УДК 004.056.5

А.С. Шабуров А.С. Никитин

Пермский национальный исследовательский политехнический университет,
Пермь, Россия

МОДЕЛЬ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК НА ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Проведен краткий анализ проблемы компьютерных атак как наиболее опасной формы воздействия на объекты критической информационной инфраструктуры. Отмечены особенности традиционных компьютерных атак. Приведена характеристика таргетированной компьютерной атаки, рассмотрены ее особенности. Приведены тенденции к увеличению угроз данного типа. Обоснована необходимость совершенствования систем обнаружения вторжений и выявления компьютерных атак. Представлена задача обнаружения атаки на уровне правил. Сформулированы проблемы классического подхода при формировании правил. Предложен подход для решения задачи обнаружения вторжений на основе машинного обучения, обладающий перечнем преимуществ и недостатков. Сформулированы требования для исключения возможных недостатков распознавания компьютерной атаки. Представлена схема сети лабораторной установки, использованной для записи анализируемого трафика, с последующим выявлением признаков компьютерной атаки. Сформулированы преимущества выбранной модели. Построены графики, иллюстрирующие асимптотическую сложность подходов к классификации трафика, предикат разбиения по индексу Джини. Приведен пример вершины дерева решений, используемого в ансамбле, а также трёх первых уровней дерева решений. Сформулирована метрика качества полученной модели. Проведена оценка модели посредством кросс-валидации на пяти выборках, а также оценена ее точность. В ходе экспериментов над разработанной моделью построена матрица ошибок. Проанализированы результаты и сделаны необходимые выводы о достаточной эффективности разработанной модели. Приведен ранжированный список параметров, которые модель посчитала важными для принятия решения. Проведена оценка работы построенной модели с точки зрения выбранных признаков параметров соединения. Сформулированы направления работы для совершенствования построенной модели.

Ключевые слова: критическая информационная инфраструктура, компьютерная атака, защита информации, система обнаружения вторжений, метод обнаружения аномалий, анализ сигнатур.

A.S. Shaburov, A.S Nikitin

Perm National Research Polytechnic University, Perm, Russian Federation

THE MODEL FOR DETECTING COMPUTER ATTACKS ON OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE

In this paper was made a brief problem analysis of computer attacks as the most dangerous form of exposure to objects of critical information infrastructure. Features of traditional computer attacks were noted. The characteristic of targeted computer attack was given and its features were considered. The trends to an increase in threats of this type were given. The necessity of improving intrusion detection systems and detecting computer attacks has been substantiated. The task of detecting attacks at the rule level was presented. The problems of the classical approach were formulated while forming the rules. An approach for solving the problem of intrusion detection, based on machine learning, has a list of advantages and disadvantages. Requirements were formulated to eliminate possible deficiencies in the recognition of a computer attack. A diagram of the laboratory setup network used to record the analyzed traffic was presented with the subsequent signs identification of a computer attack. The advantages of the selected model were formulated. Graphs illustrating the asymptotic complexity of approaches to traffic classification, predicate partitioning by the Gini index were constructed. An example was given of the vertex of the decision tree used in the ensemble, as well as the first five levels of the decision tree. The quality metric of the resulting model was formulated. The model was evaluated by cross-validation on five samples and its accuracy was estimated. During the experiments on the developed model an error matrix was constructed. The results were analyzed and the necessary conclusions were drawn about the sufficient effectiveness of the developed model. A ranked list of parameters that the model deemed important for decision making was given. The evaluation of the work of the constructed model, in terms of the selected features of the parameters of the connection, has been carried out. The directions of work for the improvement of the constructed model were formulated.

Keywords: critical information infrastructure, computer attack, information security, intrusion detection system, anomaly detection method, signature analysis.

В последнее время значительно обострилась проблема компьютерных атак на информационные системы различного назначения и топологий. Под компьютерной атакой (КА) понимается целенаправленное воздействие на информационные системы и информационно-телекоммуникационные сети программно-техническими средствами, осуществляемое в целях нарушения безопасности информации в этих системах и сетях.

