Сергей А. Климачев, Наталья А. Тишина
Оренбургский государственный университет,
пр-т Победы, 13, г. Оренбург, 460018, Россия
e-mail: sersh-nick@mail.ru, https://orcid.org/0000-0001-9664-5759
e-mail: tnatalia_oren@mail.ru, https://orcid/0000-0002-7341-6985

МЕТОДИКА ЭКСПЕРИМЕНТАЛЬНОЙ ОЦЕНКИ ТОЧНОСТИ ОБНАРУЖЕНИЯ АТАК ОБЛАЧНОЙ СРЕДЫ

DOI: http://dx.doi.org/10.26583/bit.2018.2.04

Аннотация. Статья посвящена исследованию вопроса оценки эффективности систем обнаружения атак (СОА), применяемых для защиты вычислительных платформ, характеризующихся динамичностью, сложной организационно-технической структурой и наличием большого количества разнородных параметров ее компонент. Анализ существующих методик оценки СОА позволил выявить проблемы, в частности недостатки в обосновании количественных метрик, отражающих производительность, достоверность принимаемых решений СОА, что затрудняет доказуемость методики оценки СОА. Целью исследования является: повышение объективности оценки СОА, достичь которую можно с помощью разработки правильной методики и инструментов оценки, а также надежного экспериментального стенда. В статье предложены результаты разработки и апробации методики и программного обеспечения оценки эффективности СОА на основе построения оптимального множества количественных показателей точности обнаружения атак, позволяющие решать задачи сравнительного анализа СОА, обладающих схожими функциональными возможностями. В результате проведенных исследований решены следующие задачи: выбор универсальных количественных показателей для оценки точности обнаружения атак СОА; определение обобщенного показателя точности обнаружения атак на основе построения парето-оптимального множества наборов значений количественных показателей, отражающих обеспечение конфиденциальности, целостности и доступности информации и информационных ресурсов облачной среды; разработка функциональной модели, схемы и программного обеспечения экспериментального исследования СОА облачной среды.

Ключевые слова: оценка эффективности, количественные показатели эффективности, системы обнаружения атак, облачная среда.

Для цитирования. КЛИМАЧЕВ, Сергей А.; ТИШИНА, Наталья А.. МЕТОДИКА ЭКСПЕРИМЕНТАЛЬНОЙ ОЦЕНКИ ТОЧНОСТИ ОБНАРУЖЕНИЯ АТАК ОБЛАЧНОЙ СРЕДЫ. Безопасность информационных технологий, [S.l.], n. 2, p. 54-62, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1109>. Дата доступа: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.04.

Sergey A. Klimachev, Natalia A. Tishina
Orenburg State University,
Pobedy Av., 13 Orenburg, 460018, Russia,
e-mail: sersh-nick@mail.ru, https://orcid.org/0000-0001-9664-5759
e-mail: tnatalia_oren@mail.ru https://orcid/0000-0002-7341-6985

Technique of experimental evaluation of cloud environment attacks detection accuracy

DOI: http://dx.doi.org/10.26583/bit.2018.2.04

Abstract. The article is devoted to research of efficiency evaluation of IDS used for dynamic and complex organizational and technical structure computing platform guard. The components of the platform have a set of heterogeneous parameters. Analysis of existing IDS evaluation technique revealed shortcomings in justification of quantitative metrics that describe the

efficiency and reliability IDS resolving. This makes if difficult to prove IDS evaluation technique. The purpose of the study is to increase IDS evaluation objectivity. To achive the purpose it is necessary to develop the correct technique, tools, experimental stand. The article proposes the results of development and approbation of the technique of IDS efficiency evaluation and software for it. The technique is based on defining of optimal set of attack detection accuracy scores. The technique and the software allow solving problems of comparative analysis of IDS that have similar functionality. As a result of the research, a number of task have been solved, including the selection of universal quantitative metrics for attack detection accuracy evaluation, the defining of summarised attack detection accuracy evaluation metric based on defining of pareto-optimal set of scores that ensure the confidentiality, integrity and accessibility of cloud environment information and information resources, the development of a functional model, a functional scheme and a software for cloud environment IDS research.
Keywords: efficiency evaluation, efficiency scores, IDS, cloud environment.
For citation. KLIMACHEV, Sergey A.; TISHINA, Natalia A.. Technique of experimental evaluation of cloud environment attacks detection accuracy. IT Security (Russia), [S.l.], n. 2, p. 54-62, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1109>. Date accessed: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.04

Введение

Начало XXI века ознаменовалось бурным развитием облачных вычислений, повлекшим за собой рост популярности облачных сервисов и масштабный переход организаций на новую вычислительную платформу, в результате облачные вычисления стали рассматриваться в качестве альтернативы традиционным моделям обработки информации.

