СБОРНИК **НАУЧНЫХ ТРУДОВ НГТУ. – 2019. – № 3–4 (96).** – 165–176

УДК 004.054.53 DOI: 10.17212/2307-6879-2019-3-4-165-176

ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ*

В.А. ТАБАКАЕВА[1], В.В. СЕЛИФАНОВ[2], В.Р. АН[3], С.А. БУЛАРГА[4], А.С. ВОРОЖЦОВ[5]

[1] *630108, РФ, г. Новосибирск, ул. Плахотного, 10, Сибирский государственный университет геосистем и технологий, магистрант кафедры фотоники и приборостроения. E-mail: tabakaeva1997@mail.ru*

[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, старший преподаватель кафедры защиты информации. E-mail: sfo1@mail.ru*

[3] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, магистрант кафедры вычислительной техники. E-mail: vovan2011nsk@mail.ru*

[4] *111024, РФ, г. Москва, ул. Авиамоторная, 8а, Московский технический университет связи и информатики, доцент кафедры интеллектуальных систем в управлении и автоматизации. E-mail: s.bularga@gmail.ru*

[5] *111024, РФ, г. Москва, ул. Авиамоторная, 8а, Московский технический университет связи и информатики, канд. техн. наук, доцент кафедры интеллектуальных систем в управлении и автоматизации. E-mail: as.vorojcov@mail.ru*

Рассматривается проблема использования интеллектуальных систем в управлении информационной безопасностью объектов критической информационной инфраструктуры. В настоящее время процесс развития информационных технологий достиг точки перехода на повсеместное использование различных интеллектуальных систем. При этом отмечается их применение и в сфере обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Проводится анализ использования различных интеллектуальных систем в области кибербезопасности, при этом условно выделяются две группы: интеллектуальные системы, применяемые непосредственно в средствах кибербезопасности, и интеллектуальные системы, применяемые для обеспечения эксплуатации систем кибербезопасности значимых объектов информационной инфраструктуры Российской Федерации. Среди последних особое место занимают системы управления параметрами кибербезопасности как основополагающие элементы для обеспечения безопасности в ходе эксплуатации, а также реагирования на внешние и внутренние инциденты с требуемой эффективностью и скоростью. В ходе проводимого исследования выбираются пути решения таких задач, как выбор и обоснование параметров управления информационной безопасностью интеллектуальной системы, а также критериев оценки эффективности управления. Для их

* *Статья получена 01 ноября 2019 г.*

решения предлагается применение среды имитационного моделирования AnyLogic, в ходе которого с относительно невысокими расходами можно провести выбор и обоснование применения интеллектуальных систем, критериев эффективности управления, а также оценить эффективность управления системой кибербезопасности как с применением интеллектуальных систем, так и без них; получить однозначный вывод не только о необходимости применения той или иной интеллектуальной системы, но и о разнице в качестве управления.

Ключевые слова: интеллектуальные системы, информационная безопасность, кибербезопасность, значимый объект, критическая информационная инфраструктура, параметры информационной безопасности, оценка эффективности, критерии оценки эффективности управления, имитационное моделирование

ВВЕДЕНИЕ

Системы информационной безопасности (далее – ИБ) должны обеспечивать непрерывное функционирование информационной системы, реализовывать меры защиты от внешних и внутренних угроз. Достичь нужного результата можно с использованием средств защиты информации. В одной информационной системе могут быть использованы десятки и даже сотни средств защиты.

Например, для реализации Приказа № 239 ФСТЭК зачастую необходимо использовать многокомпонентные системы, составленные из продуктов разных производителей следующих видов средств защиты:

– средства управления доступом;
– идентификации и аутентификации;
– средства обнаружения вторжений;
– средства контроля машинных носителей информации;
– средства антивирусной защиты;
– межсетевые экраны;
– средства доверенной загрузки;
– средства криптографической защиты;
– DLP;
– DPI;
– IDM;
– SIEM;
– UDP.