Традиционно обеспечение безопасности информационных систем (ИС) осуществлялось посредствам защиты от типовых массовых информационных атак, таких как компьютерные вирусы, мошенничество, сетевые атаки, внутренние утечки и т.д. Типовые системы защиты информации стали иметь шаблонный вид и содержать в себе набор определенных, однотипных функциональных средств, таких как межсетевые экраны, антивирусные средства и т.п., которые позволяют противостоять традиционным КА. При этом, как показала практика, при

осуществлении воздействия на ИС более сложных по сценарию реализации и используемым технологиям атак, традиционные средства не обеспечивают заданный уровень безопасности информации.

Кроме того, тенденцией последних лет стало появление узконаправленных компьютерных атак (целевых, таргетированных), целью которых являются конкретные коммерческие или государственные организации и их вычислительные сети. Большинство аналитических прогнозов, проводимых в данной области, свидетельствует о том, что в ближайшее время количество подобных атак будет активно возрастать [1, 2, 3]. Это обусловливает необходимость исследования проблемы и поиска эффективных с точки зрения защищенности информационной составляющей, решений.

Значительную роль в повышении эффективности ИС сыграло внедрение современных комплексных подходов к безопасности (DLP, SIEM, IDS). В то же время не все из комплексных и дорогостоящих решений в области информационной безопасности позволяли решить проблему компьютерных атак.

Разнообразие вариантов негативного информационного воздействия, которые могли бы служить объектами исследований, требует разработки их адекватного модельного представления с учетом сохранения адекватности модели действительному образу атаки. Понятие адекватности моделей следует рассматривать в двух аспектах: адекватность прототипу (корректность описания соответствующей атаки) и адекватность главной цели – применение адекватных мер противодействия со стороны системы защиты информации [4].

Одной из наиболее важных с точки зрения обнаружения и локализации КА на ИС является система обнаружения вторжений [5]. Разработка систем обнаружения вторжений (intruder detection system, IDS), как правило, выполняется с использованием списка правил (сигнатур) [6, 7].

Решение задачи обнаружения атаки на уровне правил, составленных администратором безопасности, имеет следующий вид (например, правила для IDS с открытым исходным кодом Suricata):

alert tcp $EXTERNAL_NET any -> $NET $SSH_PORT (msg:"Possible SSH brute forcing!"; threshold: type both, track by_src, count 5, seconds 30; sid:1;)

При этом существуют проблемы классического подхода формирования правил:

1. Сложность составления правил и рассмотрения всех возможных случаев атак.

2. Постоянная угроза возможности появления новых способов проникновения в сеть, для которых ещё не обновлены правила в IDS.

В данной статье предлагается иной подход к решению задачи обнаружения вторжений, на основе машинного обучения, к преимуществам которого можно отнести [6]:

1. Возможность работы в изменяющихся условиях без переконфигурирования системы.

2. Возможность обнаружения новых, ранее не исследованных угроз сетевой безопасности.

3. Отсутствие высоких требований к уровню технических знаний и квалификации администраторов безопасности.

При этом к недостаткам предлагаемого подхода, обусловленным стохастической природой алгоритмов ML, можно отнести следующие проблемы [5]:

1) неполное обнаружение угроз;

2) ложные срабатывания системы обнаружения вторжений;

3) невозможность определить основание принятия определенного решения предлагаемым алгоритмом.

Невозможность исключения вышеназванных недостатков требует выполнения следующих требований:

1) выбора такой последовательности и параметров алгоритмов машинного обучения, которые могут быть легко интерпретируемы;

2) выбора такого алгоритма, решения которого могут быть похожи на ход мыслей человека (администратора безопасности сети);

3) выбора наиболее быстрого алгоритма выполнения задачи, способного оперативно обрабатывать трафик в режиме реального времени.

Для разработки модели обнаружения компьютерных атак использована база данных UNSW-NB 15, разработанная сотрудниками Cyber Range Lab of the Australian Centre for Cyber Security [8, 9].

На рис. 1 представлена схема сети лабораторной установки, использованной для записи анализируемого трафика, с последующим выявлением признаков КА.

