Методика оценивания защищенности информационно-телекоммуникационных узлов

Шинкаренко А. Ф.
Военно-космическая академия имени А. Ф. Можайского
Санкт-Петербург, Российская Федерация
tonio87@rambler.ru

Аннотация. **В работе рассматриваются перспективные направления исследований в области анализа защищенности информационно-телекоммуникационных сетей и вводятся основные показатели для расчета их защищенности. Предлагается многоуровневый подход к оцениванию защищенности, основанный на деревьях атак и зависимостях сервисов.**

Ключевые слова: **показатели защищенности, дерево атак, оценка рисков, уязвимость.**

Введение

В условиях ограниченных ресурсно-временных возможностей по обеспечению информационной безопасности проблема повышения уровня защищенности информационно-телекоммуникационных сетей (ИТКС) [1] и узлов в отдельности, с одной стороны, является нетривиальной, а с другой – значительно влияет на эффективность мероприятий, направленных на поддержание информационной безопасности. Для каждого информационно-технического объекта на основе анализа его свойств требуется принять решение о применении тех или иных способов и средств защиты от информационно-технических воздействий.

Сети строятся с использованием коммутаторов, маршрутизаторов и других устройств, которые стали чрезвычайно сложными, поскольку они реализуют все большее число сложных распределенных протоколов, стандартизированных международной организацией технических стандартов (на сегодня число активно используемых протоколов и их версий превысило 600), вместе с этим возрастает и число уязвимостей ИТКС, которыми могут воспользоваться злоумышленники при планировании и проведении составного деструктивного программно-аппаратного воздействия. Управление и обеспечение безопасности сложной сетевой инфраструктуры – сегодня в большей степени искусство, чем инженерия. Рост сетевых атак, вирусов и других сетевых угроз свидетельствует о том, что вопросы безопасности до сих пор не имеют надежных решений. Современное международное сообщество осознало, что компьютерные и телекоммуникационные сети являются объектом национальной безопасности.

Применение традиционных средств повышения защищенности ИТКС, основанных на анализе журналов событий безопасности, в силу описанных выше обстоятельств и повышенных требований к безопасности информации является недостаточным [2, 3]. Одно из актуальных направлений решения этой проблемы в настоящее время – совершенствование сервисов защиты информации, в первую очередь, тех служб, которые оценивают состояние ИТКС, управляют защитой и адаптируют политику безопасностии компонентов системы защиты информации.

Имеющиеся программные средства анализа защищенности ИТКС можно условно разделить на следующие классы:

- сбора сведений об ИТКС и узлах: Nmap, Wireshark и др.;
- обнаружения уязвимостей ПО: Nessus (OpenVas), Acunetix, AppScanи др.;
- эксплуатации уязвимостей: ImmunityCanvas, MetasploitFramework, VulnDisco, SAINTexploitи др.

Релевантные исследования

Известно много работ в предметной области моделирования компьютерных вторжений и обоснования показателей защищенности.

S. Kumar, E. H. Spafford предложили модель компьютерных атак на основе раскрашенных сетей Петри [4]. Каждая сигнатура атаки выражается как шаблон, который показывает взаимосвязь между событиями и их содержанием. Обозначения начального и конечного состояний и связь между ними определяют шаблон событий.

K. Iglun, R. A. Kemmerer, P. A. Porras описали подход к анализу перехода состояний при вторжении для моделирования компьютерных атак [5]. В их статье компьютерная атака представляется как последовательность действий, выполняемых атакующим для компрометации безопасности компьютерной системы. Атаки описываются с помощью диаграмм перехода состояний.

В работе F. Cohen «Моделирование компьютерных атак, защита и последовательность» рассмотрен подход к оцениванию сетевой безопасности как «причинно-следственная модель атаки и защиты информационной системы» [6]. Она состоит из сети, которая отображается узлами и их связями, причинно-следственной связной описательной модели и псевдослучайного генератора чисел. Стоит указать на значительное упрощение подобного представления при моделировании компьютерных вторжений, основанном на причинно-следственной связи.

В [7] представлены наглядные модели сети, возможностей, целей и способов действий атакующего. Эти модели используются для определения устройств, которые будут скомпрометированы с наибольшей вероятностью. Для предсказания поведения атакующего используются экономические принципы, использующие компромисс «выгода – затраты».