Однако передовой характер технологии и природа ее концепции определили не только преимущества облачных вычислений, но и проблемные стороны, центральное место в списке которых заняла безопасность. Статистика угроз и анализ рынка облачных вычислений показывают, что актуальность защиты облачной среды (ОС) (Cloud Environment) очень высока [1], [2]. Однако сложная организационно-техническая структура среды и наличие большого количества разнородных параметров ее компонент значительно усложняют задачу обеспечения безопасности. При этом использование программных систем защиты информации для поддержания безопасного состояния среды приводит к возникновению новых вопросов методологического и практического характера в области исследования средств защиты информации. Среди них выделяется вопрос оценки эффективности систем обнаружения компьютерных атак, называемых Федеральной службой безопасности (ФСБ России) системами обнаружения атак (СОА), а Федеральной службой по техническому и экспортному контролю (ФСТЭК России) – системами обнаружения вторжений (СОВ).

Существуют различные методики оценки эффективности СОА, отличающиеся множеством критериев и показателей, методами расчета показателей, множеством параметров системы.

Можно выделить такие проблемы существующих методик как:

– использование только качественных или нечетко определенных количественных показателей оценки (используются тривиальные или невыразительные показатели оценки);

– используемые классификации атак не помогают в достоверной и объективной оценке, так как не охватывают все аспекты атак, обеспечивающие полноту анализа при формировании подмножества атак;

– нет четко определенной методологии, организация и последовательность методики нарушают логический порядок;

– отсутствие репрезентативных тестовых наборов нападения, основанных на полной и правильной классификационной схеме атак.

В результате существенно затрудняется оценка функциональных возможностей СОА и обоснование выбора СОА для эксплуатации в конкретных условиях. Низкий уровень обоснования количественных показателей оценки эффективности, отражающих производительность, достоверность принимаемых решений СОА затрудняет доказуемость методики оценки СОА.

Методология количественного оценивания эффективности СОА предназначена для сравнения различных СОА и определения оптимальных параметров СОА, в ней выделяют критерий, показатель и метод:

– критерий – это область оценивания (обобщенный показатель), т.е. то, что необходимо оценить и правило выбора: например, максимальная точность обнаружения атак, максимальная скорость обнаружения атак и т.п.;

– показатель (мера или метрика) определяет конкретное свойство, которое оценивается для выбранного критерия: например, процент правильно распознанных атак, время обработки пакетов, уровень максимальной пропускной способности канала передачи данных и т.п.

– метод – это способ определения соответствующего значения для данного показателя: например, сравнение распознанных атак с последовательностью сгенерированных атак, оценка времени распознавания атак в секундах и т.п.

Среди количественных критериев, характеризующих эффективность СОА, таких как точность, полнота, производительность и оперативность обнаружения атак, недостаточно исследован важнейший критерий – точность обнаружения атак, характеризующий способность СОА правильно распознавать атакующие воздействия.

Таким образом, актуальной задачей становится разработка методики оценки точности обнаружения атак СОА, позволяющей осуществить выбор наилучшей СОА и определять оптимальные параметры СОА.

Для решения данной задачи необходимо выполнить:

- Выбор показателей оценки точности обнаружения атак.
- Выбор методов расчета показателей.
- Разработку экспериментального стенда.

Целью исследования является: повышение объективности оценки СОА путем разработки правильной методики и программного обеспечения оценки, а также экспериментального стенда.

Разработка методики оценки

Разрабатываемая методика должна учитывать существующие проблемы оценки, всеобъемлющие, универсальные количественные показатели точности СОА и условия её эксплуатации – характеристики ОС. Оценка может вестись в двух направлениях: определение точности обнаружения атак по параметрам СОА и определение наиболее эффективной по точности обнаружения атак одной из нескольких СОА.

Решение задачи выбора показателей оценки, которые отражают достоверность принимаемых решений СОА, является важным аспектом формирования методики оценки точности обнаружения атак. В ходе исследовательских разработок СОА было предложено множество различных количественных показателей. Наиболее часто применяются показатели, которые измеряют соотношение между входными и выходными событиями СОА, такие как [3]:

- TP (True positive): количество истинно-положительных распознаваний атак.
- TN (True negative): количество истинно-отрицательных распознаваний атак.
- FP (False positive): количество ложно-положительных распознаваний атак.
- FN (False negative): количество ложно-отрицательных распознаваний атак.

Используя эти простые показатели, получают оценку, размытую между ними,

поэтому целесообразнее получить математическое выражение для интегрального показателя или построить множество оптимальных наборов значений показателей.

