ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056
DOI: 10.21822/2073-6185-2024-51-2-128-136 Оригинальная статья /Original article

CC BY 4.0

Алгоритм функционирования программного комплекса анализа и оценки защищенности программного обеспечения автоматизированных систем органов внутренних дел

А.Д. Попова
Воронежский институт МВД России,
394065, г. Воронеж, пр. Патриотов, 53, Россия

Резюме. Цель. Целью исследования является построение алгоритма функционирования программного комплекса, автоматизирующего процесс анализа и оценки защищенности используемого программного обеспечения и осуществляющего выбор его наиболее защищенной версии для эксплуатации на объектах информатизации органов внутренних дел. **Метод.** В ходе исследования использованы: метод системного подхода к определению показателей защищенности программного обеспечения, метод математической формализации и алгоритмизации процесса анализа и оценки защищенности программного обеспечения для разработки программного кода. **Результат.** Предложен алгоритм функционирования программного комплекса, позволяющий осуществлять анализ и количественную оценку защищенности программного обеспечения автоматизированных систем органов внутренних дел в отношении текущих уязвимостей в режиме реального времени. Алгоритм носит комплексный характер, включая в себя пять составляющих алгоритмов. Описана работа основных блоков алгоритма. **Вывод.** Практическая значимость реализации разработанного алгоритма в виде программного комплекса состоит в возможности выбора оптимальной (наиболее защищенной) версии программного обеспечения для эксплуатации на объектах информатизации органов внутренних дел с целью повышения реальной защищенности служебной информации ограниченного распространения.

Ключевые слова: автоматизированная система, программное обеспечение, защищенность программного обеспечения, анализ и количественная оценка уровня защищенности, алгоритм, программный комплекс

Для цитирования: А.Д. Попова. Алгоритм функционирования программного комплекса анализа и оценки защищенности программного обеспечения автоматизированных систем органов внутренних дел. Вестник Дагестанского государственного технического университета. Технические науки. 2024; 51(2):128-136. DOI:10.21822/2073-6185-2024-51-2-128-136

Algorithm for the functioning of the analysis and evaluation software package security of software of automated systems internal affairs bodies

A.D. Popova
Voronezh Institute of the Ministry of Internal Affairs of Russia,
53 Patriotov Ave., Voronezh 394065, Russia

Abstract. Objective. The purpose of the study is to construct an algorithm for the functioning of a software package that automates the process of analyzing and assessing the security of the software used and selecting its most secure version for use at informatization facilities of internal affairs bodies. **Method.** During the study, we used: a method of a systematic approach to determining software security indicators, a method of mathematical formalization and algorithmization of the process of analyzing and assessing software security for developing program code. **Result.** An algorithm for the functioning of a software complex is proposed that allows for analysis and quantitative assessment of the security of software of automated systems of

internal affairs bodies in relation to current vulnerabilities in real time. The algorithm is complex in nature, including five component algorithms. The operation of the main blocks of the algorithm is described. **Conclusion.** Conclusions are drawn about the importance of the practical implementation of the developed algorithm in the form of a software package that selects the optimal (most secure) version of software for operation at informatization facilities of internal affairs bodies in order to increase the actual security of limited-distribution official information.

Keywords: automated system, software, software security, analysis and quantitative assessment of security level, algorithm, software package

For citation: A.D. Popova. Algorithm for the functioning of the analysis and evaluation software package security of software of automated systems internal affairs bodies . Herald of Daghestan State Technical University. Technical Sciences. 2024; 51(2):128-136. DOI:10.21822/2073-6185-2024-51-2-128-136.

Введение. Характерной особенностью настоящего этапа развития сферы информатизации органов внутренних дел (ОВД) являются ускоряющиеся темпы роста объема и многообразия видов служебной информации ограниченного распространения, хранящейся, обрабатываемой и передаваемой в автоматизированных системах (АС) [1]. Современные АС ОВД, безусловно, следует отнести к объектам критической информационной инфраструктуры, поскольку выход их из строя наносит значительный ущерб интересам личности и государства, приводит к существенным информационным и финансовым потерям. Следовательно, вопросы, связанные с защитой служебной информации ограниченного распространения, циркулирующей на объектах информатизации ОВД, весьма актуальны. Их актуальность основывается на основных положениях Доктрины информационной безопасности (ИБ), в которой отмечается необходимость как повышения защищенности критической информационной структуры и устойчивости ее функционирования, так и развития механизмов обнаружения, защиты и предупреждения информационных угроз [2].