В [8–11] атаки описываются и исследуются в структурированной, основанной на графовых деревьях форме.

В [12] представлена высокоуровневая концептуальная модель атак, основанная на намерениях нарушителя (стратегии атаки). Широкомасштабное распределенное обнаружение вторжения сравнивается с задачей военного управления. Статья определяет намерения вторжения как дерево целей. Конечная цель вторжения соответствует корневому узлу. Узлы нижних уровней отображают альтернативные или упорядоченные подцели в достижении верхнего узла/цели. Конечные узлы (листья) являются подцелями. Они могут подкрепляться событиями, сгенерированными в различных средах.

На основе исследований в области показателей защищенности [13–15] можно выделить 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» [16].

Методика оценивания защищенности ИТКС на основе деревьев атак

В общем виде методику оценивания защищенности ИТКС можно представить в виде трех этапов: подготовительного, эксплуатации и заключительного. На подготовительном этапе для каждого узла ИТКС формируется список возможных атакующих действий, разбитых на группы по следующим параметрам: класс атаки, необходимый тип доступа и необходимый уровень знаний нарушителя, а для каждой группы, в свою очередь, формируется список конкретных атак и уязвимостей, которые эти атаки используют. На этапе эксплуатации определяется качественный уровень риска для всех угроз, также строятся деревья атак, на основе которых происходит дальнейшее оценивание защищенности ИТКС. Уровень защищенности анализируемой ИТКС на основе деревьев атак определяется на заключительном этапе.

Данная методика объединяет качественный и количественный подходы к оцениванию защищенности и позволяет определить общий уровень защищенности ИТКС. В данном подходе предлагается использовать общую систему оценивания уязвимостей CVSS (*Common Vulnerability Scoring System*) для определения критичности атакующих действий и методику FRAP (*Facilitated Risk Analysis Process*) [17].

Сбор исходной информации о компьютерной сети и формирование модели ИТКС, а также составление общего списка уязвимостей реализуются на основе описания программно-аппаратного обеспечения хоста на языке CPE и таких открытых баз уязвимостей, как NVD (*National Vulnerability Database*). Источниками данных об открытых уязвимостях также могут служить отчеты сканеров безопасности, таких как Nessus, MaxPatrol, Nmap и других. Уязвимости в системе хранятся в формате CVE [18]. По полученной информации формируются множества уязвимостей и выбираются модели нарушителей на основе знаний эксперта по безопасности. Также источниками данных об угрозах информационной безопасности и уязвимостях программного обеспечения могут служить соответствующие банк угроз и банк уязвимостей, разработанный ФСТЭК Российской Федерации [19].

Следующим этапом методики является подготовка данных для формирования деревьев атак и выделения возможных атакующих действий, доступных нарушителю для каждого узла ИТКС. Кроме отдельных уязвимостей при построении дерева атак используются шаблоны атак в формате CAPEC [20], которые могут выступать не только в качестве входной информации для построения графов атак, но и как результат анализа безопасности: они могут описывать наиболее часто встречающиеся последовательности эксплуатации уязвимостей и других действий атакующего.

Также шаблоны содержат описания атак, которые не используют уязвимости: например, первая стадия проведения анализа – это сбор информации о доступных узлах ИТКС. Для этого используется шаблон CAPEC-292 (*Host Discovery*), описывающий группу различных способов проведения сканирования хостов и портов. В эту группу, например, входят CAPEC-294 (*ICMP Address Mask Request*), CAPEC-299 (*TCP SYN Ping*), CAPEC-295 (*ICMP Timestamp Request*) и др. Следующая стадия анализа – поиск уязвимого программного обеспечения. Для этого используются следующие шаблоны: CAPEC-310 (*Scanning for Vulnerable Software*), CAPEC-312 (*Active OS Fingerprinting*), CAPEC-541 (*Application Fingerprinting*) и т. д. На третьей стадии проведения анализа используются как отдельные уязвимости из словаря CVE, так и шаблоны, например CAPEC-233 (*Privilege Escalation*) и т. д.

На этапе эксплуатации происходит первичное построение деревьев атак. Элемент модели атак, описывающий дерево атак, является вектором

$$M = \langle S, S_0, G, \pi \rangle, \quad (1)$$

где S – множество состояний сети, S_0 – начальное состояние сети, G – множество показателей, позволяющих определить процент достижения нарушителем своих целей при использовании построенного дерева атак, $\pi = S \cdot S$ – множество переходов между состояниями, которое можно определить имеющимися у злоумышленника атакующими действиями.