В настоящее время разработано множество подходов для извлечения информации о сетевых соединениях для последующего интеллектуального анализа [10, 11, 12], в том числе решения, спроектированные

с целью получения максимальной производительности для обработки больших объёмов данных в режиме реального времени [13, 14]. Для машинного обучения были использованы параметры данных, часть из которых представлена на рис. 2.

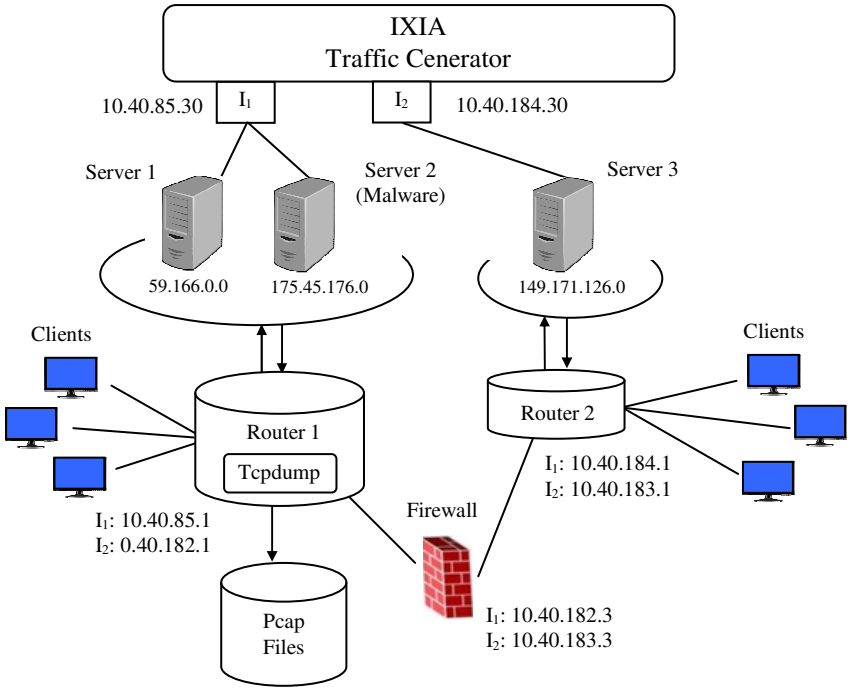

Рис. 1. Схема сети лабораторной установки, использованной для записи трафика

No.	Name	Type	Description
1	srcip	nominal	Source IP address
2	sport	integer	Source port number
3	dstip	nominal	Destination IP address
4	dsport	integer	Destination port number
5	proto	nominal	Transaction protocol
6	state	nominal	Indicates to the state and its dependent proto...
7	dur	Float	Record total duration
8	sbytes	Integer	Source to destination transaction bytes
9	dbytes	Integer	Destination to source transaction bytes
10	sttl	Integer	Source to destination time to live value
11	dttl	Integer	Destination to source time to live value
12	sloss	Integer	Source packets retransmitted or dropped

Рис. 2. Список части параметров используемых данных

В качестве модели машинного обучения предложен случайный лес (бэггинг на деревьях принятия решений). При этом выделены преимущества выбранной модели [15]:

1) скорость работы алгоритма: параллельная работа каждого из деревьев, а также логарифмическая асимптотика спуска по дереву: на рис. 3 представлены оценки сложности классического и предлагаемого подходов систем классификации сетевого трафика;

2) возможность интерпретации: деревья решений предоставляют возможность получить данные о том, насколько часто каждый из критериев задействован для задач классификации.

