ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056.57
DOI: 10.21822/2073-6185-2023-50-2-83-89 Оригинальная статья /Original Paper

Оценка уровня защищенности (безопасности функционирования) автоматизированных систем на основе их уязвимостей, формализованная при помощи теории систем массового обслуживания

А.О. Ефимов, Е.А. Рогозин
Воронежский институт МВД России,
394065, г. Воронеж, пр. Патриотов, 53, Россия

Резюме. Цель. Целью работы является разработка методологического аппарата, а также математической модели на основе теории систем массового обслуживания, предназначенных для оценки уровня защищенности автоматизированных систем. **Метод.** В качестве математического аппарата рассматривается теория систем массового обслуживания. В частности, проблема устранения уязвимостей рассматривалась как многоканальная СМО с неограниченной очередью. В качестве входящего потока заявок рассматривался поток обнаруженных уязвимостей автоматизированной системы. Система за счет возможности обнаружения множества уязвимостей за короткий срок обладает очередью из уязвимостей. В качестве каналов обслуживания рассматриваются специалисты информационной безопасности, ответственные за устранение уязвимостей в данной системе. Несмотря на возможность взаимопомощи между специалистами, в данной работе рассматривается ситуация, когда каждому сотруднику ставится задача по устранению конкретной уязвимости. Выходящим потоком заявок является поток устраненных уязвимостей автоматизированной системы. **Результат.** Разработан методологический и математический аппарат оценки уровня защищенности автоматизированных систем на основе их уязвимостей и процесса устранения уязвимостей. В качестве основы применялась теория систем массового обслуживания. Дана оценка уровней защищенности в зависимости от вероятности возникновения очереди из не устраненных уязвимостей. **Вывод.** Разработанная методика может применяться в целях оценки уровня защищенности автоматизированных систем. А также позволяет производить оценку достаточности ресурсов, затрачиваемых на устранение уязвимостей конкретной автоматизированной системы.

Ключевые слова: автоматизированная система, защита информации, система массового обслуживания, оценка защищенности, уязвимость

Для цитирования: А.О. Ефимов, Е.А. Рогозин. Оценка уровня защищенности (безопасности функционирования) автоматизированных систем на основе их уязвимостей, формализованная при помощи теории систем массового обслуживания. Вестник Дагестанского государственного технического университета. Технические науки. 2023; 50(2):83-89. DOI:10.21822/2073-6185-2023-50-2-83-89

Assessment of the level of security (safety of functioning) of automated systems based on their vulnerabilities, formalized using the theory of queuing systems

A.O. Efimov, E.A. Rogozin
Voronezh Institute of the Ministry of Internal Affairs of Russia,
53 Patriotov Str., Voronezh 394065, Russia

Abstract. **Objective**. The aim of the work is to develop a methodological apparatus, as well as a mathematical model based on the theory of queuing systems designed to assess the level of security of automated systems. **Method**. The theory of queuing systems is considered as a mathematical apparatus. In particular, the problem of eliminating vulnerabilities was considered as a multi-channel CFR with an unlimited queue. The flow of detected

vulnerabilities of the automated system was considered as an incoming flow of applications. The system, due to the possibility of detecting many vulnerabilities in a short time, has a queue of vulnerabilities. Information security specialists responsible for eliminating vulnerabilities in this system are considered as service channels. Despite the possibility of mutual assistance between specialists, this paper considers a situation where each employee is tasked with eliminating a specific vulnerability. The outgoing flow of applications is the flow of eliminated vulnerabilities of the automated system. **Result**. A methodological and mathematical apparatus for assessing the level of security of automated systems based on their vulnerabilities and the process of eliminating vulnerabilities has been developed. The theory of queuing systems was used as a basis. The assessment of security levels is given depending on the probability of a queue of unresolved vulnerabilities. **Conclusion**. The developed methodology can be used to assess the level of security of automated systems. And also allows you to assess the sufficiency of resources spent on eliminating vulnerabilities of a specific automated system.