Узлы дерева атак задают возможные атакующие действия, связанные между собой в соответствии с тем, в каком порядке их может выполнять определенный нарушитель. Маршрут атаки является частью дерева атак и представляет собой последовательность состояний ИТКС $(S_0, S_1, ..., S_n)$, причем $(S_i, S_{i+1}) \in \pi \forall i \in [0, n]$.

В результате полученных деревьев атак и маршрутов воздействий оцениваются показатели защищенности. К ним относят:

– уязвимость ИТКС;
– слабость ИТКС;
– уязвимость ИТКС к атакам нулевого дня;
– поверхность атаки;
– процент узлов без критичных уязвимостей.

Для определения показателя уязвимости ИТКС необходимо на основе известных уязвимостей узлов и базовой оценки CVSS провести выборку таких узлов, базовый вектор оценки которых превышает 7,0.

Слабость хоста *CWcwss* определяется на основе стандартов «Общее перечисление слабых мест» (*Common Weakness Enumeration, CWE*) и «Общая система оценки слабых мест» (*Common Weaknesses Scoring System, CWSS*). Учитывая, что оценка в системе CWSS может лежать в диапазоне [0,100] и критичность этой оценки начинается от 60 единиц, показатель *CWcwss* вычисляется по формуле

$$CW_{cwss}(s) = \sum_{i=1}^{n} \max(0, CWSS_{cwss}(w_i) - 60) / n, \qquad (2)$$

где s – узел ИТКС; $CWSS_{CWSS}(w_i)$ – оценка CWSS для слабого места w_i узла s; n – количество узлов ИТКС с оценкой CWSS выше 60.

Действия злоумышленника во время проведения воздействия характеризует такой показатель, как поверхность атаки – все возможные маршруты атаки, исходя из текущего положения нарушителя на дереве атак и его навыков.

Процент узлов без критичных уязвимостей (под критичными понимаются уязвимости, для которых базовая оценка CVSS – «высокая») определяется отношением количества узлов ИТКС без известных критичных уязвимостей к общему количеству узлов.

Общий уровень защищенности ИТКС также можно вычислить на основе риска для всех угроз ИТКС. Риск определяется как результат возможности (вероятности) угрозы и последствий ее реализации для всей ИТКС.

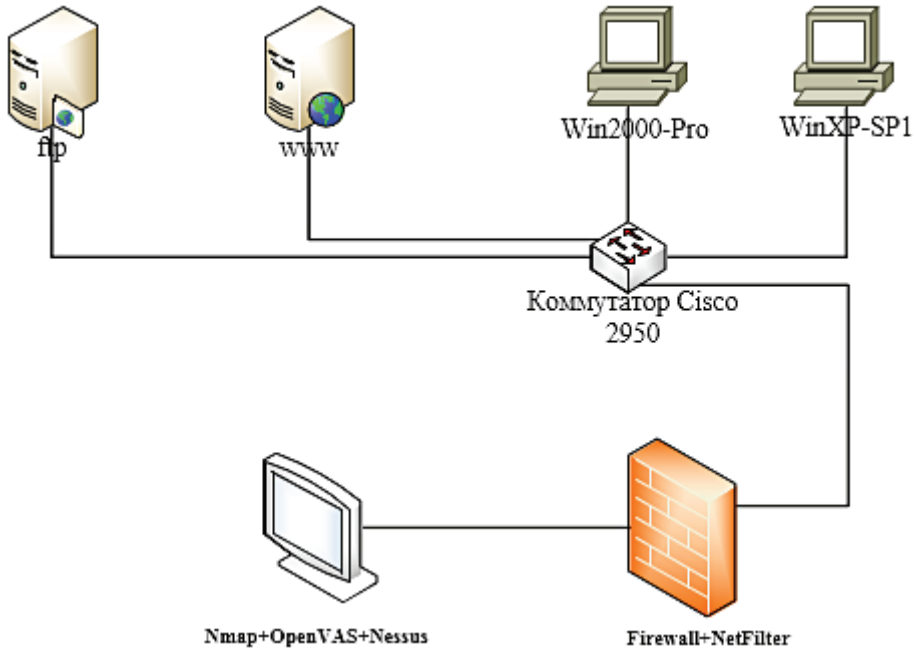
В самом общем виде методика расчета показателя «Уровень риска» выглядит следующим образом. Уровень риска атаки определяется как произведение вероятности успешной реализации атаки на ущерб, причиняемый в случае успешной реализации атаки. Вероятность успешной реализации атаки определяется исходя из навыков злоумышленника, надежности информации о событиях безопасности (показателей систем обнаружения вторжений), критичности атаки (определяется на основе базовой оценки CVSS) и потенциала атаки (определяется как отношение уже получившихся шагов воздействия 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 применения дополнительных средств защиты ко всей ИТКС в целом или к ее отдельным узлам.