При этом для работы даже средних по размерам сетей (от 1000 рабочих мест) сил одного подразделения уже не хватает, ведь надо обработать большое количество событий ИБ, поступающих не только от разных средств защиты, но и от других компонентов инфраструктуры.

При этом допустимое время реакции на цепочки событий в системе становится всё меньше, человеческому коллективу необходимы интеллектуальные помощники.

Интеллектуальные системы используются непосредственно в системах защиты информации и для управления ИБ. На данный момент рекомендаций по использованию интеллектуальных систем в ИБ нет. Поэтому данная тема является актуальной.

1. ПОСТАНОВКА ЗАДАЧИ

Главной проблемой, затрудняющей повышение качества управления параметрами ИБ, является непостоянность параметров объекта управления и постоянное изменение требований к качеству регулирования в процессе работы.

Для реализации мер необходимо разработать рекомендации по управлению параметрами ИБ с использованием интеллектуальных систем в среде имитационного моделирования Anylogic. В настоящей работе объектом исследования будет процесс управления параметрами информационной безопасности, предметом – применение интеллектуальных систем в управлении параметрами информационной безопасности.

В ходе исследования нужно решить следующие задачи:

1) анализ применения интеллектуальных систем для управления параметрами информационной безопасности;

2) выбор и обоснование параметров управления информационной безопасностью, интеллектуальной системы и критериев оценки эффективности управления;

3) построение модели управления параметрами информационной безопасности в среде Anylogic;

4) оценка эффективности управления параметрами информационной безопасности.

2. АНАЛИЗ ПРИМЕНЕНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

На данный момент интеллектуальные системы применяются в следующих системах информационной безопасности.

- Биометрические системы идентификации на основе интеллектуальных систем активно применяются в банковской сфере, всё чаще заменяют или дополняют ввод классических паролей, используются в системах контроля и управления доступом.

Существует несколько способов реализации биометрической идентификации, например нейросетевые алгоритмы. Обобщенная блок-схема нейросе-

тевой системы биометрической идентификации личности, приведенная на рис. 1, отражает следующие основные этапы обработки информации:

1) измерение биометрических данных пользователя с помощью сенсоров (входных преобразователей);

2) извлечение информативных (инвариантных) биометрических признаков;

3) построение нейросетевого биометрического эталона пользователя;

4) реализация решающего правила на основе нейросети.

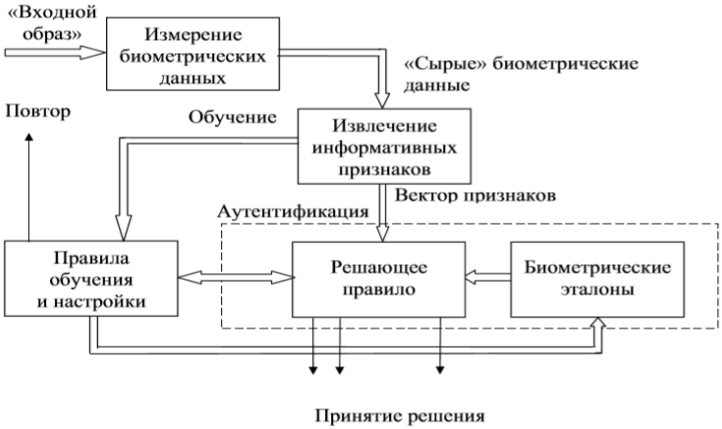

Рис. 1. Обобщенная блок-схема нейросетевой системы биометрической идентификации

- Системы обнаружения вторжений (далее – СОВ) на основе интеллектуальных систем используются для обнаружения, предупреждения, реагирования на инциденты и ликвидацию последствий компьютерных атак. Принцип реализации большинства современных СОВ сетевого уровня основывается на использовании различных методов поиска сигнатур атак, т. е. специфических признаков (индикаторов) того, что передача сетевого трафика осуществляется в рамках той или иной атаки на информационную систему. Процесс обработки информации в СОВ при этом включает в себя следующие этапы (рис. 2):

1) определение перечня признаков (параметров);

2) предварительная обработка параметров;

3) распознавание атак (классификация).