Исследователями предлагались и более сложные соотношения для показателей, такие как кривая ROC (Receiver Operating Characteristic) – кривая эксплуатационной характеристики приемника [4, 5], P(I|A) – байесовский уровень обнаружения [6], совокупная стоимость [7], ожидаемая стоимость [8], CID (Intrusion Detection Capability) – способность обнаружения вторжений [9], E_{ID} (enhanced Bayesian detection rate) – расширенная байесовская оценка [10], R_R.(Attack Recognition Rate) – уровень распознавания атак [10].

Каждый из этих показателей был основан на различных теоретических подходах, таких как оптимизационный подход [11], байесовский и информационно-энтропийный подходы [12, 13], метод имитационного моделирования [10], оценка рисков информационной безопасности [14, 15]. Однако ни один из перечисленных подходов не лишен недостатков.

Одни методики позволяют выбрать лучшую СОА, сравнивая две или более системы, в то время как каждая сравниваемая система в отдельности не является эффективной. Другие методики учитывают соотношение только некоторых частных показателей и не учитывают, что эффективность СОА зависит от большого числа показателей, которые могут быть несравнимыми. Общий недостаток большинства существующих подходов: не учитывают классификацию атак, усредняя значение показателей по всем видам атак, в то время как некоторые СОА могут быть более точными по одному из видов атак, являющемуся более опасным для конкретной защищаемой среды.

В данной работе предлагается методика оценки СОА, основанная на построении множества оптимальных наборов значений количественных показателей точности обнаружения атак. Показатели характеризуют правильность распознавания атак категорий, соответствующих стандартной модели безопасности информации CIA (Confidentiality, Integrity, Availability):

1) k^C – уровень распознавания атак конфиденциальности,
2) k^I – уровень распознавания атак целостности,
3) k^A – уровень распознавания атак доступности,

такие, что

$$k^{\{C,I,A\}} = \frac{TP + TN}{TP + FP + TN + FN}, \quad (1)$$

где TP – количество верно распознанных атак соответствующей категории; TN – количество верно распознанных легитимных воздействий; FP – количество воздействий, неверно распознанных как атаки; FN – количество воздействий, неверно распознанных как легитимные.

Предполагается, что СОА $S*$ обеспечивает некоторую точность обнаружения атак и характеризуется некоторым множеством параметров P^S, а также существует множество векторов P, определяющее всевозможные значения этих параметров, причем каждому вектору $p_i \in P,\ i = \overline{1..n}$ ставится в соответствие некоторый вектор значений показателей точности обнаружения k_{p_i} множества векторов K. Тогда задача экспериментального исследования СОА будет заключаться в выделении оптимального вектора значений показателей точности обнаружения и соответствующего ему вектора значений параметров СОА:

$$\begin{cases} L(p_i, k_{p_i}) \to \max \\ p_i \in P : k_{p_i} = A(K,U), k_{p_i} \in K \end{cases}, \quad (2)$$

где $A(K,U)$ – алгоритм, определяющий оптимальный вектор значений показателей точности обнаружения из множества векторов K по заданным условиям U; $L(p_i,k_{p_i})$ – точность обнаружения атак, обеспечиваемая СОА.

Таким образом, задача определения наилучших значений параметров СОА сводится к задаче нахождения вектора оптимальных значений показателей точности, которая в свою очередь может быть решена на основе построения парето-оптимального множества.

Решение $k^* \in K$ называется оптимальным по Парето (парето-оптимальным), если не существует такого возможного решения $k \in K$, для которого имеет место неравенство $f(k) \geq f(k^*)$. Все парето-оптимальные решения образуют множество Парето ($P_f(K)$):

$$P_f(K) = \{k^* \in K \mid \nexists k \in K, f(k) \geq f(k^*)\}. \quad (3)$$

Для нахождения множества Парето будет использоваться алгоритм, приведенный в [16]. Выбор единственного вектора парето-оптимального множества будет осуществляться на основе обобщенного показателя (4):

$$k^{общ^*} = \sum_i w_i \cdot k_i,\ i \in \{C, I, A\}, \quad (4)$$

где w_i – весовой коэффициент значимости показателя точности обнаружения атак, определяемый экспертом (1).

Тогда наилучшим будет вектор, характеризующийся максимальным $k^{общ^*}$.

Таким образом, предложенный подход позволяет: осуществлять подбор параметров СОА, при которых обеспечивается конфиденциальность, целостность и доступность информации и информационных ресурсов ОС в наибольшей степени; проводить сравнительный анализ нескольких СОА на предмет выявления системы с наилучшими показателями точности обнаружения атак.