Приведем пример применения предлагаемого подхода к оцениванию уровня защищенности ИТКС, представленной на рисунке. В качестве исходного месторасположения узла, который будет оценивать защищенности ИТКС, выбрано место, находящееся за пределами этой сети. В процессе построения дерева атак моделировались три основные стадии:

- сбор информации (предварительная разведка);
- выявление топологической структуры и связей сервисов;
- выявление уязвимостей и дальнейшее оценивание защищенности.

На первом этапе отыскиваются взаимосвязи узлов, связанных с начальным месторасположением аналитика, и узлов, связанных с конечными хостами (на рисунке это ftp-сервер, www-сервер, WinXP, Win200-Pro).

Следующим этапом при оценивании защищенности является последовательное выявление уязвимостей на обнаруженных узлах. Примером выполнения данного этапа служит найденная уязвимость CVE-2012-0383, которая позволяет использовать службу Network Address Translation (NAT) программного обеспечения Cisco IOS для удаленного проведения воздействия злоумышленником, отправляя специально сформированные SIP-пакеты, тем самым вызывая «отказ в обслуживании». На примере выявленной уязвимости оценим показатели защищенности. Напомним, что показатель «уязвимость ИТКС» формируется выборкой из всех имеющихся уязвимостей сети (всего в представленной ИТКС было выявлено 48 уязвимостей). Базовый вектор уязвимости CVE-2012-0383 (AV: N/AC: L/Au: N/C: N/I: N/A: C) составляет 7,8 единиц, что означает присоединение этой оценки к общему показателю уязвимости ИТКС [21]. Из 48 уязвимостей, базовый вектор оценки которых превышает 7,0 еди-



Экспериментальная ИТКС

ниц, было выявлено 32, средняя оценка которых составляет 8,1 единиц, что означает высокую степень уязвимости исследуемой ИТКС.

Показатель слабости ИТКС формируется также на основе всех выявленных угроз и уязвимостей согласно стандарту CWE. Оценка CWSS описанной уязвимости составляет 84 единицы, что также говорит о высокой критичности выявленной угрозы. По формуле (2) можно рассчитать показатель слабости ИТКС (оценка CWSS выше 60 единиц оказалась в 36 уязвимостях):

$$CW_{cwss} = 2844 / 36 = 79.$$

Показатель слабости ИТКС равен 79 единицам, что тоже свидетельствует о высокой критичности исследуемой ИТКС.

Процент узлов без критичных уязвимостей составляет $(16/48) \cdot 100 = 33{,}3\,\%$.

После анализа исследуемой ИТКС было построено около 80 различных маршрутов атак (маршруты атак отличаются друг от друга набором использованных уязвимостей). В результате выбран маршрут, имеющий минимальные значения сложности и максимальные значения уровня доступа для каждого узла. На основе данных об этом маршруте рассчитан уровень защищенности ИТКС в целом. Оценка уровня защищенности для анализируемой ИТКС составило 3 из 4, где уровень 1 – максимальная степень защищенности.

Таким образом, общая рекомендация к исследуемой ИТКС – повысить уровень ее защищенности, используя основные меры повышения информационной безопасности. Наиболее слабым местом в ИТКС оказался www-сервер, так как через него прошли практически все маршруты атак.

Заключение

В настоящей работе рассмотрены основные исследования в области оценивания защищенности сетей и выделены их основные показатели. На основе предложенных показателей, а также особенностей архитектуры системы анализа защищенности сформирована система методики расчета этих показателей, которые предполагаются для реализации в рамках системы оценки защищенности.