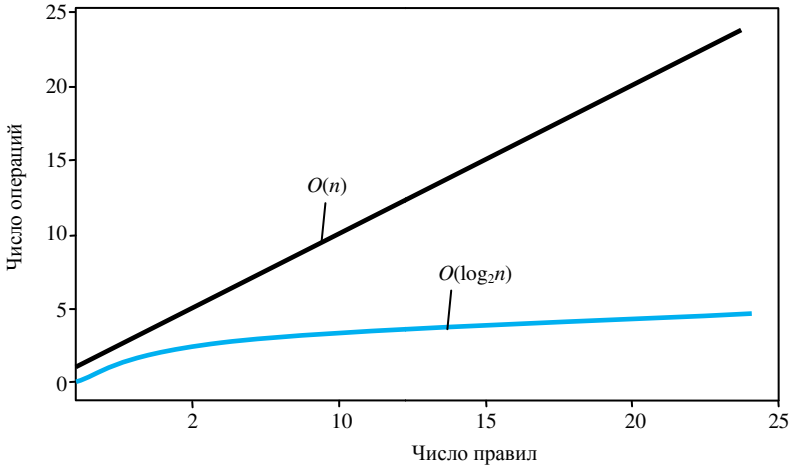

Рис. 3. Асимптотическая сложность подходов к классификации трафика: $O(n)$ – классический подход; $O(\log_2 n)$ – подход с использованием решающих деревьев

Получаем предикат разбиения по индексу Джини:

$$H = \sum_{k=1}^{K} p_k \cdot (1 - p_k). \qquad (1)$$

Таким образом, получаем вершины дерева вида, представленного на рис. 4. С каждой вершиной ассоциируется предикат разбиения выборки по некоторому параметру, а также оценивается качество разбиения, в данном случае, используя индекс Джини.

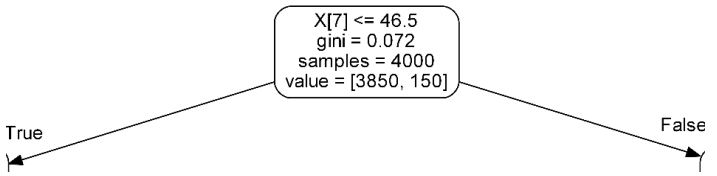

Рис. 4. Пример вершины дерева решений, используемого в ансамбле

Разбиваясь на две группы, наблюдения снова разбиваются и так далее, получая дерево решений, пример которого представлен на рис. 5. Разбиение заканчивается, когда будет выполнено одно из условий остановки построения дерева решений. Как правило, это ограничение на количество разбиений, высоту дерева, количество наблюдений, ассоциированных с листовой вершиной и пр.

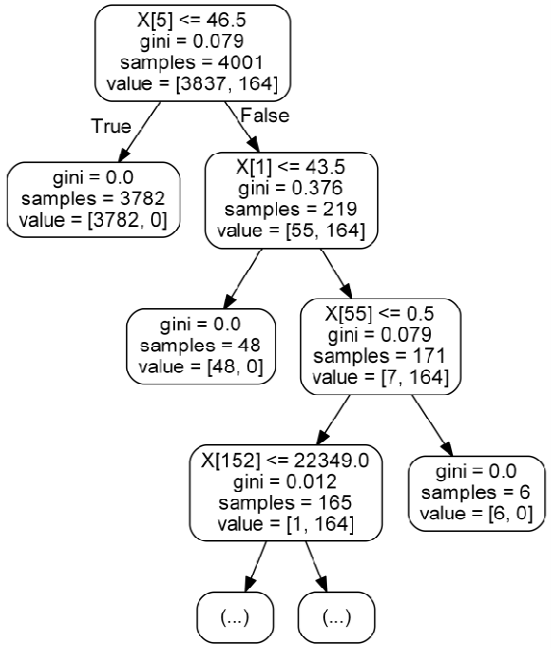

Рис. 5. Пример трёх первых уровней дерева решений

В качестве метрики качества полученной модели была выбрана F-мера – гармоническое среднее между точностью (precision) и полнотой (recall) [16]:

$$F1\text{score} = \frac{2 \cdot \text{precision} \cdot \text{recall}}{\text{precision+recall}}, \tag{2}$$

где

$$\text{recall} = \frac{\text{TP}}{\text{TP+FN}}, \tag{3}$$

$$\text{precision} = \frac{\text{TP}}{\text{TP+FP}}, \tag{4}$$

где TP – верно распознанные вредоносные соединения; FP – false positive, ошибки первого рода; FN – false negative, ошибки второго рода.

