E.V. Doynikova, I.V. Kotenko, A.A. Chechulin

Dynamic Security Assessment Of Computer Networks In Siem-Systems

Keywords: SIEM-systems, security metrics, security metrics taxonomies, risk assessment technique, attack graphs, service dependencies graphs.

The paper suggests an approach to the security assessment of computer networks. The approach is based on attack graphs and intended for Security Information and Events Management systems (SIEM-systems). Key feature of the approach consists in the application of the multilevel security metrics taxonomy. The taxonomy allows definition of the system profile according to the input data used for the metrics calculation and techniques of security metrics calculation. This allows specification of the security assessment in near real time, identification of previous and future attacker steps, identification of attackers goals and characteristics. A security assessment system prototype is implemented for the suggested approach. Analysis of its operation is conducted for several attack scenarios.

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

ДИНАМИЧЕСКОЕ ОЦЕНИВАНИЕ ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ В SIEM-СИСТЕМАХ

Введение

Необходимость обработки большого количества разнородных данных, связанных с безопасностью, поступающих в реальном времени и постоянно изменяющихся, стала толчком к развитию SIEM-систем. В настоящий момент вопросы построения таких систем являются актуальной и широко исследуемой проблемой [1]. Одной из важных задач в рамках SIEM-систем является предоставление лицу, принимающему решения по безопасности, актуальной и адекватной информации. Такую информацию может предоставить комплексная система показателей защищенности, характеризующих текущее состояние информационной системы на различных уровнях детализации и с учетом разнообразных воздействующих факторов. При этом важно учитывать особенности архитектуры SIEM-систем.

Хотя и существует большое количество исследований в области показателей защищенности, но предлагаемые методики, как правило, ограничиваются детальным исследованием только одного из наборов характеристик атак и их применения для анализа защищенности системы, например, уровнем навыков атакующего, потенциалом атаки, возможным ущербом и т.п. и, кроме того, не учитывают особенности и требования SIEM-систем.

Цель данного исследования состоит в разработке подхода к оцениванию защищенности для SIEM-систем, позволяющего адекватно отразить текущее состояние защищенности системы с учетом доступной информации в режиме, близком к реальному времени.

Для реализации поставленной цели в данном исследовании была разработана таксономия показателей защищенности, методики вычисления соответствующих показателей, подход к оцениванию уровня защищенности системы во времени, близком к реальному. Ключевым элементом предложенного подхода является учет текущей информации по защищенности и событий безопасности. На основе предложенной таксономии

реализован прототип системы оценки защищенности, основанный на предыдущих работах авторов и предлагаемом подходе [2–5].

Работа организована следующим образом. В первом и втором разделах рассмотрены основные направления исследований в области показателей защищенности и таксономий показателей защищенности, и предложена таксономия показателей защищенности для SIEM-систем. В третьем разделе описаны требования к предлагаемому подходу оценивания защищенности и представлены его основные шаги, а также приведена архитектура прототипа, реализующего предлагаемый подход. В четвертом разделе приведен пример применения прототипа и результаты экспериментов. В заключении представлены основные результаты исследования.

Релевантные работы

Показатели защищенности достаточно широко исследуются в работах по анализу рисков.

В ряде работ рассматриваются показатели, вычисляемые на основе информации о составе и топологии сети, такие как характеристики хостов [6], характеристики приложений [7], характеристики, учитывающие информацию о зависимостях сервисов [8]. Другие работы посвящены характеристикам атаки (таким как потенциал/вероятность атаки), определяемым на основе графов атак [9]. Характеристики атакующего рассматриваются в [10]. Интегральные (системные) характеристики включают характеристики, которые определяют общие оценки защищенности системы [11, 12]. В [8] рассматривается применение стоимостных показателей (стоимость ущерба и затраты на реагирование) для поддержки принятия решений по реагированию на инциденты безопасности. В [13] рассматриваются показатели, используемые при анализе возможности атак нулевого дня.