Keywords: automated system, information security, queuing system, security assessment, vulnerability

For citation: A.O. Efimov, E.A. Rogozin. Assessment of the level of security (operational safety) of automated systems based on their vulnerabilities, formalized using the theory of queuing systems. Herald of Daghestan State Technical University. Technical Science. 2023; 50(2):83-89. DOI:10.21822/2073-6185-2023-50-2-83-89

Введение. В настоящее время актуальными являются вопросы оценки защищенности автоматизированных систем. Благодаря огромному множеству вариаций средств вычислительной техники и программного обеспечения данных средств, может расходоваться огромное число ресурсов для поддержания автоматизированных систем в защищенном состоянии.

Ряд вопросов уже ранее рассматривался в работе К.А. Щеглова, А. Ю. Щеглова «Защита атак на уязвимости приложений. Модели контроля доступа» опубликованной во втором номере журнала «Вопросы защиты информации» в 2013 году [1]. Авторы данной работы представили модель оценки вероятности наличия не устранённых уязвимостей в системе, а также вероятность нахождения системы в безопасном состоянии. В качестве математического базиса исследования была использована теория системы массового обслуживания. Если говорить конкретнее, рассматривалась модель системы с бесконечным числом обслуживающих приборов – что, по мнению авторов, являлось изначальным допущением [1]. То есть, рассматривалась ситуация, когда уязвимости в системе устранялись по мере их обнаружения, и наличия способа нейтрализации обнаруженной уязвимости. Несмотря на, безусловно, достигнутый высокий результат, допущение, осуществленное в работе, к сожалению, позволяет рассматривать только «идеальную» систему, и не позволяет проводить полноценную фактическую оценку защищенности с точки зрения наличия уязвимостей.

Данная работа выполнена с учетом результатов вышеприведенного исследования, для построения модели с меньшей неопределенностью исходных данных.

Постановка задачи. Необходимо осуществить построение модели оценки защищенности автоматизированной системы на основе уязвимости используемого программного обеспечения автоматизированной системы.

В качестве математического аппарата рассматривается теория систем массового обслуживания (СМО). В частности, проблема устранения уязвимостей рассматривалась как многоканальная СМО с неограниченной очередью [2-5].

В качестве входящего потока заявок рассматривался поток обнаруженных уязвимостей автоматизированной системы. Система за счет возможности обнаружения множества уязвимостей за короткий срок обладает очередью из уязвимостей.

В качестве каналов обслуживания рассматриваются специалисты информационной

безопасности, ответственные за устранение уязвимостей в данной системе. Несмотря на возможность взаимопомощи между специалистами, в данной работе рассматривается ситуация, когда каждому сотруднику ставится задача по устранению конкретной уязвимости, и он может заниматься только ей.

Выходящим потоком заявок является поток устраненных уязвимостей автоматизированной системы. Заявки обслуживаются в соответствии с приоритетом, а именно в зависимости от оценки критичности уязвимости, рассчитанной по методике CVSS, и методике, представленной ФСТЭК России [6-7]. Наиболее критичные уязвимости обслуживаются в первую очередь.

Стоит отдельно отметить, что в качестве предельно допустимого времени обслуживания заявок принимаются временные значения, указанные в п. 3.2 «Методики оценки уровня критичности уязвимостей программных, программно-аппаратных средств» ФСТЭК России, в части сроков принятия мер по устранению уязвимостей различного уровня критичности [7].

При наличии одной или нескольких не устранённых заявок в системе без превышения вышеуказанных временных значений, полагается, что система функционирует условно безопасно. При наличии одной или нескольких не устраненных уязвимостей, с превышением указанных временных значений, полагается, что система находится под угрозой, и эксплуатация системы должна быть прекращена, до устранения всех заявок с превышением времени нахождения в системе.

Поток заявок случайный, информация об обнаружении новых уязвимостей может быть получена в любое время работы системы.