На первом этапе осуществляется захват трафика сети. Сбор необходимых данных производится с помощью специального программного модуля – сниффера пакетов, который перехватывает все пакеты, приходящие по прото-

колу TCP, и осуществляет их фильтрацию. В качестве первичных признаков (параметров), характеризующих анализируемый трафик, в данном случае выступают значения полей заголовков сетевых пакетов.

Рис. 2. Схема процесса обработки информации в СОА

Второй этап связан с выделением (на базе входных данных) наиболее существенных параметров, характеризующих активность сети и представленных в такой форме, в которой они наиболее эффективно могут использоваться для их последующей обработки с помощью классификатора.

Третий этап заключается в обнаружении и распознавании атак. Использование нейросети на данном этапе является более предпочтительным по сравнению с классическими СОВ, осуществляющими простое сравнение данных заголовков пакетов с известными сигнатурами атак, поскольку нейросеть всегда пытается определить, насколько похожи признаки текущей сетевой активности на образцы атак из обучающей выборки. В силу способности нейросети к обобщению, при достаточном объеме и представительности обучающей выборки нейросеть может экстраполировать свои знания об известных видах сетевых атак на неизвестные виды. Решающую роль в данном случае играет выбор архитектуры нейросети, адекватной поставленной задаче обнаружения вторжений.

- Интеллектуальные системы антивирусной защиты применяются для контроля каналов проникновения вирусов, для защиты от вирусов, «червей», нежелательных программ, для оповещения при «заражении», для «лечения»

от вирусов. Системы антивирусной защиты, так же как и СОВ, основываются на использовании методов сигнатурного анализа для борьбы с вирусами.

- Средства анализа и управления информационными рисками на основе интеллектуальных систем применяются для определения потенциального ущерба от реализации атаки с использованием существующих в системе уязвимостей и вероятности реализации атаки. Для управления рисками применяется когнитивное моделирование с целью использовать неполную, нечеткую или даже противоречивую информацию об объекте исследования, которой располагают эксперты, выявить наиболее существенные, значимые взаимосвязи, определить «веса» факторов, влияющих на изучаемую проблему, в данном случае проблему анализа рисков и построения эффективной системы управления ИБ.

После анализа интеллектуальных систем планируется провести выбор и обоснование интеллектуальной системы для управления параметрами информационной безопасности в среде имитационного моделирования Anylogic (схема управления изображена на рис. 3).

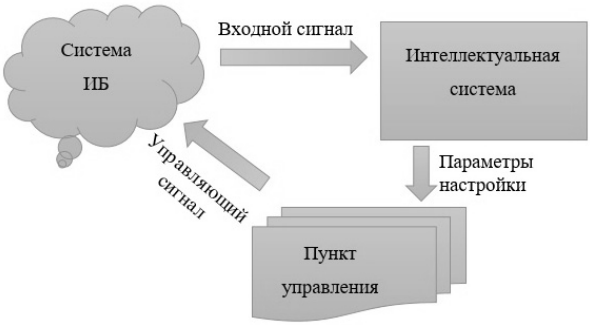

Рис. 3. Схема управления параметрами ИБ

ЗАКЛЮЧЕНИЕ

В статье проанализированы две группы интеллектуальных систем информационной безопасности: интеллектуальные системы, применяемые непосредственно в средствах кибербезопасности, и интеллектуальные системы, применяемые для обеспечения эксплуатации систем кибербезопасности значимых объектов информационной инфраструктуры Российской Федерации. В дальнейшем будут разработаны модель управления параметрами информационной безопасности и рекомендации по ее использованию.

СПИСОК ЛИТЕРАТУРЫ

1. *Лиховидов В.Н., Герасимец И.В,. Корнюшин П.Н.* Применение нейронных сетей для формирования эталонов в системах биометрической идентификации личности // Известия ТРТУ. – 2006. – № 7 (62). – URL: https://cyberleninka.ru/article/v/primenenie-neyronnyh-setey-dlya-formirovaniya-etalonov-v-sistemah-biometricheskoy-identifikatsii-lichnosti (дата обращения: 19.12.2019).