При этом спектр используемых показателей достаточно широк, методики их вычисления отличаются в различных работах, и нет единой системы их применения. Хотя попытки создания таксономий показателей защищенности уже существуют. Так, в ряде работ категории показателей выделяются согласно объектам оценки защищенности, например, категория управления, техническая и организационная категории [14]. В [10] показатели разделены согласно шести бизнес-функциям (в том числе, управление инцидентами, управление уязвимостями и т.п.). В [15] выделяется 8 категорий показателей согласно типу значений показателей (таких как порядковое числительное, количественное числительное и т.п.).

Однако не удалось обнаружить таксономию показателей, основанных на графах атак и применимую для оценивания защищенности в SIEM-системах. В данном исследовании в соответствии с рассмотренными релевантными работами и этапами анализа защищенности была разработана таксономия, представленная на рис. 1.

Таксономия включает следующие категории: показатели топологического уровня (показатели, учитывающие топологию и характеристики хостов сети), показатели уровня графа атак (показатели, рассчитываемые на основе графа атак), показатели уровня атакующего (показатели, рассчитываемые с учетом профиля атакующего), показатели уровня событий (показатели, рассчитываемые с учетом информации о событиях безопасности), и интегральные показатели, отражающие уровень защищенности системы в целом. Каждая категория включает три подкатегории: основные показатели, стоимостные характеристики (рассчитываемые с учетом стоимости ресурсов), характе-

ристики нулевого дня (рассчитываемые с учетом возможности уязвимостей нулевого дня).

Рассматриваемый в данной работе динамический подход к анализу защищенности соответствует уровню событий данной таксономии.

Рис.1. Таксономия показателей защищенности

Предлагаемый подход к динамической оценке защищенности

В рамках SIEM-системы подход к оцениванию защищенности должен удовлетворять следующим требованиям: возможность применения в режиме, близком к реальному времени; возможность учета новой информации по безопасности и событий безопасности, возникающих в процессе функционирования сети; предоставление информации для оператора (в том числе о наличии атаки, уровне навыков и позиции атакующего, предыдущих и последующих шагах атаки и цели атаки) в удобном для анализа виде для поддержки принятия решений по реагированию.

Кроме того, для решения поставленных в исследовании задач были сформулированы следующие требования: учет последних исследований в области показателей защищенности; моделирование шагов атакующего в виде графов атак; совместимость с существующими протоколами и стандартами представления входных данных.

Входными данными для оценивания защищенности являются:

модель оцениваемой сети, включающая характеристики хостов, информацию о ее топологии и зависимостях сервисов и значения топологических показателей;

граф атак (вершины графа соответствуют группам эксплуатируемых уязвимостей, а дуги – переходам между уязвимостями, возможность перехода определяется пред- и постусловиями эксплуатации уязвимостей согласно системе оценивания уязвимостей CVSS [16]), для представления входных данных используются протокол автоматизации управления данными безопасности (Security Content Automation Protocol, SCAP) и стандарты, входящие в его состав;

вычисленные безусловные вероятности для каждого узла графа (определяются на основе локальных распределений условных вероятностей каждого узла S_i графа, $i \in [1, n]$: $Pr(S_1,...,S_n) = \prod_{i=1}^{n} Pr(S_i \mid Pa[S_i])$ $\mathrm{i}\in[1,\mathrm{n}]\ \mathrm{Pr}(\mathrm{S_1},\ldots,\mathrm{S_n}) = \prod_{\mathrm{i=1}}^{\mathrm{n}} \mathrm{Pr}(\mathrm{S_i}|\mathrm{Pa}[\mathrm{S_i}])$, где $\mathrm{Pa}[\mathrm{S_i}]$ – набор всех предков S_i, условные вероятности переходов между узлами определяются на основе индекса CVSS (*Сложность доступа*);

события безопасности, включающие информацию об атакованном хосте и полученных привилегиях и/или ущербе на хосте.

На основе вышесказанного был разработан следующий подход к динамическому оцениванию защищенности системы.