Программное обеспечение и схема эксперимента

Описанная методика была положена в основу аналитической компоненты программного средства оценки точности обнаружения атак СОА. Работоспособность программного средства подтверждена в результате эксперимента (рисунок 1), в котором в качестве анализируемой СОА выступила система Snort. Snort использует язык правил, комбинирующий возможности сигнатурного поиска, протокольного анализа и обнаружения аномалий. Схема экспериментального стенда облачной среды для испытаний СОА представлена на рисунке 2.

Основной отличительной особенностью экспериментального стенда для оценки СОА в условиях облачных вычислений является использование технологии виртуализации и балансировщика нагрузки. Обнаружение атак осуществляется либо путем маршрутизации всего трафика через СОА, установленную на выделенный сервер как на рисунке 2, либо же путем мониторинга трафика на каждом сервере в отдельности.

Для сравнительного анализа использовано 10 различных наборов правил. Выполнение атакующих воздействий осуществлялось в соответствии с планом (таблица 1), включающим три серии атак, направленных на нарушение конфиденциальности, целостности и доступности информации. Значение «1» плана определяет реализацию атаки, «0» - генерацию сетевой нагрузки. Каждая серия атак состоит из 10 позиций.

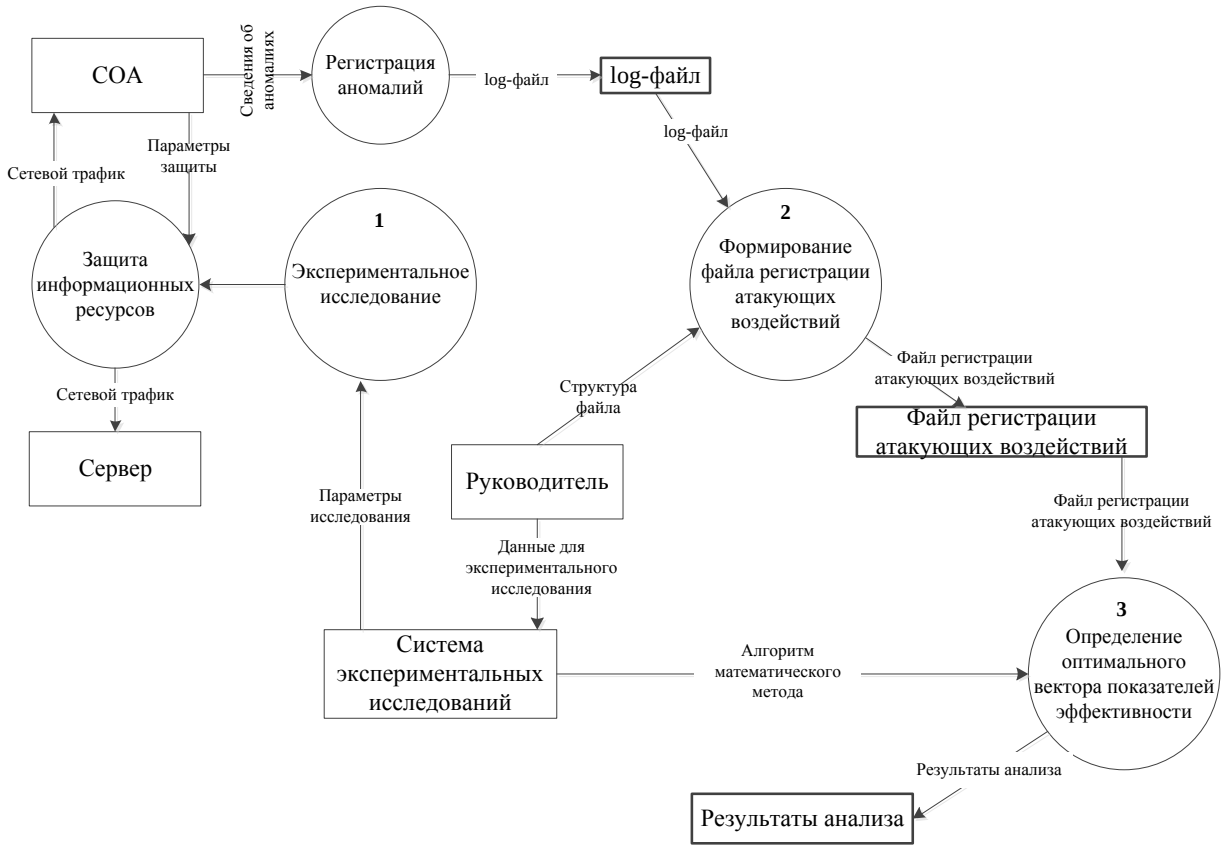

Рис. 1. Схема проведения эксперимента
(Fig. 1. Scheme of the experiment)