При рассмотрении вопроса обеспечения ИБ современных АС ОВД определяющее значение имеет повышение уровня защищенности используемого программного обеспечения (ПО) [3–5] в процессе эксплуатации в системе – уровня его эксплуатационной информационной безопасности (ЭИБ), под которым в соответствии с [6, 7] понимается свойство ПО функционировать в безопасном состоянии, в том числе, на заданном интервале времени, – без обнаруженных в нем, либо внесенных в него в процессе эксплуатации и неустраненных уязвимостей, позволяющих осуществить несанкционированный доступ (НСД) к информации в АС ОВД. Выбор наиболее защищенной версии ПО для эксплуатации на объектах информатизации ОВД предполагает использование адекватных количественных показателей защищенности ПО [8], а также соответствующих моделей и алгоритмов их аналитического расчета в режиме реального времени, реализованных в программном комплексе анализа и количественной оценки изменения данных показателей в отношении текущих уязвимостей (типов уязвимостей) в ПО[9] в динамике его функционирования в АС ОВД [10].

Постановка задачи. В [11] предложен и обоснован комплексный показатель защищенности ПО в АС ОВД ($\boldsymbol{V}_{\text{з0 ПО}}$), полученный путем агрегирования количественных показателей, позволяющих адекватно оценивать реальную защищенность (ЭИБ) ПО с учетом недостатков его эксплуатации на объектах информатизации ОВД: уровня критичности уязвимостей в ПО – статического показателя защищенности ПО ($\boldsymbol{V}_{\text{кр0}}$); коэффициента готовности ПО к безопасной эксплуатации в отношении уязвимостей, интервального показателя нарушения защищенности ПО, показателя временной защищенности ПО ($\boldsymbol{V}_{\text{г0}}$, $\boldsymbol{V}_{\text{ин0}}$, $\boldsymbol{V}_{\text{вз0}}(\boldsymbol{t})$) – динамических показателей защищенности ПО.

Аналитические модели и алгоритмы расчета данных показателей в соответствии с концепциями пригодности, оптимальности, адаптивизации, описывающими рациональное поведение системы, подробно рассмотрены в [12–14].

Целью данной статьи является построение алгоритма функционирования программного комплекса (ПК), реализующего предложенные модели и алгоритмы, позволяющего автоматизировать процесс анализа и оценки защищенности ПО, а также выбора на этой основе его оптимальной (наиболее защищенной) версии для эксплуатации на объектах информатизации ОВД.

Методы исследования. При проведении исследования используется метод математической формализации и алгоритмизации поставленных задач для разработки программного кода. Комплексный характер проблемы оценивания изменения уровня защищенности ПО в отношении текущих уязвимостей в процессе его функционирования на объектах информатизации ОВД предполагает реализацию системного подхода к определению показателей защищенности ПО.

Обсуждение результатов. Предлагаемый алгоритм функционирования ПК анализа и оценки защищенности ПО АС ОВД представлен на рис.1.

Работу алгоритма можно описать следующим образом.

Блок 1. Формирование совокупности из Z версий исследуемого ПО.

Блок 2. Организация цикла с параметром i для расчета $V_{\text{з0 ПО}i}$.

Блок 3. Ввод i-ой версии ПО.

Блок 4. Тестирование i-ой версии ПО на наличие уязвимостей [15].

Блок 5. Расчет $V_{\text{з0 ПО}i}$ [13] (блок Start) (рис. 2).

Блок 6. Вывод результатов расчета $V_{\text{з0 ПО}i}$.

Блок 7. Проверка выполнения условия по выбору максимального значения $V_{\text{з0 ПО}i}$. При выполнении условия реализуется переход к блоку 8, при невыполнении – к блоку 9.

Блоки 8, 9. Выбор оптимальной (наиболее защищенной) версии ПО.

Блок 10. Вывод номера оптимальной версии ПО – результата работы алгоритма, представленного на рис. 1.