1. Определение позиции атакующего на графе атак на основе события безопасности: (a) определение списка уязвимостей для хоста, описанного в событии; (b) выбор уязвимостей, дающих привилегии и\или приводящих к ущербу, описанному в событии (последующие шаги методики выполняются для узлов, соответствующих эксплуатации выбранных уязвимостей, если условиям не удовлетворяет ни одна уязвимость, то событие определяется как эксплуатация уязвимости нулевого дня).
2. Определение уровня навыков атакующего на основе события безопасности: (a) определение наиболее вероятного пути атаки до узла, соответствующего текущей позиции атакующего (на основе теоремы Байеса); (b) определение узлов выбранного пути, соответствующих уязвимостям с максимальными значениями индекса CVSS *Сложность доступа*; (c) определение уровня атакующего согласно максимальным значениям индекса как «Высокий»/«Средний»/«Низкий» (количественно определим как 0.7, 0.5 и 0.3 соответственно); (d) определение точности оценки уровня атакующего как (количество узлов пути с данным уровнем *Сложности доступа* уязвимостей)/(общее количество узлов пути).
3. Вычисление вероятностей путей атаки, идущих через узел, соответствующий позиции атакующего, с учетом уровня навыков атакующего и того, что вероятность компрометации данного узла стала равна 1.
4. Определение рисков путей атаки, проходящих через скомпрометированный узел на основе критичности целевого узла, ущерба от атаки и вероятности пути атаки. На рис. 2 приведено общее описание методик, используемых для расчета таких показателей как: *Критичность хоста*, *Ущерб от атаки* и *Потенциал атаки* [8, 9].
5. Выбор пути с максимальным значением риска в качестве наиболее вероятного пути атаки, а его конечной точки – как цели атакующего.

Таким образом, результатом работы подхода является профиль атаки, включающий уровень навыков атакующего, путь и цель атаки.

На основе предложенного подхода был реализован прототип компонента оценивания защищенности, архитектура которого представлена на рис. 3.