Оценка работы модели осуществлялась посредством кросс-валидации на пяти выборках. Подход позволяет оценить обобщающую способность алгоритма на различных подмножествах данных [17]:

$$\text{score} = \frac{1}{N}\sum_{n}^{N} \text{score}_n. \quad (5)$$

Анализ метрик (рис. 6) позволяет сделать вывод о том, что полученная модель имеет достаточную точность определения КА, близкую к 100 %. Однако для задачи классификации с очень несбалансированной выборкой классов (обычных соединений всегда существенно больше, чем вредоносных) наиболее показательными являются метрики precision и recall [18]. Совокупность значений задействованных метрик показывает, что модель достигает приемлемого качества для использования в реальных системах даже при небольшом количестве деревьев принятия решений в ансамбле.

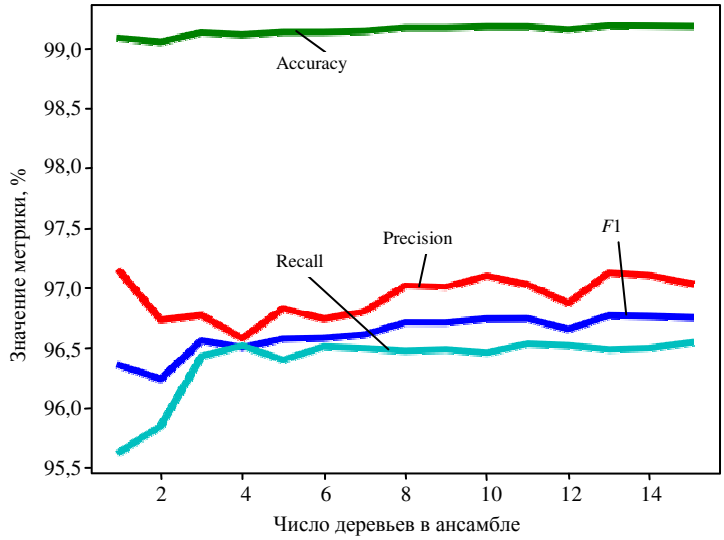

Рис. 6. Метрики полученной модели

В ходе одного из экспериментов над разработанной моделью, была построена матрица ошибок, представленная на рис. 7. Видно, что подавляющая доля тестовых примеров была распознана корректно.

Примечательно, что в ходе эксперимента не было ни одного примера вредоносного соединения, которое было распознано как безопасное. Однако нельзя быть уверенными в том, что это преимущество разработанной модели и подобное свойство будут проявляться на любых других данных.

Ранжированный список параметров, которые модель посчитала важными для принятия решения, следующий: sttl, sport, djit, sintpkt, dtcpb, sbytes, dintpkt, stcpb, dbytes, smeansz, proto_icmp,dsport, dloss, spkts, dpkts, dmeansz, sloss, dttl, proto_tcp, остальные параметры имеют нулевой вклад в решение модели.

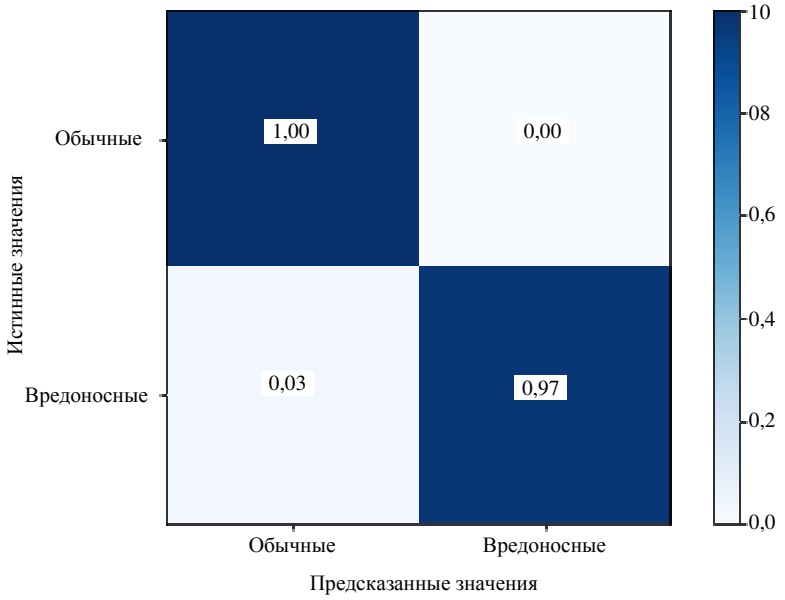

Рис. 7. Нормализованная матрица ошибок модели

При этом выбор признаков получился достаточно логичным:

1. Модель считает важным порт, используемый соединением (sport, dsport), который ассоциируется с конкретным приложением.

2. Модель считает, что UDP-соединения подозрительнее TCP-соединений.

3. Модель считает, что аномальное количество потерянных пакетов в соединении является подозрительным (sloss, dloss).

4. Аналогично этому модель считает подозрительным аномальное число переданных пакетов за соединение (spkts, dpkts), а также переданных байтов (sbytes, dbytes).

5. Модель считает подозрительными соединения, в которых аномальное количество пакетов с небольшим содержимым (smeansz, dmeansz).

Дальнейшая работа по совершенствованию и оценке разработанной модели предполагает ответы на следующие вопросы:

1. На каком основании модель оценивает соединения по ttl (sttl, dttl)?

2. На каком основании модель считает важным признак джиттера (разброс максимального/минимального времени прохождения пакета) для получателя, но не источника?

3. На каком основании модель считает важным начальный sequence number tcp-соединения (stcpb, dtcpb)?

Кроме этого, требуется проведение фильтрации части независимых переменных модели по результатам корреляционного анализа [19]. Вместо фильтрации лишних переменных рекомендуется использовать методы уменьшения размерности, например, метод главных компонентов (principal component analysis, PCA) для замены нескольких коррелирующих переменных одной составной [20].

Таким образом, рост количества компьютерных атак на информационные системы, необходимость защиты объектов КИИ требуют поиска наиболее эффективных способов обнаружения атак. Разработанная модель, позволяет представить работу системы обнаружения вторжений, а также оценить эффективность ее функционирования.

Библиографический список

1. En-Najjary T., Urvoy-Keller. G. A first look at traffic classification in enterprise networks // Proceedings of the 6th International Wireless Communications and Mobile Computing Conference. – ACM, 2010.

2. Обзор задач и методов их решения в области классификации сетевого трафика / А.И. Гетьман, Ю.В. Маркин, Е.Ф. Евстропов, Д.О. Обыденков // Труды ИСП РАН. – 2017. – Т. 29, вып. 3. – С. 117–150.

3. Система фильтрации интернет-трафика на основе методов data mining / В.В. Глазкова, В.А. Масляков, И.В. Машечкин, М.И. Петровский // Программные продукты и системы. – 2008. – № 2.

4. Шабуров А.С. О разработке модели обнаружения компьютерных атак на объекты критической информационной инфраструктуры // Вестник ПНИПУ. Электротехника, информационные технологии, системы управления. – 2018. – № 26. – С. 199–213.

5. Микова С.Ю. Оладько В.С. Модель системы обнаружения аномалий сетевого трафика // Информационные системы и технологии. – 2016. – № 97(5). – С. 115–121.

6. Браницкий А.А. Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. – 2016. – № 2(45). – С. 207–244.

7. Костин Д.В. Шелухин О.И. Сравнительный анализ алгоритмов машинного обучения для проведения классификации сетевого зашифрованного трафика // T-Comm: Телекоммуникации и транспорт. – 2016. – № 9. – С. 46–52.

8. Moustaf N., Slay J. Creating novel features to anomaly network detection using DARPA-2009 data set // Proceedings of the 14th European Conference on Cyber Warfare and Security. – 2015. – P. 204.

9. Moustafa N. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)' // Military Communications and Information Systems Conference, MilCIS 2015. – Canberra, Australia, November 10–12, 2015. – P. 1–6.

10. Петров В.В., Богатырев Е.А. Статистический анализ сетевого трафика // Радиоэлектроника, электротехника и энергетика: тез. докл. X Междунар. науч.-техн. конф. студ. и аспир. – 2003. – Vol. 1.