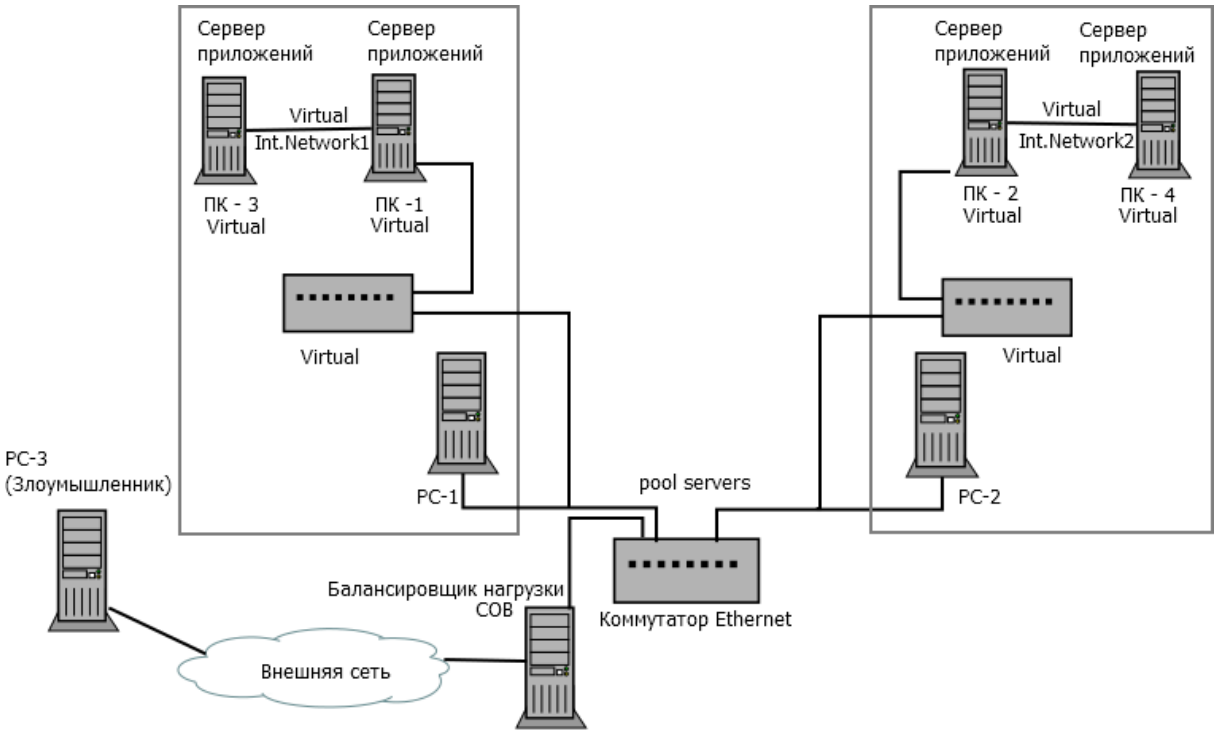

Рис. 2. Схема экспериментального стенда
(Fig. 2. The scheme of experimental stand)

Таблица 1. План выполнения атакующих воздействий

Серии атак	Атакующие воздействия									
Конфиденциальность	1	1	0	1	1	0	1	1	1	1
Целостность	1	0	1	1	1	0	1	0	1	1
Доступность	1	1	1	0	1	1	1	1	0	1

На основе результатов экспериментальных исследований в соответствии с вышеописанным планом и результатов анализа log-файлов СОА в соответствии с формулой (1) для каждого набора правил СОА Snort получены следующие показатели точности СОА (таблица 2).

Таблица 2. Показатели точности СОА

Показатель	Номер набора правил Snort									
	1	2	3	4	5	6	7	8	9	10
k_C	1	0,8	0,6	0,8	0,8	0,6	0,9	0,7	0,6	0,6
k_I	0,8	0,8	1	0,9	1	0,8	0,8	0,9	0,9	0,7
k_A	0,9	0,9	0,9	0,9	0,8	0,9	0,9	0,8	0,9	0,8

В результате нахождения парето-оптимального множества векторов показателей точности СОА наилучшим набором правил Snort определен набор №1 (рисунок 3).

Таким образом, предложенная методика на основе парето-оптимального множества позволила осуществить выбор наилучшего набора правил СОА, минимизируя участие эксперта в процессе оценивания.