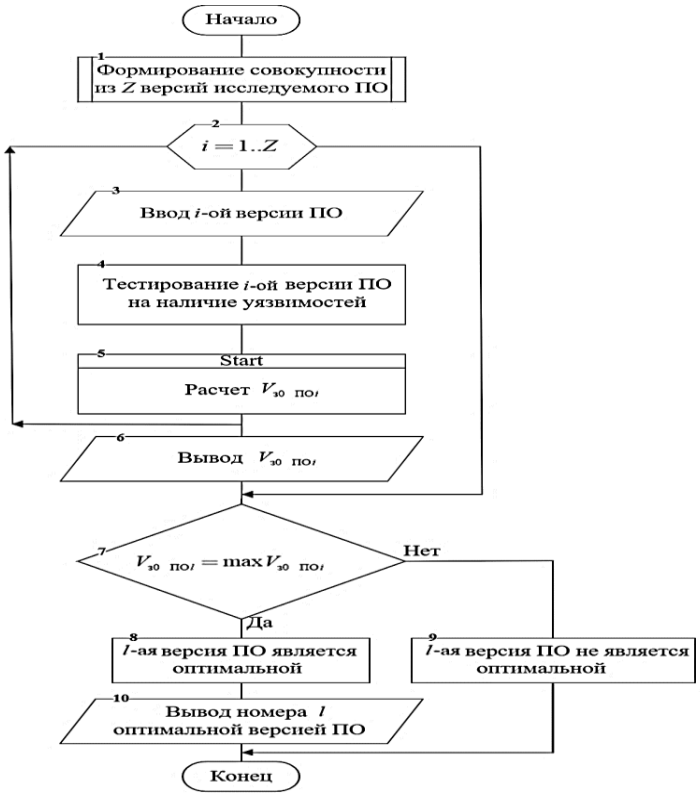

Рис. 1. Алгоритм функционирования ПК анализа и оценки защищенности ПО АС ОВД
Fig. 1. Algorithm for PC functioning of analysis and security assessment of ATS software

Алгоритм аналитического расчета комплексного показателя защищенности ПО в АС ОВД $V_{\text{з0 ПО}}$ (блок Start), разработанный на основе предложенных моделей, представлен на рис. 2.

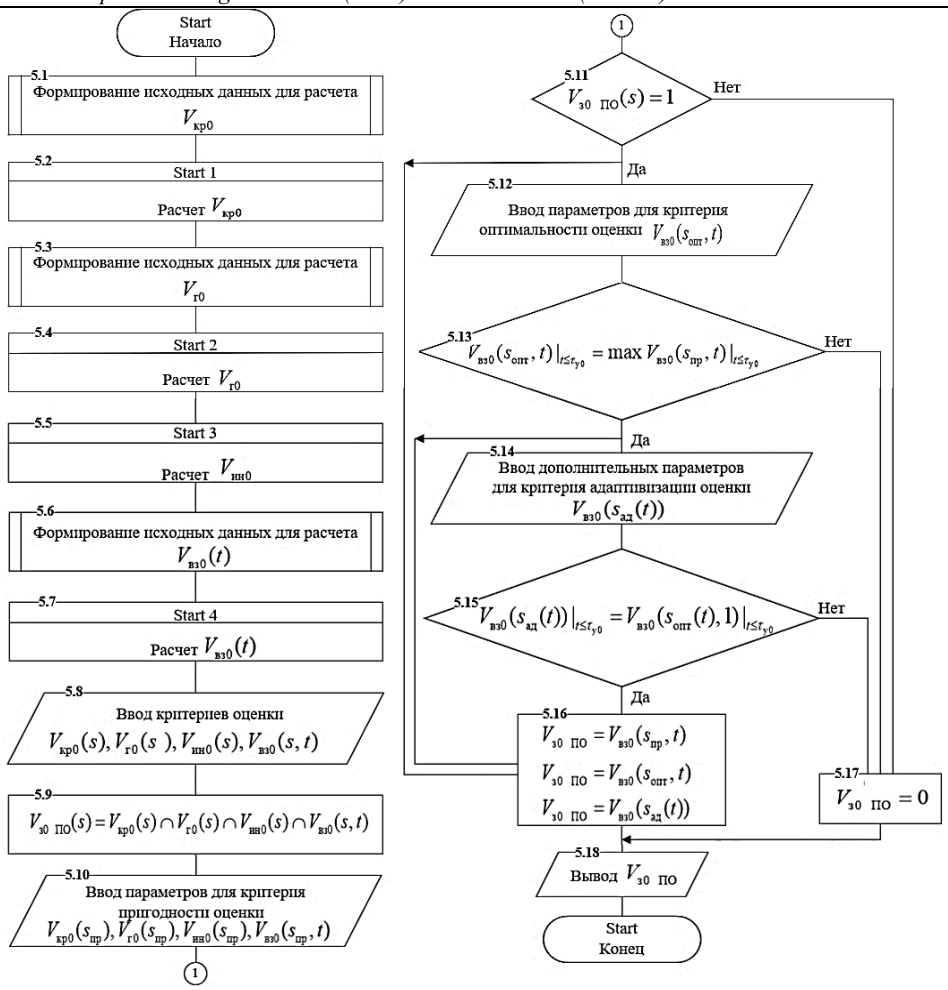

Рис. 2. Алгоритм аналитического расчета комплексного показателя защищенности ПО в АС ОВД