Рассматриваемая система представлена ниже, в виде структурной схемы на рис. 1:

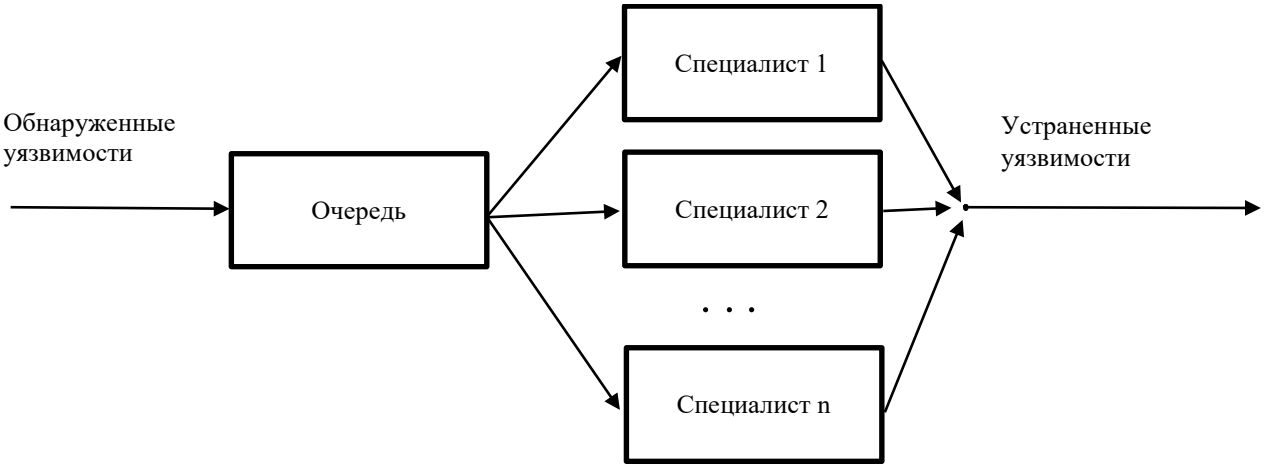

Рис. 1. Структурная схема системы устранения уязвимостей
Fig. 1. A block diagram of the vulnerability elimination system

Отдельно стоит отметить, что число специалистов всегда конечное, а очередь без ограничений по размерам. Устранение уязвимостей может осуществляться различными способами, не оказывающими серьёзного влияния на приведенную СМО.

Методы исследования. Так как необходимо устранение любых уязвимостей, обнаруженных в автоматизированной системе, то берется во внимание тот факт, что по своей сути на очереди нет никаких ограничений. Длина очереди и время нахождения заявок в очереди не оказывают влияние на функционирование СМО. Указанные ранее, временные промежутки, данные на устранение уязвимостей отслеживаются специалистами, и оказывают логическое влияние на уровень защищенности автоматизированной системы.

Как правило, состояния системы нумеруются по числу занятых каналов и числу заявок, находящихся в очереди, т. е. по числу заявок, находящихся в системе [2-5]:

S_0 — система свободна, т. е. каналы не заняты, очереди нет;

S_1 — один канал занят, обслуживается одна заявка, очереди нет;

S_2 — заняты два канала, обслуживаются две заявки, очереди нет;

S_3 — три канала заняты, система обслуживает три заявки, очереди нет; …;

S_n — все n каналов заняты обслуживанием заявок, очереди нет;
S_{n+1} – все n каналов заняты обслуживанием, в очереди стоит одна заявка; …;
S_{n+r} — n каналов заняты обслуживанием, в очереди стоят r заявок; и т.д.

Так как очередь в нашей системе не имеет ограничений, то число состояний стремится к бесконечности, а переход между состояниями происходит с постоянной интенсивностью (интенсивностью заявок) [2-5].