Литература

1. ГОСТ Р 52653-2006. Информационно-коммуникационные технологии в образовании. Термины и определения. – М. : Стандартинформ, 2006. – 11 с.

2. Котенко И. В. Перспективные направления исследований в области компьютерной безопасности / И. В. Котенко, Р. М. Юсупов // Защита информации. Инсайд. – 2006. – № 2. – С. 46–57.

3. Blakely B. A. Cyberprints Identifying cyber attackers by feature analysis : Doctoral Diss. – Iowa State Univ. 2012.

4. Kumar S. An Application of Pattern Matching in Intrusion Detection / S. Kumar, E. H. Spafford // Tech. Rep. CSDTR 94013. The COAST Project. Department of Comput. Sci. Purdue Univ. – West Lafayette, 1994.

5. Iglun K. State Transition Analysis: A Rule-Based Intrusion Detection System / K. Iglun, R. A. Kemmerer, P. A. Porras // IEEE Trans. Software Eng. – 1995. – No. 21 (3).

6. Cohen F. Simulating Cyber Attacks, Defenses, and Consequences / F. Cohen // IEEE Symp. Security and Privacy. – Berkeley, CA. 1999.

7. Yuill J. Intrusion-detection for incident-response, using a military battlefield-intelligence process / J. Yuill, F. Wu, J. Settle, F. Gong, R. Forno, M. Huang, J. Asbery // Comput. Networks. – 2000. – No. 34.

8. Huang M.-Y. A Large-scale Distributed Intrusion Detection Framework Based on Attack Strategy Analysis / M.-Y. Huang, T. M. Wicks // First Int. Workshop on the Recent Advances in Intrusion Detection, Raid'98. – Louvain-la-Neuve, Belgium, 1998.

9. Schneier B. Attack Trees / B. Schneier // Dr. Dobb's J. – 1999. –Vol. 12.

10. Котенко И. В. Применение графов атак для оценки защищенности компьютерных сетей и анализа событий безопасности / И. В. Котенко, А. А. Чечулин // Системы высокой доступности. – 2013. – Т. 9, № 3. – С. 103–110.

11. Абрамов Е. С. Применение графов атак для моделирования вредоносных сетевых воздействий / Е. С. Абрамов, А. В. Андреев, Д. В. Мордвин // Изв. ЮФУ. Технические науки. – 2012. – № 1. – С. 165–174.

12. Moitra S. D. A Simulation Model for Managing Survivability of Networked Information Systems / S. D. Moitra, S. L. Konda // Tech. Rep. CMU/SEI-2000-TR-020 ESC-TR-2000-020. – 2000. – 47 p.

13. Chi S.-D. Network Security Modeling and Cyber Attack Simulation Methodology / S.-D. Chi, J. S. Park, K.-C. Jung, J.-S. Lee // Lecture Notes in Computer Sci. – Carnegie Mellon Univ., 2001. – Vol. 2119.

14. Templeton S. J. A Requires/Provides Model for Computer Attack / S. J. Templeton, K. Levitt // NSPW 2000 : Proc. of the 2000 Workshop on New Security Paradigms. – NY : ACM, 2000. – P. 31–38.

15. Morin B. M2d2 : A formal data model for ids alert correlation / B. Morin, L. Me, H. Debar, M. Ducasse // Lecture Notes in Comput. Sci. – Berlin : Springer-Verlag, 2002. – Vol. 1516. – P. 115–137.

16. Меры защиты информации в государственных информационных системах : методический документ (утв. ФСТЭК РФ 11.02.2014).

17. Peltier T. R. How to complete a risk assessment in 5 days or less / T. R. Peltier // Auerbach publ. – 2008. – P. 1–55.

18. http://cve.mitre.org (дата обращения 25.11.2015).

19. Банк данных угроз безопасности информации ФСТЭК РФ – URL : http://bdu.fstec.ru/threat (дата обращения 25.11.2015).

20. http://capec.mitre.org (дата обращения 25.11.2015).

21. http://bdu.fstec.ru/calc (дата обращения 25.11.2015).