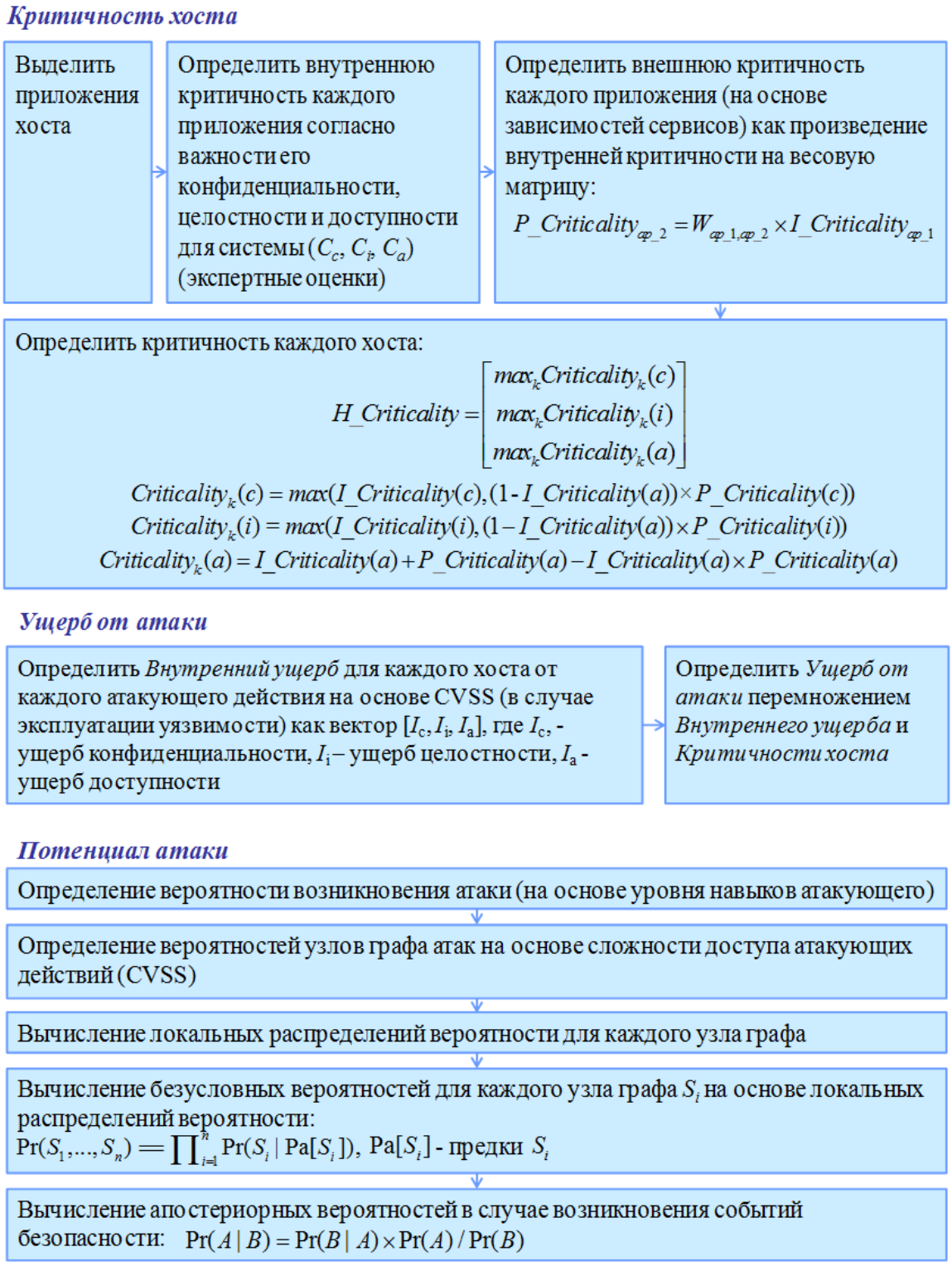

Рис. 2. Методики вычисления показателей, используемых для определения уровня риска атаки