Размеченный граф системы будет выглядеть следующим образом [2-5]:

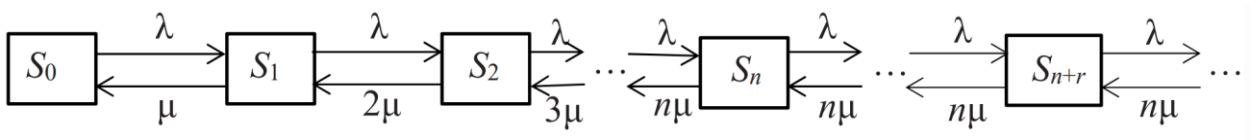

Рис. 2. Размеченный граф системы
Fig. 2. The marked-up graph of the system

Следующая формула обозначает интенсивность обслуживания заявок (загрузки каналов обслуживания).

$$\rho = \frac{\lambda}{\mu} = \lambda * \bar{t}_{об} \quad (1)$$

где, λ – интенсивность потока уязвимостей в ед. времени, μ – интенсивность потока обслуживаний, $\bar{t}_{об}$ – средняя продолжительность устранения уязвимости.

В целях того, чтобы очередь не возрастала до бесконечности, необходимо соблюдение следующего условия: число исполнителей заявок (специалистов) больше, чем число поступающих заявок:

$$\frac{\rho}{n} < 1 \quad (2)$$

где, ρ – интенсивность обслуживания заявок, n – число каналов СМО.

Определим предельную вероятность того, что система свободна, т.е. в системе отсутствуют не устранённые уязвимости:

$$p_0 = (1 + \rho + \frac{\rho^2}{2!} + \frac{\rho^3}{3!} + \cdots + \frac{\rho^n}{n!} + \frac{\rho^{n+1}}{n!(n-p)})^{-1} \quad (3)$$

Так как отказ от обслуживания исполнителем невозможен, то получаем [2]:

$$P_{отк} = 0 \quad (4)$$

Вероятность возникновения очереди из числа не устраненных уязвимостей будет определяться по следующей формуле:

$$P_{оч} = \frac{\rho^{n+1}}{n!(n-p)} p_0 \quad (5)$$

При этом относительная пропускная способность системы равна стопроцентному обслуживанию заявок. Потерь среди поступающих заявок нет. Абсолютная пропускная способность будет равна интенсивности входящего потока заявок. Логично, что интенсивность исходящего потока будет равна интенсивности входящего потока [2-5].

Коэффициент загрузки специалиста отражает среднюю долю времени, в течение которого каждый специалист занят устранением уязвимости. Также он показывает вероятность того, с какой вероятностью выбранный специалист окажется занятым устранением уязвимости в данный момент времени [2]:

$$P_{зан} = k_{заг} = \frac{\rho}{n} \quad (6)$$

Среднее число уязвимостей, ожидающих устранения, будет определяться следующей формулой:

$$L_{оч} = \frac{n}{n-\rho} P_{оч} \quad (7)$$

Число устраняемых в настоящий момент уязвимостей будет равно числу специалистов (каналов обслуживания).

Среднее число уязвимостей в системе будет определяться как сумма среднего числа устраняемых уязвимостей и среднее число уязвимостей в очереди:

$$L_{сист} = P_{оч} + \rho \quad (8)$$

Определим среднее время устранения уязвимости специалистом:

$$T_{об} = \frac{L_{об}}{\lambda} = \frac{\rho}{\lambda} = \frac{1}{\mu} \quad (9)$$

То есть для данного типа систем, среднее время устранения уязвимости по отношению ко всем обнаруженным уязвимостям равно среднему времени устранения одной уязвимости.

Среднее время пребывания уязвимости в очереди на устранение:

$$T_{оч} = \frac{L_{оч}}{\lambda} \quad (10)$$

Среднее время пребывания уязвимости в системе:

$$T_{сист} = \frac{L_{сист}}{\lambda} \quad (11)$$

Именно этот показатель и указывает на защищенность в целом, и определяет безопасность функционирования автоматизированной системы. В случае если обнаруженные уязвимости не находятся в автоматизированной системе (как в СМО) более 24 часов, то можно сделать вывод об условно безопасном функционировании автоматизированной системы вне зависимости от критичности обнаруживаемых уязвимостей [7].