Fig. 2. Algorithm for analytical calculation of a complex indicator of software security in automated air traffic control systems

Блок 5.1. Формирование исходных данных для расчета уровня критичности уязвимостей в ПО АС ОВД ($V_{кр0}$):

– формирование исходных данных для расчета показателя уровня опасности уязвимостей в ПО (I_{cvss0}): показателей базовых метрик (показателей возможности эксплуатации уязвимостей: AV, UI, PR, AC, AT; показателей воздействия: VC, VI, VA, SC, SI, SA), показателя метрик угроз (доступности средств эксплуатации), показателей метрик окружения (корректировки базовых метрик, CR, IR, AR), показателей дополнительных метрик (по необходимости) (S, AU, R, V, RE, U) [16–19];

– формирование исходных данных для расчета показателя влияния уязвимостей в ПО на процесс функционирования АС ОВД, использующей данное ПО (I_{infr0}): показателей K, L, P, весовых коэффициентов рассматриваемых показателей k, l, p в соответствии с таблицей, представленной в [20].

Блок 5.2. Расчет показателя $V_{кр0}$ [13, 14, 21] (блок Start 1) (рис. 3).

Блок 5.3. Формирование исходных данных для расчета коэффициента готовности ПО АС ОВД к безопасной эксплуатации ($V_{г0}$): числа каналов обслуживания (M), количества обслуживающих приборов (C), количества используемых нарушителем текущих уязвимостей в ПО (N), времен выявления и устранения текущих уязвимостей в ПО ($\tau_{вуi}$, $\tau_{уyi}$, $i = 1..N$).

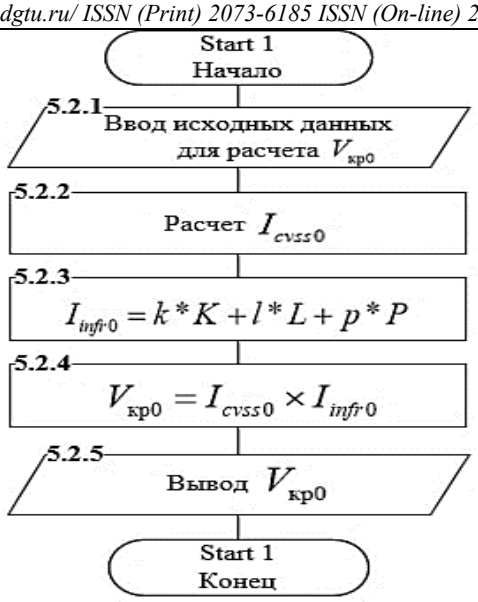

Рис. 3. Алгоритм аналитического расчета уровня критичности уязвимостей в ПО АС ОВД

Fig. 3. Algorithm for analytical calculation of the level of criticality of vulnerabilities in ATS software

Блок 5.4. Расчет показателя $V_{г0}$ [13, 14] (блок Start 2) (рис. 4).

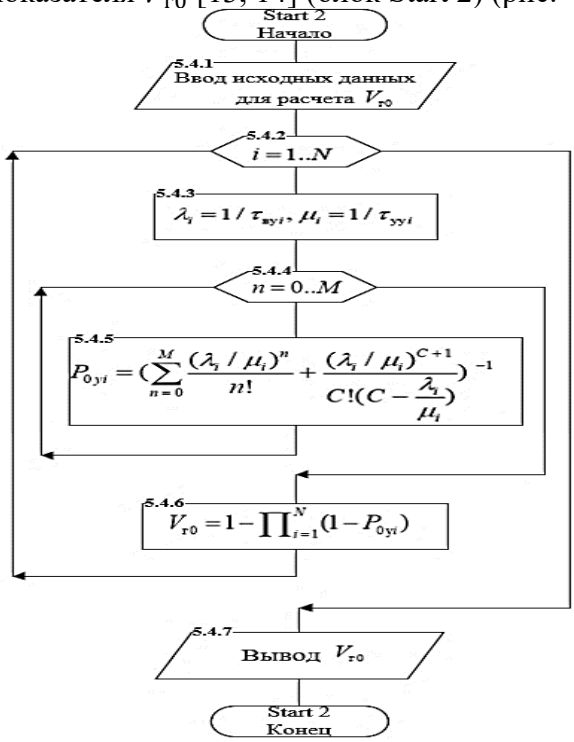

Рис. 4. Алгоритм аналитического расчета коэффициента готовности ПО АС ОВД к безопасной эксплуатации

Fig. 4. Algorithm for analytical calculation of the coefficient of readiness of ATS software for safe operation

Блок 5.5. Расчет интервального показателя нарушения защищенности ПО в АС ОВД ($V_{ин0}$) [13, 14] (блок Start 3) (рис. 5).