11. Шелухин О.И., Симонян А.Г. Ванюшина А.В. Эффективность алгоритмов выделения атрибутов в задачах классификации приложений при интеллектуальном анализе трафика // Электросвязь. – 2016. – № 11. – С. 79–85.

12. Farah T., Trajkovic L. Anonym: A tool for anonymization of the Internet traffic // IEEE 2013 International Conference on Cybernetics (CYBCONF). – 2013. – P. 261–266.

13. Risso F., Degioanni L. An Architecture for High Performance Network Analysis // Proceedings of the 6th IEEE Symposium on Computers and Communications (ISCC 2001). – Hammamet, Tunisia, July 2001.

14. Orebaugh Angela, Gilbert Ramirez, Jay Beale. Wireshark & Ethereal network protocol analyzer toolkit. – Elsevier, 2006.

15. Yanyan Zhang, Yao Yuan. Study of database intrusion detection based on improved association rule algorithm // Computer Science and Information Technology (ICCSIT). 3rd IEEE International Conference on. – IEEE 2010. – 2010. – Vol. 4. – P. 673–676.

16. Komer Brent, James Bergstra, Chris Eliasmith. Hyperopt-sklearn: automatic hyperparameter configuration for scikit-learn // ICML workshop on AutoML. – 2014.

17. Safavian S. Rasoul, David Landgrebe. A survey of decision tree classifier methodology // IEEE transactions on systems, man, and cybernetics. – 1991. – 21.3. – P. 660–674.

18. Nascimento Gustavo, Miguel Correia. Anomaly-based intrusion detection in software as a service // Dependable Systems and Networks Workshops (DSN-W). – 2011. – IEEE/IFIP 41st International Conference on. – IEEE, 2011.

19. Andrew Galen & Arora, Raman & Bilmes, Jeff & Livescu K. Deep Canonical Correlation Analysis // Proc. of the 30th Intl. Conference on Machine Learning. – 2013.

20. Tharwat Alaa. Principal component analysis – a tutorial // International Journal of Applied Pattern Recognition. – 2016. – Vol. 3. – P. 197–240. DOI: 10.1504/IJAPR.2016.079733

References

1. En-Najjary T., Urvoy-Keller. G. A first look at traffic classification in enterprise networks. *Proceedings of the 6th International Wireless Communications and Mobile Computing Conference*. ACM, 2010.

2. Get'man A.I., Markin Iu.V., Evstropov E.F., Obydenkov D.O. Obzor zadach i metodov ikh resheniia v oblasti klassifikatsii setevogo trafika [A survey of problems and solution methods in network traffic classification]. *Trudy Institut sistemnogo programmirovaniia Rossiiskoi akademii nauk*, 2017, vol. 29, iss. 3, pp. 117-150.

3. Glazkova V.V., Masliakov V.A., Mashechkin I.V., Petrovskii M.I. Sistema fil'tratsii internet-trafika na osnove metodov data mining [Internet traffic filtering system based on data mining approach]. *Programmnye produkty i sistemy*, 2008, no. 2.

4. Shaburov A.S. O razrabotke modeli obnaruzheniia komp'iuternykh atak na ob"ekty kriticheskoi informatsionnoi infrastruktury [On the development of a model for detecting computer attacks on objects of critical information infrastructure]. *Vestnik Permskogo natsional'nogo issledovatel'skogo politekhnicheskogo universiteta. Elektrotekhnika, informatsionnye tekhnologii, sistemy upravleniia*, 2018, no. 26, pp. 199-213.

5. Mikova S.Iu. Olad'ko V.S. Model' sistemy obnaruzheniia anomalii setevogo trafika [Network traffic anomaly detection system model]. *Informatsionnye sistemy i tekhnologii*, 2016, no. 97(5), pp. 115-121.

6. Branitskii A.A. Kotenko I.V. Analiz i klassifikatsiia metodov obnaruzheniia setevykh atak [Analysis and classification of methods for network attack detection]. *Trudy Sankt-Peterburgskogo instituta informatiki i avtomatizatsii Rossiiskoi akademii nauk*, 2016, no. 2(45), pp. 207-244.