В дополнение к этому может применяться формула (5), по которой можно определить вероятность наличия очереди из не устранённых уязвимостей. Что даст объективную количественную оценку защищенности автоматизированной системы с точки зрения уязвимостей. На основе вероятности наличия очереди, а также превышения времени устранения уязвимостей, можно определить несколько уровней защищенности. Значения $P_{оч}$, будут отражать уровень защищенности АС в зависимости от конфигурации системы устранения уязвимостей и уязвимости компонент. Для перевода количественной оценки в качественную может применяться следующая таблица значений:

Таблица 1. Соответствие оценок защищенности
Table 1. Compliance with security assessments

№	Количественная оценка Quantification	Оценка уровня защищенности Evaluation of the level of security
1.	$0{,}7 \le P_{оч} \le 1{,}0$	Низкий/ Short
2.	$0{,}45 \le P_{оч} < 0{,}7$	Средний/ Average
3.	$0{,}15 \le P_{оч} < 0{,}45$	Выше среднего/ Above average
4.	$P_{оч} < 0{,}15$	Высокий/ High

Примечание: В случае превышения времени, данного на устранение уязвимости различной критичности, дается оценка «низкий уровень защищенности».

Обсуждение результатов. Применение данной математической модели позволяет производить оценку состояния защищенности автоматизированной системы, как со стороны числа специалистов защиты информации с получением необходимого уровня защищенности, так и от необходимого уровня защищенности в сторону выбора числа необходимого числа специалистов.

Под устранением уязвимости в данной работе понимается как устранение путем обновления программных средств, так и принятие достаточных компенсирующих мер [7].

Рис. 3. Схема устранения уязвимостей
Fig. 3. Vulnerability elimination scheme

Недостатком разработанной методики является рассмотрение системы без явной классификации уязвимостей по степени критичности. Предусматривается, что наиболее критичные уязвимости устраняются в первую очередь. Под временем нахождения (нали-

чия) уязвимости в системе, подразумевается временной промежуток с момента обнаружения уязвимости в данной конкретной автоматизированной системе, либо публикация в базах данных уязвимостей об уязвимости конкретного применяемого программного продукта, до момента устранения этих уязвимостей, либо принятия достаточных компенсирующих мер.

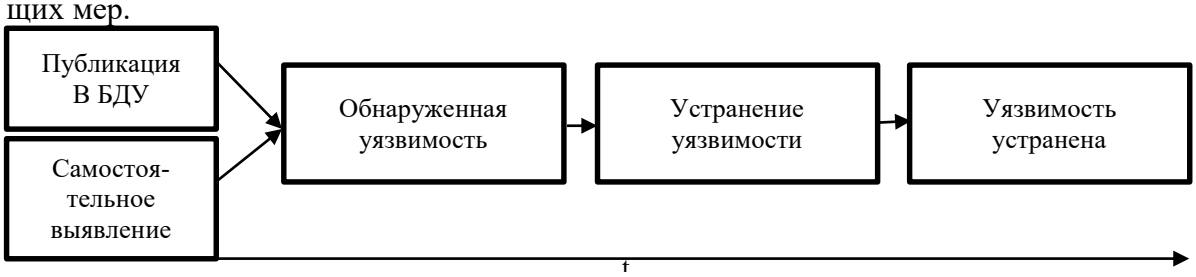

Рис. 4. Схема времени нахождения уязвимости в системе
Fig. 4. The scheme of the time of the vulnerability in the system

Вывод. Разработанная методика может применяться в целях оценки уровня защищенности автоматизированных систем, а также позволяет производить оценку достаточности ресурсов затрачиваемых на устранение уязвимостей конкретной автоматизированной системы. Одним из ключевых аспектов оценки остаются временные интервалы, в рамках которых должны устраняться уязвимости различной критичности.