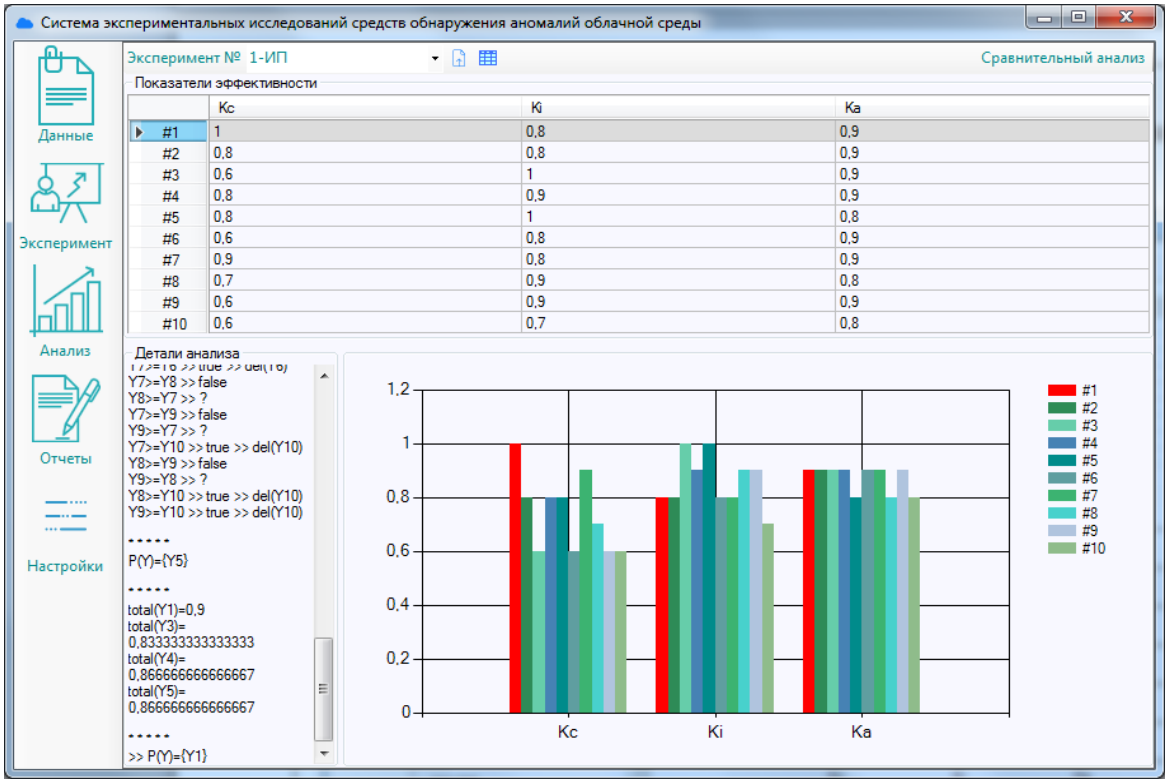

Рис. 3. Результаты экспериментальных исследований
(Fig. 3. The results of experimental studies)

Заключение

В результате проведенных исследований достигнуты следующие результаты:

– выбраны универсальные количественные показатели для оценки точности обнаружения атак СОА.

– определен обобщенный показатель точности обнаружения атак на основе построения парето-оптимального множества наборов значений количественных показателей, отражающих обеспечение конфиденциальности, целостности и доступности информации и информационных ресурсов ОС.

– разработаны схема проведения эксперимента, схема экспериментального стенда и программное обеспечение экспериментального исследования СОА облачной среды.

Таким образом, разработанная методика и программное обеспечение оценки позволяют вне зависимости от архитектуры СОА и реализованных в ней методов обнаружения атак осуществлять сравнительный анализ СОА, обладающих схожими функциональными возможностями на предмет выявления системы с наилучшими показателями точности обнаружения атак и определять наилучший набор значений параметров СОА.

СПИСОК ЛИТЕРАТУРЫ:

1. Architectures and Protocols for Secure Information Technology. Ruiz-Martinez, Pereniguez-Garcia, and Marin-Lopez (Eds.), IGI-Global, USA, 2013.
2. Security Issues in Cloud Environments – A Survey Diogo A. B. Fernandes, Liliana F. B. Soares, João V. Gomes, Mário M. Freire, Pedro R. M. Inácio. International Journal of Information Security, Volume 13 Issue 2, April 2014 pp. 113-170.
3. Vasim Iqbal Memon, Gajendra Singh Chandel A Design and Implementation of New Hybrid System for Anomaly Intrusion Detection System to Improve Efficiency. Vasim Iqbal Memon, Gajendra Singh Chandel. Vasim Iqbal Memon et al Int. Journal of Engineering Research and Applications www.ijera.com ISSN: 2248-9622, Vol. 4, Issue 5 (Version 1), May 2014, pp.01-07.
4. Jacob W. Ulvila, John E. Gaffney, Jr Evaluation of Intrusion Detection Systems, Journal of Research of the National Institute of Standards and Technology, Volume 108, Number 6, November-December 2003 [Электронный ресурс]. – Режим доступа: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4844520.
5. Lippmann, R.; Fried, D.; Graf, I.; Haines, J.; Kendall, K.; Mcclung, D.; Weber, D.; Webster, S.; et al.: Evaluating Intrusion Detection Systems: The 1998 DARPA Off-line Intrusion Detection Evaluation. In: Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'00). vol. 2. Los Alamitos, CA, USA: IEEE, 2000, pp. 12–26.
6. Axelsson, S. The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection. In: Proceedings of the 6th ACM Conference on Computer and Communications Security (CCS'99). Singapore: ACM Press, 1999, pp. 1–7.
7. Stolfo, S.; Fan, W.; Lee, W.; Prodromidis, A.; Chan, P.: Cost-Based Modeling for Fraud and Intrusion Detection: Results from the JAM Project. In: Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'00). vol. 2. South Carolina, USA: IEEE, 2000, pp. 130–144.
8. Gaffney, J.E.; Ulvila, J.W. Evaluation of Intrusion Detectors: A Decision Theory Approach. In: Proceedings of the IEEE Symposium on Security and Privacy (S&P'01). Oakland, CA, USA: IEEE, 2001, pp. 50–61.
9. Gu, G.; Fogla, P.; Dagon, D.; Lee, W.; Skoric, B.: Measuring Intrusion Detection Capability: An Information-Theoretic Approach. In: Proceedings of the ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS'06). Taipei, Taiwan: ACM, 2006, pp. 90–101.
10. Nasr, Khalid. Performance analysis of wireless intrusion detection systems. PhD, Institut National Polytechnique de Toulouse, 2013 [Электронный ресурс]. – Режим доступа: http://oatao.univ-toulouse.fr/14136
11. Методы оценки эффективности систем защиты информационных систем. Н.А. Маслова Искусственный интеллект. — 2008. — № 4. — С. 253-264.
12. Зикратов Игорь Алексеевич, Одегов Степан Викторович Оценка информационной безопасности в облачных вычислениях на основе байесовского подхода. Научно-технический вестник информационных технологий, механики и оптики. 2012. №4 (80) [Электронный ресурс]. – Режим доступа: http://cyberleninka.ru/article/n/otsenka-informatsionnoy-bezopasnosti-v-oblachnyh-vychisleniyah-na-osnove-bayesovskogo-podhoda
13. Анищенко В. В., Земцов Ю. В. Методика испытаний систем обнаружения атак. Известия ЮФУ. Технические науки. 2007. №1 [Электронный ресурс]. – Режим доступа: http://cyberleninka.ru/article/n/metodika-ispytaniy-sistem-obnaruzhe-niya-atak.
14. Зикратов Игорь Алексеевич, Одегов Степан Викторович, Смирных Александр Валентинович Оценка рисков информационной безопасности в облачных сервисах на основе линейного программирования. Научно-технический вестник информационных технологий, механики и оптики. 2013. №1 (83) [Электронный ресурс]. – Режим доступа: http://cyberleninka.ru/article/n/otsenka-riskov-informatsionnoy-bezopasnosti-v-oblachnyh-servisah-na-osnove-lineynogo-programmirovaniya.

15. Царегородцев А.В., Макаренко Е.В. Методика количественной оценки риска в информационной безопасности облачной инфраструктуры организации. Национальные интересы: приоритеты и безопасность. 2014. №44 [Электронный ресурс]. – Режим доступа: http://cyberleninka.ru/article/n/metodika-kolichestvennoy-otsenki-riska-v-informatsionnoy-bezopasnosti-oblachnoy-infrastruktury-organizatsii-1.
16. В.Д. Ногин. Принятие решений при многих критериях. Учебно-методическое пособие. – СПб. Издательство «ЮТАС», 2007. – 104 с.