2. *Гришко А.К., Лукин В.С., Юрков Н.К.* Синтез тестовых образов для оценки стойкости нейросетевых преобразователей в системах биометрической идентификации // Надежность и качество сложных систем. – 2017. – № 2 (18). – URL: https://cyberleninka.ru/article/v/sintez-testovyh-obrazov-dlya-otsenki-stoykosti-neyrosetevyh-preobrazovateley-v-sistemah-biometricheskoy-identifikatsii (дата обращения: 19.12.2019).

3. Нейросетевая технология распознавания рукописных символов в системах биометрической идентификации и аутентификации / Р.И. Гумерова, А.О. Евсеева, А.С. Катасёв, А.П. Кирпичников // Вестник технологического университета. – 2017. – Т. 20, № 5. – URL: https://cyberleninka.ru/article/v/neyrosetevaya-tehnologiya-raspoznavaniya-rukopisnyh-simvolov-v-sistemah-biometricheskoy-identifikatsii-i-autentifikatsii (дата обращения: 19.12.2019).

4. *Сулавко А.Е., Жумажанова С.С., Фофанов Г.А.* Перспективные алгоритмы распознавания динамических биометрических образов в пространстве взаимозависимых признаков // Динамика систем, механизмов и машин. – 2018. – Т. 6, № 4. – URL: https://cyberleninka.ru/article/v/perspektivnye-neyrosetevye-algoritmy-raspoznavaniya-dinamicheskih-biometricheskih-obrazov-v-prostranstve-vzaimozavisimyh-priznakov (дата обращения: 19.12.2019).

5. Fuzzy extractors for biometric identification / N. Li, F. Guo, Y. Mu, W. Susilo, S. Nepal // 2017 IEEE 37th International Conference on Distributed Computing Systems. – 2017. – Vol. 1. – P. 667–677. – DOI: 10.1109/ICDCS.2017.107.

6. *Ghayoumi M., Ghazinour K.* An adaptive fuzzy multimodal biometric system for identification and verification // 2015 IEEE/ACIS 14th International Conference on Computer and Information Science. – Las Vegas, NV, USA, 2015. – P. 137–141. – DOI: 10.1109/ICIS.2015.7166583.

7. *Kaur T., Kaur M.* Cryptographic key generation from multimodal template using fuzzy extractor // 2017 Tenth International Conference on Contemporary Computing (IC3). – Noida, India, 2017. – P. 1–6. – DOI: 10.1109/IC3.2017.8284321.

8. Экспериментальная оценка надежности верификации подписи сетями квадратичных форм, нечеткими экстракторами и персептронами / П.С. Ложникова, А.Е. Сулавкова, А.В. Еременко, Д.А. Волкова // Информационно-управляющие системы. – 2016. – № 5. – URL: https://cyberleninka.ru/

article/v/eksperimentalnaya-otsenka-nadezhnosti-verifikatsii-podpisi-setyami-kvadratichnyh-form-nechetkimi-ekstraktorami-i-perseptronami (дата обращения: 19.12.2019).

9. *Сычугов А.А., Токарев В.Л., Анчишкин А.П.* Обнаружение сетевых атак на основе искусственных иммунных систем // Известия ТулГУ. Технические науки. – 2018. – № 10. – URL: https://cyberleninka.ru/article/v/obnaruzhenie-setevyh-atak-na-osnove-iskusstvennyh-immunnyh-sistem (дата обращения: 19.12.2019).

10. Приказ ФСТЭК от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

11. *Branitskiy A., Kotenko I.* Network attack detection based on combination of neural, immune and neuro-fuzzy classifiers // 2015 IEEE 18th International Conference on Computational Science and Engineering (CSE). – Porto, Portugal, 2015. – P. 152–159. – DOI: 10.1109/CSE.2015.26.