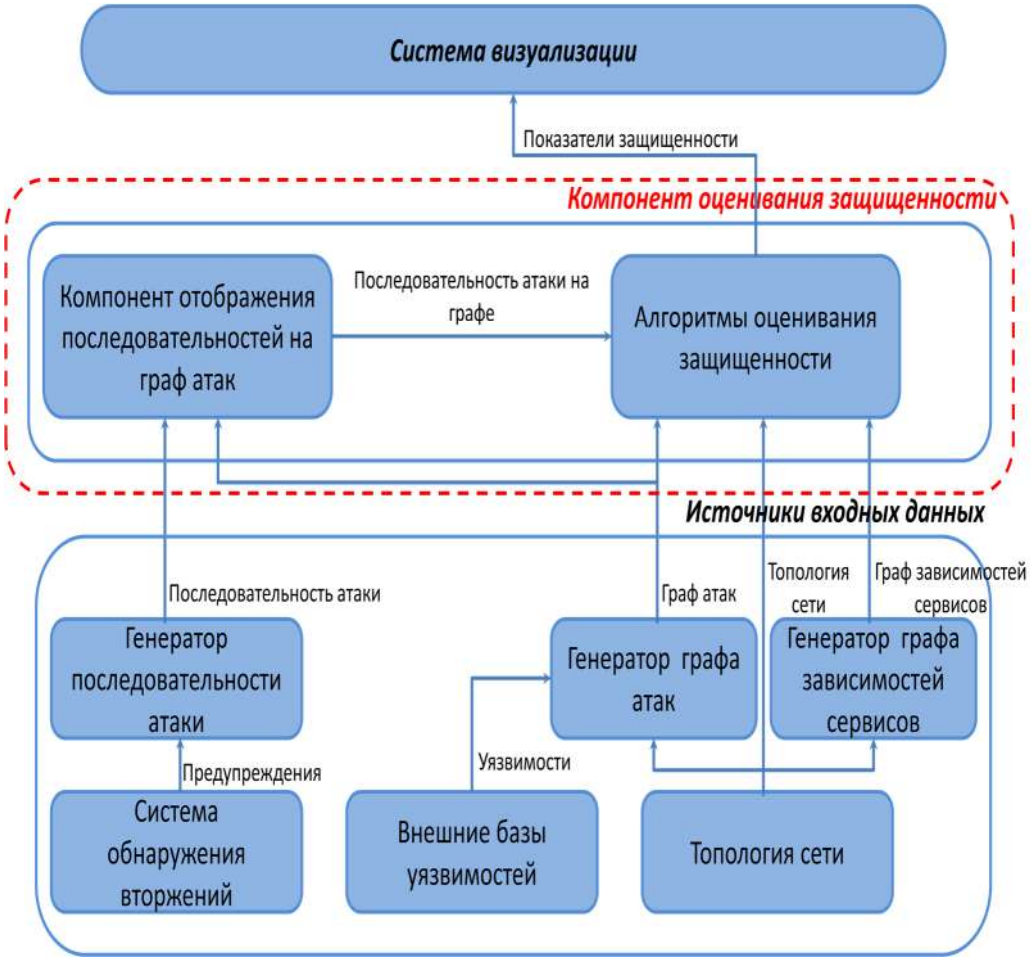

Рис. 3. Архитектура компонента оценивания защищенности

Ядром компонента является набор алгоритмов для вычисления показателей защищенности. Кроме того, важным элементом является компонент отображения последовательностей на граф атак (позволяет определить позицию атакующего на основе событий безопасности и графа атак). Компонент оценивания защищенности получает входные данные от генератора графа атак (строит графы атак для анализируемой сети) [17], генератора графа зависимостей сервисов (формирует граф зависимостей между сервисами сети), и генератора последовательностей атак (генерирует шаги текущей атаки на основе предупреждений от системы обнаружения вторжений). Выходные данные компонента включают вычисленные показатели защищенности в соответствии с предложенной ранее таксономией. Выходные данные передаются для отображения системе визуализации.

Тестовый пример

Для проведения экспериментов использовались следующие входные данные: топология реальной сети Олимпийских игр 2008 г. в Пекине [1] (фрагмент сети приведен на рис.4), значения топологических показателей (в том числе *Критичность* хостов, которая отображена на рис.4 как вектор из трех значений для конфиденциальности, целостности и доступности), граф атак для анализируемой сети, события безопасности.

