловные вероятности узлов B и C были вычислены выше: $\Pr(B) = 0,2166$, $\Pr(C) = 0,355$. $\Pr(B \mid C) = 0,61$. Тогда: $\Pr(C \mid B) = 0,61 \times \frac{0,355}{0,2166} = 0,9999$, таким образом, вероятность C значительно возросла, при условии того, что B произошло.

На рис. 3 показаны изменения *Потенциала Атаки* для пути атаки (1) (см. рис. 2) при добавлении информации различных уровней показателей защищенности. Новая информация об уровне навыков атакующего снижает значение показателя, т.к. атакующий не может использовать все уязвимости (из-за недостатка знаний). На уровне событий значение показателя растет из-за обнаружения нового события. Это позволяет делать предположения о предыдущих и последующих шагах атаки (с учетом критичности хостов на пути атакующего). Также на основе

сложности предыдущих шагов и направления атаки можно делать предположения об уровне знаний атакующего.

Рис. 3. Изменения значения *Потенциала Атаки*.

5. Заключение. В статье представлена методика оценивания защищенности на основе графов атак, которая учитывает профили атакующих и события безопасности. Методика объединяет различные подходы к расчету показателей защищенности и позволяет пересчитывать их в зависимости от учитываемой информации. Описан пример пересчета показателя, характеризующего потенциал атаки, для тестовой компьютерной сети. Представленная методика может быть использована в SIEM-системах для адекватного расчета показателей 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. № 2, 2012. С. 57–68.
2. *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.
3. *Blakely B.A.* Cyberprints Identifying cyber attackers by feature analysis. Doctoral Dissertation: Iowa State University. 2012.
4. CIS Security Metrics. The Center for Internet Security, , 2009.
5. *Dantu R., Kolan P., Cangussu J.* Network risk management using attacker profiling // Security and Communication Networks, 2009. Vol.2, No.1. P. 83–96.
6. *Dawkins J., Campbell C., Hale J.* Modeling network attacks: Extending the attack tree paradigm // Proceedings of the Workshop on Statistical and Machine Learning Techniques in Computer Intrusion Detection, Johns Hopkins University, 2002.
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., Doynikova E.* Security metrics for risk assessment of distributed information systems // The IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2013). Proceedings. Berlin, Germany, September 12-14, 2013. P.646–650.
13. *Kotenko I., Chechulin A.* A Cyber Attack Modeling and Impact Assessment Framework // 5th International Conference on Cyber Conflict 2013 (CyCon 2013). Proceedings. IEEE and NATO COE Publications. 4-7 June 2013, Tallinn, Estonia. 2013. P.119–142.
14. *Kotenko I., Chechulin A., Novikova E.* Attack Modelling and Security Evaluation for Security Information and Event Management // Proceedings of the International Conference on Security and Cryptography (SECRYPT 2012), Rome, Italy, 24-27 July 2012. P. 391-394.
15. *Kotenko I., Chechulin A.* Attack Modeling and Security Evaluation in SIEM Systems // International Transactions on Systems Scie nce and Applications, Vol.8, December 2012. P. 129-147.
16. *Kotenko I., Chechulin A.* Computer Attack Modeling and Security Evaluation based on Attack Graphs // The IEEE 7th International Conference on “Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications” (IDAACS'2013). Proceedings. Berlin, Germany, September 12-14, 2013. P.614-619.
17. *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.
18. *Manadhata P.K., Wing J.M.* An attack surface metric // IEEE Transactions on Software Engineering, 2010. P. 371–386.
19. MASSIF FP7 Project. MAnagement of Security information and events in Service Infrastructures. http://www.massif-project.eu.
20. *Mayer A.* Operational Security Risk Metrics: Definitions, Calculations, Visualizations // Metricon 2.0. CTO RedSeal Systems, 2007.
21. *Mell P., Scarfone K., Romanosky S.* A Complete Guide to the Common Vulnerability Scoring System Version 2.0, 2007.
22. *Moore A. P., Ellison R. J., Linger R. C.* Attack Modeling for Information Security and Survivability // Technical Note CMU/SEI-2001-TN-001. Survivable Systems, 2001.
23. *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.
24. *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.
25. *Schneier B.* Attack Trees – Modeling Security Threats // Dr.Dobbs Journal, December, 1999.
26. *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.
27. *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.
28. *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.

Котенко Игорь Витальевич — д.т.н., проф., заведующий лабораторией проблем компьютерной безопасности СПИИРАН. Область научных интересов: безопасность компьютерных сетей, в том числе управление политиками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, защита программного обеспечения от взлома и управление цифровыми правами, технологии моделирования и визуализации для противодействия кибер–терроризму. Число научных публикаций — более 450. ivkote@comsec.spb.ru, www.comsec.spb.ru; СПИИРАН, 14-я линия В.О., д.39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328–2642, факс +7(812)328–4450.