12. *Zhao G., Zhang C., Zheng L.* Intrusion detection using deep belief network and probabilistic neural network // 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC). – Guangzhou, China, 2017. – P. 639–642. – DOI: 10.1109/CSE-EUC.2017.119.

13. *Ioannou L., Fahmy S.* Network intrusion detection using neural networks on FPGA SoCs // 2019 29th International Conference on Field Programmable Logic and Applications (FPL). – Barcelona, Spain, 2019. – P. 232–238. – DOI: 10.1109/FPL.2019.00043.

14. Flow-based malware detection using convolutional neural network / M. Yeo, Y. Koo, Yoon Y., T. Hwang, J. Ryu, J. Song, C. Park // 2018 International Conference on Information Networking (ICOIN). – Chiang Mai, Thailand, 2018. – P. 910–913. – DOI: 10.1109/ICOIN.2018.8343255.

15. Guha S., Yau S., Buduru A. Attack detection in cloud infrastructures using artificial neural network with genetic feature selection // 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech). – Auckland, New Zealand, 2016. – P. 414–419. – DOI: 10.1109/DASC-PICom-DataCom-CyberSciTec.2016.32.

Табакаева Валерия Александровна, магистрант кафедры фотоники и приборостроения Сибирского государственного университета геосистем и технологий. E-mail: tabakaeva1997@mail.ru

Селифанов Валентин Валерьевич, старший преподаватель кафедры защиты информации Новосибирского государственного технического университета. E-mail: sfo1@mail.ru

Ан Владимир Робертович, магистрант кафедры вычислительной техники Новосибирского государственного технического университета. E-mail: vovan2011nsk@mail.ru

Буларга Сергей Андреевич, доцент кафедры интеллектуальных систем в управлении и автоматизации Московского технического университета связи и информатики. E-mail: s.bularga@gmail.ru

Ворожцов Анатолий Сергеевич, кандидат технических наук, доцент кафедры интеллектуальных систем в управлении и автоматизации Московского технического университета связи и информатики. E-mail: as.vorojcov@mail.ru

DOI: 10.17212/2307-6879-2019-3-4-165-176

Intelligent information security management systems*

V.A. Tabakaeva[1], V.V. Selifanov[2], V.R. An[3], S.A. Bularga[4], A.S. Vorozhtsov[5]

[1] *Siberian State University of geosystems and technologies, Plakhotnogo Street, 10, Novosibirsk, 630108, Russian Federation, master of the Department of Photonics and instrumentation. E-mail: tabakaeva1997@mail.ru*

[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, senior lecturer at the Department of information security. E-mail: sfo1@mail.ru*

[3] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, master of computer science Department. E-mail: vovan2011nsk@mail.ru*

[4] *Moscow Technical University of communications and Informatics, 8A Aviamotornaya Street, Moscow, 111024, Russian Federation, associate Professor of the Department of intelligent systems in management and automation. E-mail: s.bularga@gmail.ru*

[5] *Moscow Technical University of communications and Informatics, 8A Aviamotornaya Street, Moscow, 111024, Russian Federation, Ph. D., associate Professor of the Department of intelligent systems in management and automation. E-mail: as.vorojcov@mail.ru*

This article deals with the problem of using intelligent systems in managing information security of critical information infrastructure objects. Currently, the process of information technology development has reached the point of transition to the widespread use of various intel-

* *Received 01 November 2019.*

ligent systems. At the same time, their application is also noted in the sphere of ensuring the security of significant objects of the critical information infrastructure of the Russian Federation. The authors analyze the use of various intelligent systems in the field of cybersecurity, and conditionally distinguish two groups: intelligent systems used directly in cybersecurity tools and intelligent systems used to ensure the operation of cybersecurity systems of significant objects of the information infrastructure of the Russian Federation. Among the latter, cybersecurity management systems have a special place as fundamental elements for ensuring security during operation, as well as responding to external and internal incidents with the required efficiency and speed. In the course of the research, the ways of solving such problems as choosing and justifying the parameters of information security management of an intelligent system, as well as criteria for evaluating the effectiveness of management are selected. To solve them, we propose the use of the AnyLogic simulation environment, during which you can select and justify the use of intelligent systems, management efficiency criteria, and evaluate the effectiveness of cybersecurity system management with or without the use of intelligent systems with relatively low costs. Get an unambiguous conclusion not only about the need to use a particular intellectual system, but also about the difference in the quality of management. There are no recommendations for using intelligent information security management systems.