Блок 5.6. Формирование исходных данных для расчета показателя временной защищенности ПО в АС ОВД ($V_{вз0}(t)$):

– статистических параметров переходов между состояниями процесса эксплуатации уязвимостей в ПО АС ОВД, характеризующих реализацию нарушителем вредоносных функций: π_{ijr} – мгновенных вероятностей достижения каждого из состояний на этапах

процесса эксплуатации r-ой уязвимости в ПО; τ_{ir} – среднего времени пребывания процесса эксплуатации r-ой уязвимости в i-м состоянии;

– n – общего количества состояний (реализуемых нарушителем вредоносных функций при эксплуатации r-ой уязвимости);

– t – времени реализации вредоносных функций (времени эксплуатации нарушителем r-ой уязвимости в ПО).

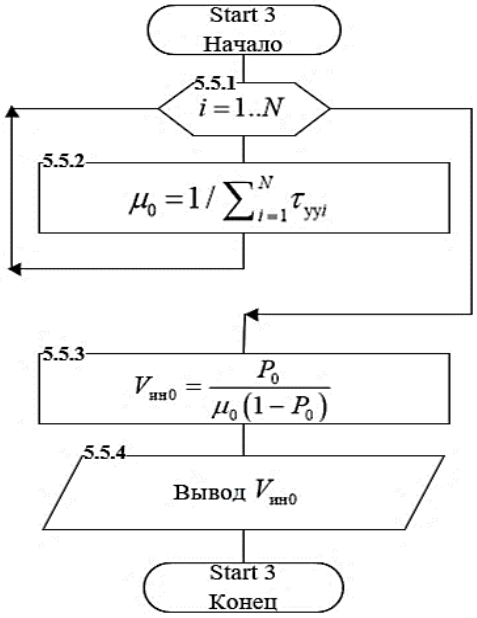

Рис. 5. Алгоритм аналитического расчета интервального показателя нарушения защищенности ПО в АС ОВД

Fig. 5. Algorithm for analytical calculation of the interval indicator of software security violations in automated air traffic control systems

Блок 5.7. Расчет показателя $V_{вз0}(t)$ в программной среде MATLAB R2020b [14] (блок Start 4) (рис. 6).

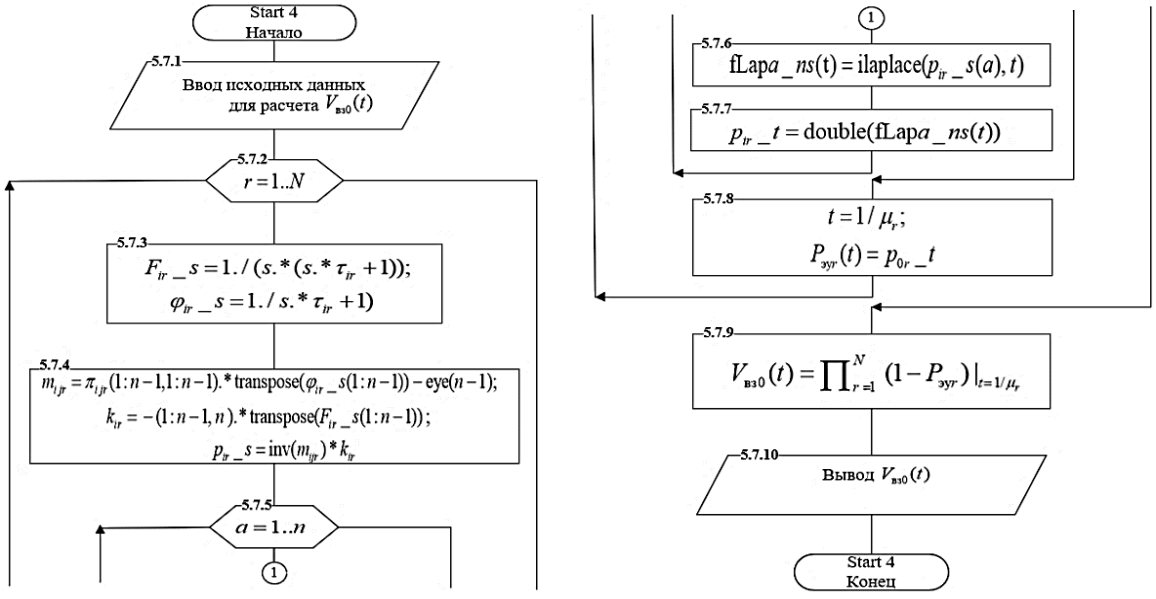

Рис. 6. Расчет показателя $V_{вз0}(t)$ в программной среде MATLAB R2020b [14] (блок Start 4)

Fig. 6. Calculation of the indicator V_(rise0) (t) in the MATLAB R2020b software environment [14] (Start 4 block)

Блок 5.8. Ввод критериев оценки $V_{кр0}(s)$, $V_{г0}(s)$, $V_{ин0}(s)$, $V_{вз0}(s,t)$ [12].