The method of estimation of the security of information and telecommunication

Shinkarenko A. F.
Military Space academy named after A. F. Mozhaisky
S. Petersburg, Russia
tonio87@rambler.ru

Abstract. **The work considers the perspective directions of research in the field of security metrics and establishes key indicators, based on which the calculation of the security of the system. Proposed tiered approach to the assessment of security and their calculation methodology based on attack trees and dependency services.**

Keywords: **security metrics, attack tree, risk assessment, vulnerability.**

References

1. GOST R 52653-2006 *Informatsionno-kommunikatsionnye tekhnologii v obrazovanii. Terminy i opredeleniya* [Information and communication technologies in education. Terms and definitions], Moscow, Standartinform, 2006, 11 p.

2. Kotenko I. V., Yusupov R. M. Promising areas of research in the field computer security [Perspektivnie napravleniya issledovaniy v oblasti komp'yuternoy bezopasnosti], *Zashchita informacii. Insayd [Data protection. Inside]*, 2006, no. 2, pp. 46-57.

3. Blakely B. A. Cyberprints Identifying cyber attackers by feature analysis. Doctoral Dissertation: Iowa State Univ. 2012.

4. Kumar S., Spafford E. H. An Application of Pattern Matching in Intrusion Detection, *Tech. Rep. CSDTR 94 013. The COAST Project. Department of Comput. Sci. Purdue Univ.*, West Lafayette, 1994.

5. Iglun K., Kemmerer R. A., Porras P. A. State Transition Analysis: A Rule-Based Intrusion Detection System *IEEE Trans. Software Eng.*, 1995, no. 21 (3).

6. Cohen F. Simulating Cyber Attacks, Defenses, and Consequences, *IEEE Symp. Security and Privacy*, Berkeley, CA. 1999.

7. Yuill J., Wu F., Settle J., Gong F., Forno R., Huang M., Asbery J. Intrusion-detection for incident-response, using a military battlefield-intelligence process, *Comput. Networks*, 2000, no. 34.

8. Huang M.-Y., Wicks T. M. A Large-scale Distributed Intrusion Detection Framework Based on Attack Strategy Analysis, *First Int. Workshop on the Recent Advances in Intrusion Detection, Raid'98*, Louvain-la-Neuve, Belgium, 1998.

9. Schneier B. Attack Trees, *Dr. Dobb's J.*, 1999, Vol. 12.

10. Kotenko I. V., Chechulin A. A. The use of attack to evaluate the security of computer networks and analysis of security events [Primenenie grafov atak dlya otsenki zashchishchennosti komp'yuternykh setey i analiza sobytiy bezopasnosti], *Sistemy vysokoy dostupnosti [High Availability Systems]*, 2013, Vol. 9, no. 3, pp. 103-110.

11. Abramov E. S., Andreev A. V., Mordvin D. V. The use of attack graphs for modelling malicious network effects [Primenenie grafov atak dlya modelirovaniya vredonosnykh setevykh vozdeystviy], *Izvestiya YuFU [News SFU]*, 2012, no. 1, pp. 165-174.

12. Moitra S. D., Konda S. L. A Simulation Model for Managing Survivability of Networked Information Systems. Tech. Rep. CMU/SEI-2000-TR-020 ESC-TR-2000-020, 2000, 47 p.

13. Chi S.-D., Park J. S., Jung K.-C., Lee J.-S. Network Security Modeling and Cyber Attack Simulation Methodology, *Lecture Notes in Comput. Sci.*, 2001, Vol. 2119.

14. Templeton S. J., Levitt K. A Requires/Provides Model for Computer Attack, *NSPW 2000: Proc. of the 2000 Workshop on New Security Paradigms*, NY, ACM, 2000, pp. 31-38.

15. Morin B., Me L., Debar H., Ducasse M. M2d2: A formal data model for ids alert correlation, *Lecture Notes in Comput. Sci.*, Berlin, Springer-Verlag, 2002, Vol. 1516, pp. 115-137.

16. *Mery zashchity informatsii v gosudarstvennykh informatsionnykh sistemakh* [Rrotection of information in state information systems], methodical document FSTEK RF, from 11.02.2014.

17. Peltier T. R. How to complete a risk assessment in 5 days or less, Auerbach publ., 2008, pp. 1-55.

18. http://cve.mitre.org (accessed 25 Nov. 2015).

19. http://bdu.fstec.ru/threat (accessed 25 Nov. 2015).

20. http://capec.mitre.org (accessed 25 Nov. 2015).

21. http://bdu.fstec.ru/calc (accessed 25 Nov. 2015).