Keywords: intelligent systems, information security, cybersecurity, significant object, critical information infrastructure, information security parameters, efficiency assessment, criteria for evaluating management effectiveness, simulation

REFERENCES

1. Likhovidov V.N., Gerasimets I.V.Kornyushin P.N. Primenenie neironnykh setei dlya formirovaniya etalonov v sistemakh biometricheskoi identifikatsii lichnosti [Application of neural networks for the formation of standards in biometric identification systems]. *Izvestiya TRTU – Izvestiya TSURE*, 2006, no. 7 (62). Available at: https://cyberleninka.ru/article/v/primenenie-neyronnyh-setey-dlya-formirovaniya-etalonov-v-sistemah-biometricheskoy-identifikatsii-lichnosti (accessed 19.12.2019).

2. Grishko A.K., Lukin V.S., Yurkov N.K. Sintez testovykh obrazov dlya otsenki stoikosti neirosetevykh preobrazovatelei v sistemakh biometricheskoi identifikatsii [Synthesis of test images for assessing the stability of neural network converters in biometric identification systems]. *Nadezhnost' i kachestvo slozhnykh sistem – Reliability and Quality of Complex Systems*, 2017, no. 2 (18). Available at: https://cyberleninka.ru/article/v/sintez-testovyh-obrazov-dlya-otsenki-stoykosti-neyrosetevyh-preobrazovateley-v-sistemah-biometricheskoy-identifikatsii (accessed 19.12.2019).

3. Gumerova R.I., Evseeva A.O., Katasev A.S., Kirpichnikov A.P. Neirosetevaya tekhnologiya raspoznavaniya rukopisnykh simvolov vsistemakh biometricheskoi identifikatsii i autentifikatsii [Neural Network technology for recognizing handwritten characters in biometric identification and authentication sys-

tems]. *Vestnik tekhnologicheskogo universiteta – Herald of Technological university*, 2017, vol. 20, no. 5. Available at: https://cyberleninka.ru/article/v/neyrosetevaya-tehnologiya-raspoznavaniya-rukopisnyh-simvolov-v-sistemah-biometricheskoy-identifikatsii-i-autentifikatsii (accessed 19.12.2019).

4. Sulavko A.E., Zhumazhanova S.S., Fofanov G.A. Perspektivnye algoritmy raspoznavaniya dinamicheskikh biometricheskikh obrazov v prostranstve vzaimozavisimykh priznakov [Perspective neural network algorithms for dynamic biometric pattern recognition in the space of interdependent features]. *Dinamika sistem, mekhanizmov i mashin – Dynamics of Systems, Mechanisms and Machines*, 2018, vol. 6, no. 4. Available at: https://cyberleninka.ru/article/v/perspektivnye-neyrosetevye-algoritmy-raspoznavaniya-dinamicheskih-biometricheskih-obrazov-v-prostranstve-vzaimozavisimyh-priznakov (accessed 19.12.2019).

5. Li N., Guo F., Mu Y., Susilo W., Nepal S. Fuzzy extractors for biometric identification. *2017 IEEE 37th International Conference on Distributed Computing Systems*, 2017, vol. 1, pp. 667–677. DOI: 10.1109/ICDCS.2017.107..

6. Ghayoumi M., Ghazinour K. An adaptive fuzzy multimodal biometric system for identification and verification. *2015 IEEE/ACIS 14th International Conference on Computer and Information Science*, Las Vegas, NV, USA, 2015, pp. 137–141. DOI: 10.1109/ICIS.2015.7166583.