7. Kostin D.V. Shelukhin O.I. Sravnitel'nyi analiz algoritmov mashinnogo obucheniia dlia provedeniia klassifikatsii setevogo zashifrovannogo trafika [Comparsion of machine learning algorithms for encrypted traffic classification]. *T-Comm: Telekommunikatsii i transport*, 2016, no. 9, pp. 46-52.

8. Moustaf N., Slay J. Creating novel features to anomaly network detection using DARPA-2009 data set. *Proceedings of the 14th European Conference on Cyber Warfare and Security*, 2015, 204 p.

9. Moustafa N. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)'. *Military Communications and Information Systems Conference, MilCIS 2015*. Canberra, Australia, November 10-12, 2015, pp. 1-6.

10. Petrov V.V., Bogatyrev E.A. Statisticheskii analiz setevogo trafika [Statistical analysis of network traffic]. *Radioelektronika, elektrotekhnika i energetika. Tezisy dokladov X Mezhdunarodnoi nauchno-tekhnicheskoi konferentsii studentov i aspirantov*, 2003, vol. 1.

11. Shelukhin O.I., Simonian A.G. Vaniushina A.V. Effektivnost' algoritmov vydeleniia atributov v zadachakh klassifikatsii prilozhenii pri intellektual'nom analize trafika [Efficiency of attribute allocation algorithms in application classification problems in traffic mining]. *Elektrosviaz'*, 2016, no. 11, pp. 79-85.

12. Farah T., Trajkovic L. Anonym: A tool for anonymization of the Internet traffic. *In IEEE 2013 International Conference on Cybernetics (CYBCONF)*, 2013, pp. 261-266.

13. Risso F., Degioanni L. An Architecture for High Performance Network Analysis. *Proceedings of the 6th IEEE Symposium on Computers and Communications (ISCC 2001)*. Hammamet, Tunisia, July 2001.

14. Orebaugh Angela, Gilbert Ramirez, Jay Beale. Wireshark & Ethereal network protocol analyzer toolkit. Elsevier, 2006.

15. Yanyan Zhang, Yao Yuan. Study of database intrusion detection based on improved association rule algorithm. *Computer Science and Information Technology (ICCSIT), 2010, 3rd IEEE International Conference on. IEEE*, 2010, vol. 4, pp. 673-676.

16. Komer Brent, James Bergstra, Chris Eliasmith. Hyperopt-sklearn: automatic hyperparameter configuration for scikit-learn. *CML workshop on AutoML*, 2014.

17. Safavian S. Rasoul, David Landgrebe. A survey of decision tree classifier methodology. *IEEE transactions on systems, man, and cybernetics*, 1991, 21.3, pp. 660-674.

18. Nascimento Gustavo, Miguel Correia. Anomaly-based intrusion detection in software as a service. *Dependable Systems and Networks Workshops (DSN-W), 2011, IEEE/IFIP 41st International Conference on. IEEE*, 2011.

19. Andrew Galen & Arora, Raman & Bilmes, Jeff & Livescu K. Deep Canonical Correlation Analysis. *Proc. of the 30th Intl. Conference on Machine Learning*, 2013.

20. Tharwat Alaa. Principal component analysis - a tutorial. *International Journal of Applied Pattern Recognition*, 2016, vol. 3, pp. 197-240. DOI: 10.1504/IJAPR.2016.079733

Сведения об авторах

Шабуров Андрей Сергеевич (Пермь, Россия) – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: shans@at.pstu.ru).

Никитин Алексей Сергеевич (Пермь, Россия) – студент Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: siriousbiz@yandex.ru).

About the authors

Shaburov Andrey Sergeevich, (Perm, Russian Federation) is a Ph.D. in Technical Sciences, Associate Professor of the Department of Automation and Telemechanics Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: shans@at.pstu.ru).

Nikitin Aleksey Sergeevich (Perm, Russian Federation) is a Student Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: siriousbiz@yandex.ru).

Получено 17.01.2019