Библиографический список:

1. Щеглов, К. А. Защита от атак на уязвимости приложений. Модели контроля доступа / К. А. Щеглов, А. Ю. Щеглов // Вопросы защиты информации. – 2013. – № 2(101). – С. 36-43. – EDN QAVHRX.
2. Плескунов, М. А. Теория массового обслуживания: Учебное пособие для студентов вуза, обучающихся по УГН 01.00.00 «Математика и механика» / М. А. Плескунов; Министерство науки и высшего образования Российской Федерации, Уральский федеральный университет имени первого Президента России Б.Н. Ельцина. – Екатеринбург: Издательство Уральского университета, 2022. – 264 с. – ISBN 978-5-7996-3539-8. – EDN RSQUKA.
3. Вентцель, Е.С. Исследование операций / Е.С. Вентцель. – Москва: Советское радио, 1972. – 552 с.
4. Вентцель, Е.С. Исследование операций: Задачи, принципы, методология: учеб. пособие / Е.С. Вентцель. – 5-е изд., стер. – Москва: КноРус, 2010. – 192 с.
5. Саати, Т.Л. Элементы теории массового обслуживания и ее приложение / Т.Л. Саати. – Москва: Советское радио, 1965. – 510 с.
6. Common Vulnerability Scoring System v3.0: Specification Document. FIRST Org. Inc, 2015. -21 p. (https://www.first.org/cvss/specification-document).
7. Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств: утв. ФСТЭК России 28 октября 2022 г.: Методический документ ФСТЭК России от 28.02.2022 г.
8. Коноваленко С.А., Королев И.Д. Выявление уязвимостей информационных систем посредством комбинированного метода анализа параметрических данных, определяемых системами мониторинга вычислительных сетей. Альманах современной науки и образования. 2016, № 11(113), с. 60–66. – EDN XEEDXH.
9. Сердечный А.Л., Тарелкин М.А., Ломов А.А., Симонов К.В. Карты источников, содержащих сведения об уязвимостях программного обеспечения. Информация и безопасность. 2019, т. 22, № 3, с. 411–422. – EDN ZOUMGN.
10. Федорченк А.В., Чечулин А.А., Котенко И.В. Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных сетей. Информационно-управляющие системы. 2014, № 5(72), с. 72–79. – EDN SXXXKH.
11. Сердечный А.Л.,. Герасимов И.В,. Макаров О.Ю и др. Технология выявления сведений об уязвимостях сторонних компонентов программного обеспечения с открытым исходным кодом. Информация и безопасность. 2020, т. 23, № 3, с. 347–364. DOI: http://dx.doi.org/10.36622/VSTU.2020.23.3.003. – EDN PYXOUT.
12. Аветисян А.И., Белеванцев А.А., Чукляев И.И. Технологии статического и динамического анализа уязвимостей программного обеспечения. Вопросы кибербезопасности. 2014, № 3(4), с. 20–28. – EDN SSYPXV.
13. Russell R. et al. Automated Vulnerability Detection in Source Code Using Deep Representation Learning. 17th IEEE International Conference on Machine Learning and Applications (ICMLA), Orlando, FL, USA. 2018, p. 757–762. DOI: http://dx.doi.org/10.1109/ICMLA.2018.00120.

14. Wang T., Wei T., Gu G. and Zou W. TaintScope: A Checksum-Aware Directed Fuzzing Tool for Automatic Software Vulnerability Detection. IEEE Symposium on Security and Privacy, Oakland, CA, USA. 2010, p. 497–512. DOI: http://dx.doi.org/10.1109/SP.2010.37.
15. Lin G., Wen S., Han Q. -L., Zhang J. and Xiang Y. Software Vulnerability Detection Using Deep Neural Networks: A Survey in Proceedings of the IEEE. Oct. 2020, vol. 108, no. 10, p. 1825–1848. DOI: http://dx.doi.org/10.1109/JPROC.2020.2993293.