7. Kaur T., Kaur M. Cryptographic key generation from multimodal template using fuzzy extractor. *2017 Tenth International Conference on Contemporary Computing (IC3)*, Noida, India, 2017, pp. 1–6. DOI: 10.1109/IC3.2017.8284321.

8. Lozhnikova P.S., Sulavkoa A.E., Eremenko A.V., Volkova D.A. Eksperimental'naya otsenka nadezhnosti verifikatsii podpisi setyami kvadratichnykh form, nechetkimi ekstraktorami i perseptronami [Experimental evaluation of reliability of signature verification by quadratic form networks, fuzzy extractors and perceptrons]. *Informatsionno-upravlyayushchie sistemy – Information and Control Systems*, 2016, no. 5. Available at: https://cyberleninka.ru/article/v/eksperimentalnaya-otsenka-nadezhnosti-verifikatsii-podpisi-setyami-kvadratichnyh-form-nechetkimi-ekstraktorami-i-perseptronami (accessed 19.12.2019).

9. Sychugov A.A., Tokarev V.L., Anchishkin A.P. Obnaruzhenie setevykh atak na osnove iskusstvennykh immunnykh sistem [Detection of network attack on the basis of artificial immune systems]. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki – News of the Tula state university. Technical sciences*, 2018, no. 10. Available at: https://cyberleninka.ru/article/v/obnaruzhenie-setevyh-atak-na-osnove-iskusstvennyh-immunnyh-sistem (accessed 19.12.2019).

10. FSTEC order N 239 of December 25, 2017 "On approval of requirements for security of significant objects of critical information infrastructure of the Russian Federation". (In Russian).

11. Branitskiy A., Kotenko I. Network attack detection based on combination of neural, immune and neuro-fuzzy classifiers. *2015 IEEE 18th International Conference on Computational Science and Engineering (CSE)*, Porto, Portugal, 2015, pp. 152–159. DOI: 10.1109/CSE.2015.26.

12. Zhao G., Zhang C., Zheng L. Intrusion detection using deep belief network and probabilistic neural network. *2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, Guangzhou, China, 2017, pp. 639–642. DOI: 10.1109/CSE-EUC.2017.119.

13. Ioannou L., Fahmy S. Network intrusion detection using neural networks on FPGA SoCs. *2019 29th International Conference on Field Programmable Logic and Applications (FPL)*, Barcelona, Spain, 2019, pp. 232–238. DOI: 10.1109/FPL.2019.00043.

14. Yeo M., Koo Y., Yoon Y., Hwang T., Ryu J., Song J., Park C. Flow-based malware detection using convolutional neural network. *2018 International Conference on Information Networking (ICOIN)*, Chiang Mai, Thailand, 2018, pp. 910–913. DOI: 10.1109/ICOIN.2018.8343255.

15. Guha S., Yau S., Buduru A. Attack detection in cloud infrastructures using artificial neural network with genetic feature selection. *2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)*, Auckland, New Zealand, 2016, pp. 414–419. DOI: 10.1109/DASC-PICom-DataCom-CyberSciTec.2016.32.

Для цитирования:

Интеллектуальные системы управления информационной безопасностью / В.А. Табакаева, В.В. Селифанов, В.Р. Ан, С.А. Буларга, А.С. Ворожцов // Сборник научных трудов НГТУ. – 2019. – № 3–4 (96). – С. 165–176. – DOI: 10.17212/2307-6879-2019-3-4-165-176.

For citation:

Tabakaeva V.A., Selifanov V.V., An V.R., Bularga S.A., Vorozhtsov A.S. Intellektual'nye sistemy upravleniya informatsionnoi bezopasnost'yu [Intelligent information security management systems]. *Sbornik nauchnykh trudov Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta – Transaction of scientific papers of the Novosibirsk state technical university*, 2019, no. 3–4 (96), pp. 165–176. DOI: 10.17212/2307-6879-2019-3-4-165-176.