Блок 5.9. Расчет $V_{зо\,ПО}(s)$ – конъюнкции показателей $V_{кр0}(s)$, $V_{г0}(s)$, $V_{ин0}(s)$,

$V_{\text{взо}}(s,t)$ [12, 14].

Блок 5.10. Ввод параметров для критерия пригодности оценки $V_{\text{кро}}(s_{\text{пр}})$, $V_{\text{го}}(s_{\text{пр}})$, $V_{\text{ино}}(s_{\text{пр}})$, $V_{\text{взо}}(s_{\text{пр}},t)$ [12].

Блок 5.11. Проверка выполнения условия по критерию пригодности, то есть $V_{\text{зо ПО}}(s)=1$. При выполнении условия реализуется переход к блоку 5.12, при его достаточности – к блоку 5.16, при невыполнении – к блоку 5.17.

Блок 5.12. Ввод параметров для критерия оптимальности оценки $V_{\text{взо}}(s_{\text{опт}},t)$ [12].

Блок 5.13. Проверка выполнения условия по критерию оптимальности. При выполнении условия реализуется переход к блоку 5.14, при его достаточности – к блоку 5.16, при невыполнении – к блоку 5.17.

Блок 5.14. Ввод дополнительных параметров для критерия адаптивизации оценки $V_{\text{взо}}(s_{\text{ад}}(t))$ [12].

Блок 5.15. Проверка выполнения условия по критерию адаптивизации. При выполнении условия реализуется переход к блоку 5.16, при невыполнении – к блоку 5.17.

Блок 5.16. При выполнении условий в блоках 5.11, 5.13, 5.15 комплексный показатель защищенности ПО равен показателю временной защищенности ПО ($V_{\text{зо ПО}}=V_{\text{взо}}(t)$) [11, 13].

Блок 5.17. При невыполнении условий в блоках 5.11, 5.13, 5.15 значение комплексного показателя защищенности ПО равно нулю ($V_{\text{зо ПО}}=0$).

Блок 5.18. Вывод найденного значения комплексного показателя защищенности ПО в АС ОВД ($V_{\text{зо ПО}}$) – результата работы алгоритма, представленного на рисунке 2.

Вывод. В статье предложен комплексный алгоритм функционирования программного комплекса, позволяющего осуществлять анализ и количественную оценку уровня защищенности ПО АС ОВД в отношении текущих уязвимостей в режиме реального времени. Наглядно представлена и описана работа основных блоков алгоритма.

Планируемая в дальнейшем практическая реализация разработанного алгоритма в виде программного комплекса анализа и оценки защищенности ПО позволит осуществлять выбор оптимальной (наиболее защищенной) версии ПО для эксплуатации на объектах информатизации ОВД с целью повышения реальной защищенности служебной информации ограниченного распространения.

Библиографический список:

1. Вопросы организации информационно-правового обеспечения деятельности органов внутренних дел Российской Федерации: приказ МВД России от 25 августа 2017 г. № 680 (в ред. приказа МВД России от 23.03.2018 № 155) [Электронный ресурс]. – Режим доступа: https://base.garant.ru/72617376/?ysclid=lmduxlmjdz739176488 (дата обращения: 10.04.2024).
2. Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента Российской Федерации от 5 декабря 2016 г. № 646 // Собрание законодательства Российской Федерации от 2016 г. – № 50. – С. 7074 – 12 с.
3. ГОСТ Р ИСО/МЭК 9126-93. Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/gost-r-iso-mek-9126-93 (дата обращения: 15.04.2024).
4. ГОСТ Р 56939-2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования. – Москва: Стандартинформ, 2016. – 24 с.
5. ГОСТ Р ИСО/МЭК 25051-2017. Информационные технологии. Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения. – Москва: Стандартинформ, 2017. – 32 с.
6. Щеглов К.А. Математические модели и методы формального проектирования систем защиты информационных систем: учебное пособие / К.А. Щеглов, А.Ю. Щеглов. – Санкт-Петербург: СПбГУ ИТМО, 2014. – 83 с.
7. Щеглов А.Ю. Элементы теории эксплуатационной информационной безопасности: учебное пособие / А.Ю. Щеглов. – Санкт-Петербург: СПбГУ ИТМО, 2014. – 59 с.
8. Ефимов А.О. Концептуальные основы оценки уровня защищенности автоматизированных систем на основе их уязвимости / А.О. Ефимов, И.И. Лившиц, Т.В. Мещерякова, Е.А. Рогозин // Безопасность информационных технологий = IT Security. – Том 30. – № 2(2023). – С. 63–79.