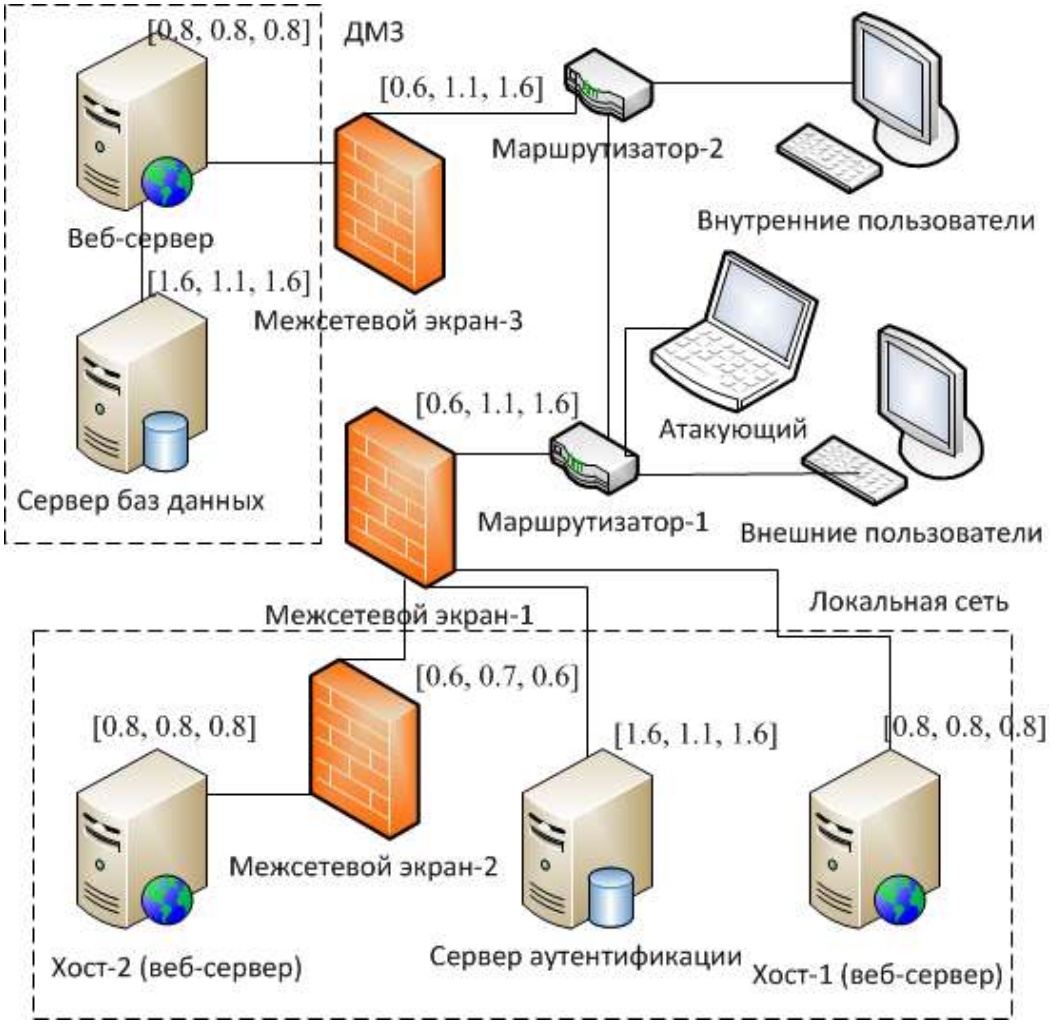

Рис.4. Топология тестовой сети

Был сформирован набор различных профилей атак, включающий: навыки атакующего, путь атаки и цели атаки. Вычисления для каждого профиля проводились для различных наборов событий безопасности. Далее вычисленные значения показателей, формирующих профиль атаки, сравнивались с заданными профилями на различных этапах оценивания (в зависимости от количества событий).

На рис. 5 приведен фрагмент графа атак для сети, изображенной на рис.4. Каждый узел графа соответствует определенной группе уязвимостей хоста (соответствующие хосты обведены рамками). Для каждого узла определено численное значение, соответствующее вероятности достижения постусловий, получаемых при компрометации одной из уязвимостей группы. Сверху представлен заданный профиль атаки (внешний атакующий со средним уровнем навыков, цель которого – получить доступ к информации в базе данных). Шаги атакующего на графе выделены более темным цветом (последний узел пути соответствует группе уязвимостей, которые позволяют нарушить конфиденциальность на сервере баз данных). При этом видно, что исходное распределение вероятностей, без учета событий, не позволяет определить цель атаки. Снизу представлен вычисляемый профиль атаки. Над каждым узлом отображено новое значение показателей вероятности компрометации с поступлением новых событий *c1* и *c2*. В качестве наиболее вероятного направления атаки выбирается маршрут, включающий текущую позицию атакующего и имеющий наибольшее значение вероятности.