References:

1. Shcheglov, K. A. Protection against attacks on application vulnerabilities. Access control models / K. A. Shcheglov, A. Yu. Shcheglov. *Questions of information protection*. 2013; 2(101):36-43. (In Russ)
2. Pleskunov, M. A. Theory of queuing: A textbook for university students studying at the USN 01.00.00 “Mathematics and Mechanics” ; Ministry of Science and Higher Education of the Russian Federation, Ural Federal University named after the first President of Russia B.N. Yeltsin. – Yekaterinburg: Ural University Publishing House, 2022; 264. – ISBN 978-5-7996-3539-8.
3. Wentzel, E.S. Operations research / E.S. Wentzel. Moscow: Soviet Radio, 1972; 552 .
4. Wentzel, E.S. Operations research: Tasks, principles, methodology: textbook. manual / E.S. Wentzel. – 5th ed., erased. Moscow: KnoRus, 2010; 192.
5. Saati T.L. Elements of queuing theory and its application. Moscow: Sovetskoe radio, 1965; 510.
6. Common Vulnerability Scoring System v3.0: Specification Document. FIRST Org. Inc, 2015; 21. (https://www.first.org/cvss/specification-document).
7. Methodology for assessing the level of criticality of vulnerabilities of software, hardware and software: approved by the FSTEC of Russia on October 28, 2022: Methodological Document of the FSTEC of Russia dated 02/28/2022.
8. Konovalenko S.A., Korolev I.D. Identification of vulnerabilities of information systems by means of a combined method of analysis of parametric data determined by monitoring systems of computer networks, Al’manah sovremennoj nauki i obrazovaniya. 2016; 11(113): 60–66 (in Russ)
9. Serdechnyj A.L., Tarelkin M.A., Lomov A.A., Simonov K.V. Maps of sources containing information about software vulnerabilities. Informaciya i bezopasnost’. 2019; 22(3): 411–422 (in Russ).
10. Fedorchenko A.V., CHechulin A.A., Kotenko I.V. Research of open databases of vulnerabilities and assessment of the possibility of their application in systems of security analysis of computer networks. Informacionno-upravlyayushchie sistemy. 2014; 5(72):72–79 (in Russ).
11. Serdechnyj A.L., Gerasimov I.V., Makarov O.YU. i dr. Technology for identifying information about vulnerabilities of third-party components of open source software. Informaciya i bezopasnost’. 2020; 23 (3):347–364 (in Russ.).
12. Avetisyan A.I., Belevancev A.A., Chuklyaev I.I. Technologies of static and dynamic analysis of software vulnerabilities. Voprosy kiberbezopasnosti. 2014; 3(4): 20–28 (in Russ).
13. Russell R. et al. Automated Vulnerability Detection in Source Code Using Deep Representation Learning. 17th IEEE International Conference on Machine Learning and Applications (ICMLA), Orlando, FL, USA. 2018; 757–762. DOI: http://dx.doi.org/10.1109/ICMLA.2018.00120.
14. Wang T., Wei T., Gu G. and Zou W. TaintScope: A Checksum-Aware Directed Fuzzing Tool for Automatic Software Vulnerability Detection. IEEE Symposium on Security and Privacy, Oakland, CA, USA. 2010;. 497–512. DOI: http://dx.doi.org/10.1109/SP.2010.37.
15. Lin G., Wen S., Han Q. -L., Zhang J. and Xiang Y. Software Vulnerability Detection Using Deep Neural Networks: A Survey in Proceedings of the IEEE. Oct. 2020;108(10):1825–1848. DOI: http://dx.doi.org/10.1109/JPROC.2020.2993293.

Сведения об авторах:

Ефимов Алексей Олегович, адъюнкт очной формы обучения; ea.aleksei@yandex.ru

Рогозин Евгений Алексеевич, доктор технических наук, профессор, профессор кафедры автоматизированных информационных систем органов внутренних дел; evgenirogozin@yandex.ru

Information about authors:

Aleksey O. Yefimov, Full-time adjunct; ea.aleksei@yandex.ru

Evgeny A. Rogozin, Dr. Sci. (Eng.), Prof., Prof., Department of Automated Information Systems of Internal Affairs Bodies; evgenirogozin@yandex.ru

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/Received 28.04.2023.

Одобрена после рецензирования/ Reviced 20.05.2023.

Принята в печать/Accepted for publication 20.05.2023.