9. Карты источников, содержащих сведения об уязвимостях программного обеспечения / А.Л. Сердечный [и др.]. Информация и безопасность. – 2019. – Т. 22. – № 3. – С. 411-422. – EDN ZOUMGN.
10. Дровникова И.Г. Способы оценки уровня защищенности программного обеспечения автоматизированных систем органов внутренних дел и направления их совершенствования / И.Г. Дровникова, А.Д. Попова // Вестник Дагестанского государственного технического университета. Технические науки. – 2023. – Т. 50. – № 4. – С. 85–92.
11. Дровникова И.Г. Показатели защищенности программного обеспечения, используемого на объектах информатизации органов внутренних дел / И.Г. Дровникова, А.Д. Попова // Вестник Воронежского института МВД России. – 2024. – № 1. – С. 50–59.
12. Дровникова И.Г. Теоретические аспекты расчета показателей защищенности программного обеспечения автоматизированных систем органов внутренних дел / И.Г. Дровникова, А.Д. Попова // Вестник Воронежского института ФСИН России. – 2024. – № 2.
13. Дровникова И.Г. Аналитические модели расчета показателей защищенности программного обеспечения автоматизированных систем органов внутренних дел / И.Г. Дровникова, А.Д. Попова // Вестник Воронежского института МВД России. – 2024. – № 2 –22-33.
14. Попова А.Д. Методика анализа и оценки уровня защищенности программного обеспечения, используемого на объектах информатизации органов внутренних дел / А.Д. Попова, И.Г. Дровникова // Безопасность информационных технологий = IT Security, Том 31, № 2 (2024).- С.51-64.
15. Методика тестирования обновлений безопасности программных, программно-аппаратных средств: Методический документ от 28 октября 2022 г. // ФСТЭК России [Электронный ресурс]. – Режим доступа:https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g (дата обращения: 24.04.2024).
16. Common Vulnerability Scoring System version 4.0: Specification Document [Электронный ресурс]. – Режим доступа: https://www.first.org/cvss/v4.0/specification-document (дата обращения: 28.04.2024).
17. Common Vulnerability Scoring System version 4.0: User Guide [Электронный ресурс]. – Режим доступа: https://www.first.org/cvss/v4.0/user-guide (дата обращения: 28.04.2024).
18. Common Vulnerability Scoring System version 4.0: Examples [Электронный ресурс]. – Режим доступа: https://www.first.org/cvss/v4.0/examples (дата обращения: 28.04.2024).
19. CVSS 4.0: аналитический обзор новой версии популярного стандарта [Электронный ресурс]. – Режим доступа: https://www.habr.com>ru/companies/pt/articles/ 788310/ (дата обращения: 28.04.2024).
20. Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств: Методический документ от 28 октября 2022 г. // ФСТЭК России [Электронный ресурс]. – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/ spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g-2 (дата обращения: 30.04.2024).
21. Common Vulnerability Scoring System Version 4.0: Calculator [Электронный ресурс]. – Режим доступа: https://www.first.org/cvss/calculator/4.0 (дата обращения: 30.04.2024).

References:

1. Issues of organizing information and legal support for the activities of internal affairs bodies of the Russian Federation: order of the Ministry of Internal Affairs of Russia dated August 25 2017 No. 680 (as amended by order of the Ministry of Internal Affairs of Russia dated March 23, 2018 No. 155) [Electronic resource]. – Access mode: https://base.garant.ru/72617376/?ysclid=lmduxlmjdz739176488 (date of access: 04/10/2024). (In Russ)
2. On approval of the Information Security Doctrine of the Russian Federation: Decree of the President of the Russian Federation dated December 5, 2016 No. 646 // Collection of Legislation of the Russian Federation of 2016 - No. 50. Art. 7074; 50:12. (In Russ)
3. GOST R ISO/IEC 9126-93. Information technology. Evaluation of software products. Quality characteristics and guidelines for their use [Electronic resource]. – Access mode: http://docs.cntd.ru/document/gost-r-iso-mek-9126-93 (access date: 04/15/2024). (In Russ)
4. GOST R 56939-2016. Data protection. Secure software development. General requirements. – Moscow: Standardinform, 2016;24. (In Russ)
5. GOST R ISO/IEC 25051-2017. Information Technology. System and software engineering. Requirements and quality assessment of systems and software. Moscow: Standardinform, 2017; 32. (In Russ)
6. Shcheglov K.A. Mathematical models and methods of formal design of information systems protection systems: textbook. K.A. Shcheglov, A.Yu. Shcheglov. – St. Petersburg: St. Petersburg State University ITMO, 2014; 83. (In Russ)
7. Shcheglov A.Yu. Elements of the theory of operational information security: textbook / A.Yu. Shcheglov. – St. Petersburg: St. Petersburg State University ITMO, 2014; 59. (In Russ)
8. Efimov A.O. Conceptual basis for assessing the level of security of automated systems based on their vulnerability / A.O. Efimov, I.I. Livshits,T.V. Meshcheryakova, E.A. Rogozin. *Information technology security =IT Security.* 2023; 30 (2): 63–79. (In Russ)

9. Maps of sources containing information about software vulnerabilities A.L. Heart [and others]. *Information and security.* 2019; 22(3): 411-422. – EDN ZOUMGN. (In Russ)
10. Drovnikova I.G. Methods for assessing the level of security of software of automated systems of internal affairs bodies and directions for their improvement/ I.G. Drovnikova, A.D. Popova. *Herald of the Dagestan State Technical University. Technical Sciences.* 2023; 50(4): 85–92. (In Russ)
11. Drovnikova I.G. Indicators of security of software used at informatization facilities of internal affairs bodies / I.G. Drovnikova, A.D. Popova. *Herald of the Voronezh Institute of the Ministry of Internal Affairs of Russia*. 2024;1: 50–59. (In Russ)
12. Drovnikova I.G. Theoretical aspects of calculating security indicators of software of automated systems of internal affairs bodies /Drovnikova, A.D. Popova. *Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia*. 2024; 2. (In Russ)
13. Drovnikova I.G. Analytical models for calculating security indicators of software of automated systems of internal affairs bodies /Drovnikova, A.D. Popova // *Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia*. 2024; 2: 22-33. (In Russ)
14. Popova A.D. Methodology for analyzing and assessing the level of security of software used at informatization facilities of internal affairs bodies /HELL. Popova, I.G. Drovnikova. *Information technology security = IT Security,* 2024; 31(2):51-64. (In Russ)
15. Methodology for testing security updates of software, firmware and hardware: Methodological document dated October 28, 2022//FSTEC of Russia [Electronic resource]. – Access mode: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g (date of access: 04/24/2024). (In Russ)
16. Common Vulnerability Scoring System version 4.0: Specification Document [Electronic resource]. – Access mode: https://www.first.org/cvss/v4.0/specification-document (access date: 04/28/2024).
17. Common Vulnerability Scoring System version 4.0: User Guide [Electronic resource]. – Access mode: https://www.first.org/cvss/v4.0/user-guide (access date: 04/28/2024).
18. Common Vulnerability Scoring System version 4.0: Examples [Electronic resource]. – Access mode: https://www.first.org/cvss/v4.0/examples (access date: 04/28/2024).
19. CVSS 4.0: analytical review of the new version of the popular standard [Electronic resource]. – Access mode: https://www.habr.com>ru/companies/pt/articles/ 788310/ (date of access: 04/28/2024). (In Russ)
20. Methodology for assessing the level of criticality of software, software and hardware vulnerabilities: Methodological document dated October 28, 2022 // FSTEC of Russia [Electronic resource]. – Access mode:https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g-2 (date of access: 04/30/2024). (In Russ)
21. Common Vulnerability Scoring System Version 4.0: Calculator [Electronic resource]. – Access mode: https://www.first.org/cvss/calculator/4.0 (access date: 04/30/2024).

Сведения об авторе:
Попова Арина Дмитриевна, адъюнкт кафедры автоматизированных информационных систем органов внутренних дел; arnpva@mail.ru
Information about the author:
Arina D. Popova, Adjunct, Department of Automated Information Systems of Internal Affairs Bodies; arnpva@mail.ru

Конфликт интересов/Conflict of interest.
Автор заявляет об отсутствии конфликта интересов/The author declare no conflict of interest.
Поступила в редакцию/ Received 29.01.2024.
Одобрена после рецензирования/ Reviced 26.02.2024.
Принята в печать/ Accepted for publication 26.02.2024.