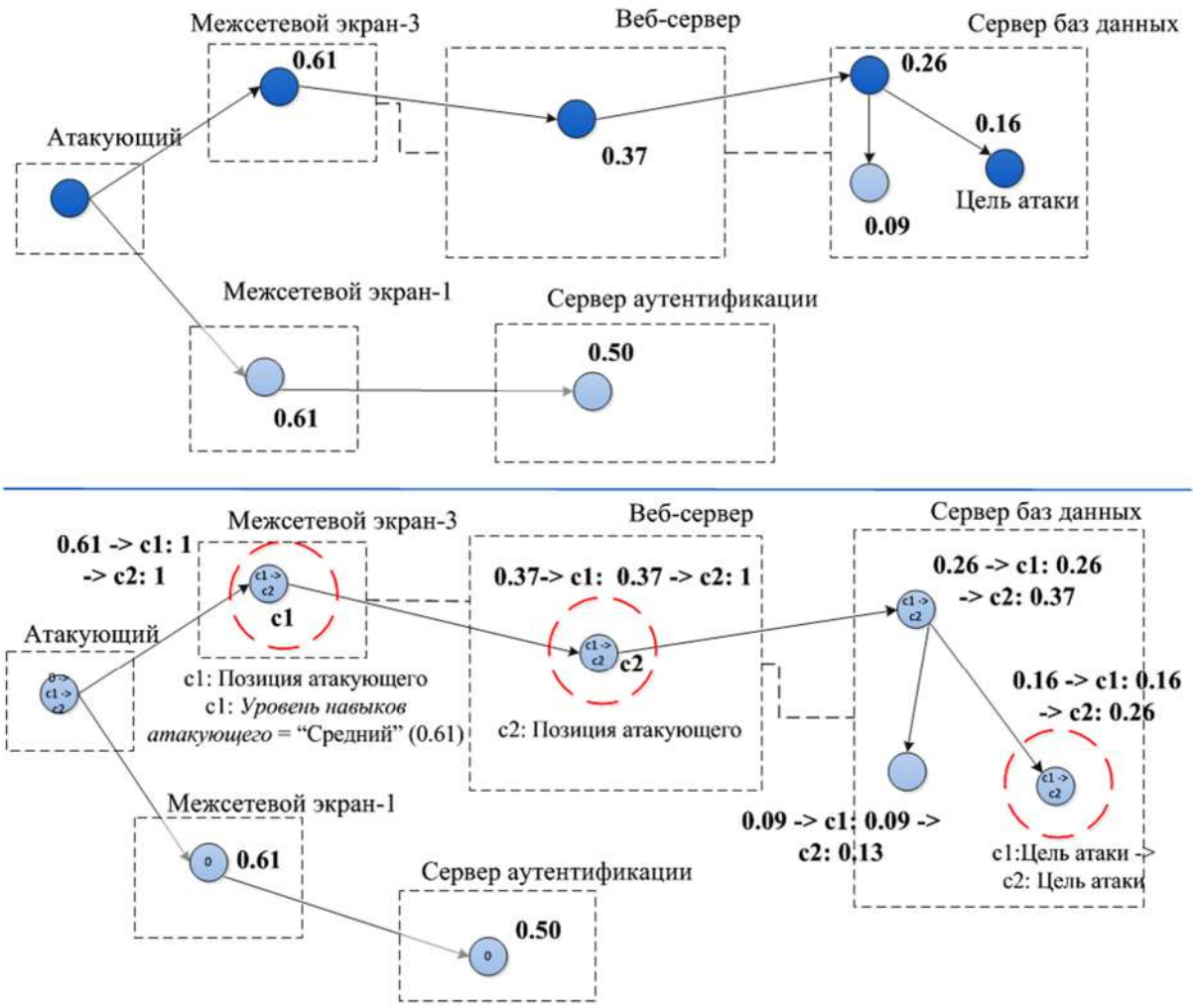

Рис.5. Фрагмент графа атак с вычисленными значениями показателей защищенности

Заключение

В работе предложен подход к динамическому определению уровня защищенности системы. Подход ориентирован на режим, близкий к реальному времени, который позволяет учитывать происходящие в системе события, но имеет ограничения на время анализа. В работе представлен набор показателей защищенности, определяющих профиль защищенности системы, и показано, как учитывается возникновение событий безопасности при вычислении показателей.

В дальнейшем планируется провести большое количество экспериментов на различных сетевых конфигурациях с использованием различных сценариев атак и уточнить подход в соответствии с результатами экспериментов.

Работа выполняется при финансовой поддержке РФФИ (13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417), программы фундаментальных исследований ОНИТ РАН (контракт №2.2), проекта ENGENSEC программы Европейского Сообщества TEMPUS и государственного контракта №14.BBB.21.0097.