REFERENCES:

[1] Architectures and Protocols for Secure Information Technology. Ruiz-Martinez, Pereniguez-Garcia, and Marin-Lopez (Eds.), IGI-Global, USA, 2013.
[2] Security Issues in Cloud Environments – A Survey Diogo A. B. Fernandes, Liliana F. B. Soares, João V. Gomes, Mário M. Freire, Pedro R. M. Inácio. International Journal of Information Security, Volume 13 Issue 2, April 2014 pp. 113-170.
[3] Vasim Iqbal Memon, Gajendra Singh Chandel A Design and Implementation of New Hybrid System for Anomaly Intrusion Detection System to Improve Efficiency. Vasim Iqbal Memon, Gajendra Singh Chandel. Vasim Iqbal Memon et al Int. Journal of Engineering Research and Applications www.ijera.com ISSN: 2248-9622, Vol. 4, Issue 5 (Version 1), May 2014, pp.01-07.
[4] Jacob W. Ulvila, John E. Gaffney, Jr Evaluation of Intrusion Detection Systems, Journal of Research of the National Institute of Standards and Technology, Volume 108, Number 6, November-December 2003 [Электронный ресурс]. – Режим доступа: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4844520.
[5] Lippmann, R.; Fried, D.; Graf, I.; Haines, J.; Kendall, K.; Mcclung, D.; Weber, D.; Webster, S.; et al.: Evaluating Intrusion Detection Systems: The 1998 DARPA Off-line Intrusion Detection Evaluation. In: Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'00). vol. 2. Los Alamitos, CA, USA: IEEE, 2000, pp. 12–26.
[6] Axelsson, S. The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection. In: Proceedings of the 6th ACM Conference on Computer and Communications Security (CCS'99). Singapore: ACM Press, 1999, pp. 1–7.
[7] Stolfo, S.; Fan, W.; Lee, W.; Prodromidis, A.; Chan, P.: Cost-Based Modeling for Fraud and Intrusion Detection: Results from the JAM Project. In: Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'00). vol. 2. South Carolina, USA: IEEE, 2000, pp. 130–144.
[8] Gaffney, J.E.; Ulvila, J.W. Evaluation of Intrusion Detectors: A Decision Theory Approach. In: Proceedings of the IEEE Symposium on Security and Privacy (S&P'01). Oakland, CA, USA: IEEE, 2001, pp. 50–61.
[9] Gu, G.; Fogla, P.; Dagon, D.; Lee, W.; Skoric, B.: Measuring Intrusion Detection Capability: An Information-Theoretic Approach. In: Proceedings of the ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS'06). Taipei, Taiwan: ACM, 2006, pp. 90–101.
[10] Nasr, Khalid. Performance analysis of wireless intrusion detection systems. PhD, Institut National Polytechnique de Toulouse, 2013 [Электронный ресурс]. – Режим доступа: http://oatao.univ-toulouse.fr/14136
[11] Methods for evaluating the effectiveness of information systems security. H. Ah. Maslov Artificial intelligence. - 2008. — No. 4. — P. 253-264. (in Russian).
[12] Zikratov Igor' Alekseyevich, Odegov Stepan Viktorovich Evaluation of information security in cloud computing based on Bayesian approach. Journal scientific and technical of information technologies, mechanics and optics. 2012. No. 4 (80) [Electronic resource]. – Mode of access: http://cyberleninka.ru/article/n/otsenka-informatsionnoy-bezopasnosti-v-oblachnyh-vychisleniyah-na-osnove-bayesovskogo-podhoda. (in Russian).
[13] Anishchenko V. V., Zemtsov Y. V. Methods of testing systems to detect attacks. Izvestiya yufu. Technical science. 2007. No. 1 [Electronic resource]. - Access mode: http://cyberleninka.ru/article/n/metodika-ispytaniy-sistem-obnaruzhe-niya-atak. (in Russian).
[14] Zikratov Igor' Alekseyevich, Odegov Stepan Viktorovich, Smirnykh Aleksandr Valentinovich Assessment of information security risks in cloud services based on linear programming. Journal scientific and technical of information technologies, mechanics and optics. 2013. No. 1 (83) [Electronic resource]. – Mode of access: http://cyberleninka.ru/article/n/otsenka-riskov-informatsionnoy-bezopasnosti-v-oblachnyh-servisah-na-osnove-lineynogo-programmirovaniya. (in Russian).
[15] Tsaregorodtsev A.V., Makarenko Y.V. Methods of quantitative risk assessment in information security of cloud infrastructure of the organization. National interests: priorities and security. 2014. No. 44 [Electronic resource]. – Mode of access: http://cyberleninka.ru/article/n/metodika-kolichestvennoy-otsenki-riska-v-informatsionnoy-bezopasnosti-oblachnoy-infrastruktury-organizatsii-1. (in Russian).
[16] Nogin V.D. Decision-making under many criteria. Educational and methodical manual. – SPb. Yutas publishing house, 2007. - 104 p. (in Russian).

Поступила в редакцию – 05 марта 2018 г. Окончательный вариант –27 апреля 2018 г.
Received – March 05, 2018. The final version – April 27, 2018.