Kotenko Igor Vitalievich — Ph.D., Dc.Sci., Professor, Head of Laboratory of Computer Security Problems, SPIIRAS. Research interests: computer network security, including security policy management, access control, authentication, network security analysis, intrusion detection, firewalls, deception systems, malware protection, verification of security systems, digital right management, modeling, simulation and visualization technologies for counteraction to cyber terrorism; The number of publications — more 450. ivkote@comsec.spb.ru, www.comsec.spb.ru; SPIIRAS, 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone +7(812) 328–2642, fax +7(812)328–4450.

Дойникова Елена Владимировна — аспирант 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, Laboratory of computer security problems, SPIIRAS. Research interests: information security risk assessment techniques. The 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.

Чечулин Андрей Алексеевич — научный сотрудник лаборатории проблем компьютерной безопасности СПИИРАН. Область научных интересов: безопасность компьютерных сетей, обнаружение вторжений, анализ сетевого трафика, анализ уязвимостей. Число научных публикаций — 70. chechulin@comsec.spb.ru; СПИИРАН, 14-я линия В.О., 39, Санкт-Петербург, 199178, РФ; р.т. +7(812)328–2642, факс +7(812)328–4450. Научный руководитель — И.В. Котенко.

Chechulin Andrey Alexeevich — research scientist, Laboratory of Computer Security Problems, SPIIRAS. Research interests: computer network security, intrusion detection, analysis of

the network traffic, analysis of vulnerability. The number of publications — 70. chechulin@comsec.spb.ru; SPIIRAS, 14-th line, 39, St. Petersburg, 199178, Russia; office phone +7(812) 328–2642, fax +7(812)328–4450. Supervisor — I.V. Kotenko.

Поддержка исследований. В публикации представлены результаты исследований, поддержанные грантами РФФИ (проекты 13–07–13159–офи_м_РЖД, 13–01–00843–а и 11–07–00435–а) и программой фундаментальных исследований ОНИТ РАН (проект 2.2).

Рекомендовано лабораторией проблем компьютерной безопасности, заведующий лабораторией Котенко И.В., д.т.н., проф.
Статья поступила в редакцию 09.09.2013.

РЕФЕРАТ

Котенко И.В., Дойникова Е.В., Чечулин А.А. **Динамический перерасчет показателей защищенности на примере определения потенциала атаки.**

В настоящее время недостаточно статической оценки ситуации по безопасности, важно также динамически отслеживать изменение ситуации и оперативно принимать решения в случае обнаружения атакующих действий. Существует большое количество подходов к расчету показателей защищенности. Однако нет общего подхода, позволяющего гибко адаптироваться к той или иной ситуации. В данной статье рассматривается подход к анализу защищенности, основанный на учете при расчете показателей защищенности новой информации, поступающей в реальном времени. Гибкость подхода обеспечивается выделением различных уровней оценивания, зависящих от используемой при расчете показателей информации, и ее статического или динамического характера.

Предлагаемая методика описывается на примере одного из важных в области оценивания защищенности показателей, показателя потенциала атаки. Авторы рассматривают алгоритм вычисления показателя и его изменения в зависимости от новой информации, поступающей на вход системы оценивания защищенности. В зависимости от типа поступающей информации выделяются различные уровни расчета показателя. На первом уровне, уровне графа атак, учитывается только статическая информации о сложности атакующих действий. На следующем уровне атакующего алгоритм расчета показателя модифицируется для учета информации о характеристиках атакующего. На уровне событий расчеты показателя модифицируются для учета информация о событиях безопасности.

Работа предлагаемой методики рассмотрена на примере расчетов для тестовой компьютерной сети. Показано, как новые данные меняют значение вероятности атаки. Так, при ограничении знаний атакующего, вероятность успешной реализации атаки снижается, а событие, сообщающее о компрометации хоста, увеличивает вероятность атак, проходящих через него, и снижает вероятность несвязанных с данным хостом атак.

SUMMARY

Kotenko I.V., Doynikova E.V., Chechulin A.A. **Dynamical recalculation of the security metrics on the example of attack potentiality.**

Currently static assessment of the information security is not enough. It is important to monitor dynamic changes and make decisions on-the-fly in case of disclosing of the attack actions. There are a lot of approaches to the calculation of the security metrics. But there is not common approach which allows flexibly response on changes in security environment. This paper considers approach to the security analysis which is based on the taking into account real-time information in the process of calculation of security metrics. Flexibility of the approach is provided by the separation of the assessment levels. Levels depend on the considered in the calculations information and its static or dynamic nature.

Suggested technique is described on the example of the important security metric which characterizes attack potentiality. Authors provide algorithm of calculation of the metric and modifications of the algorithm with new input information. According to the input information different assessment levels are defined. On the first attack graph level only static information about complexity of the attack actions is considered. On the next attacker level algorithm of calculation of the attack potentiality metric is modified with information about attack characteristics. On the events level metric calculations are changed with information about security events.

Operation of the suggested technique is analyzed on the example of the calculations for the test computer network. It is shown how new data influence on the attack potentiality value. For example, when attacker skills are limited, potentiality of the successful attack is reduced. On the other hand security event which means that some host is compromised results in increase in potentiality of attacks that go through this host and reduces potentiality of attacks that are not connected with the host.