СПИСОК ЛИТЕРАТУРЫ:

1. MASSIF FP7 Project. Management of Security information and events in Service Infrastructures. http://www.massif-project.eu.
2. Kotenko I., Stepashkin M. Network Security Evaluation based on Simulation of Malefactor's Behavior // SECRYPT 2006. International Conference on Security and Cryptography. Proceedings. Portugal. 7-10 August 2006. P.339-344.
3. 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.
4. 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, September 11-14, 2012. Los Alamitos, California. IEEE Computer Society. 2012. P. 94-101.
5. Ruiz J.F., Harjani R., Maña A., Desnitsky V., Kotenko I., Chechulin A. A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components // Proceedings - 20th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, PDP 2012 20th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, PDP 2012. Garching, 2012. C.261-268.
6. *Mayer A*. Operational Security Risk Metrics: Definitions, Calculations, Visualizations // Metricon 2.0. CTO RedSeal Systems, 2007.
7. The Center for Internet Security, The CIS Security Metrics, 2009.
8. *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.
9. *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.
Dantu R., Kolan P., Cangussu J. Network risk management using attacker profiling // Security and Communication Networks, 2009. Vol.2, No.1. P. 83–96.
10. *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.
11. *Manadhata P.K.*, *Wing J.M.* An attack surface metric // IEEE Transactions on Software Engineering, 2010. P. 371-386.
12. *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.
13. *Swanson M.*, *Bartol, N.*, *Sabato J.*, *Hash J.*, *Graffo L.* Security Metrics Guide for Information Technology Systems. NIST Special Publication 800-55, Jul. 2003.
14. *Axelrod C. W.* Accounting for Value and Uncertainty in Security Metrics. Information Systems Control Journal, 2008. Vol.6, P.1-6.
15. *Mell P.*, *Scarfone K.*, *Romanosky S.* A Complete Guide to the Common Vulnerability Scoring System Version 2.0, 2007.
16. *Kotenko I.*, *Chechulin A.* A Cyber Attack Modeling and Impact Assessment Framework // Proceedings of the 5th International Conference on Cyber Conflict 2013 (CyCon 2013). IEEE and NATO COE Publications. Tallinn, Estonia, 2013. P.119-142.

REFERENCES:

1. MASSIF FP7 Project. Management of Security information and events in Service Infrastructures. http://www.massif-project.eu.
2. Kotenko I., Stepashkin M. Network Security Evaluation based on Simulation of Malefactor's Behavior // SECRYPT 2006. International Conference on Security and Cryptography. Proceedings. Portugal. 7-10 August 2006. P.339-344.
3. Kotenko I.V., Stepashin M.V., Bogdanov V.S. Arkhitekturi i modeli komponentov aktivnogo analiza zashishennosti na osnove imitatsii deistviy zloumishlennikov // Problemi informatsionnoiy bezopasnosti. Komputernie sistemi. 2006, № 2, C.7-24.
4. 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, September 11-14, 2012. Los Alamitos, California. IEEE Computer Society. 2012. P. 94-101.
5. Ruiz J.F., Harjani R., Maña A., Desnitsky V., Kotenko I., Chechulin A. A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components // Proceedings - 20th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, PDP 2012 20th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, PDP 2012. Garching, 2012. C.261-268.
6. *Mayer A*. Operational Security Risk Metrics: Definitions, Calculations, Visualizations // Metricon 2.0. CTO RedSeal Systems, 2007.
7. The Center for Internet Security, The CIS Security Metrics, 2009.
8. *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.

9. *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.
Dantu R., Kolan P., Cangussu J. Network risk management using attacker profiling // Security and Communication Networks, 2009. Vol. 2, No. 1. P. 83-96.
10. *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.
11. *Manadhata P.K.*, *Wing J.M.* An attack surface metric // IEEE Transactions on Software Engineering, 2010. P. 371-386.
12. *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.
13. *Swanson M.*, *Bartol, N.*, *Sabato J.*, *Hash J.*, *Graffo L.* Security Metrics Guide for Information Technology Systems. NIST Special Publication 800-55, Jul. 2003.
14. *Axelrod C. W.* Accounting for Value and Uncertainty in Security Metrics. Information Systems Control Journal, 2008. Vol.6, P.1-6.
15. *Mell P.*, *Scarfone K.*, *Romanosky S.* A Complete Guide to the Common Vulnerability Scoring System Version 2.0, 2007.
16. *Kotenko I.*, *Chechulin A.* A Cyber Attack Modeling and Impact Assessment Framework // Proceedings of the 5th International Conference on Cyber Conflict 2013 (CyCon 2013). IEEE and NATO COE Publications. Tallinn, Estonia, 2013. P.119-142.