УДК 004.056
doi: 10.26583/bit.2024.2.03

Арина Д. Попова[1], Ирина Г. Дровникова[2]
Воронежский институт министерства внутренних дел Российской Федерации,
пр-т Патриотов, 53, Воронеж, 394065, Россия
[1]*e-mail: arpva@mail.ru, https://orcid.org/0009-0009-8596-6448*
[2]*e-mail: idrovnikova@mail.ru, https://orcid.org/0000-0001-5265-5875*

МЕТОДИКА АНАЛИЗА И ОЦЕНКИ УРОВНЯ ЗАЩИЩЕННОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИСПОЛЬЗУЕМОГО НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Аннотация. Целью статьи является разработка методики, позволяющей осуществлять анализ и количественную оценку уровня защищенности программного обеспечения, используемого в автоматизированных системах органов внутренних дел, в режиме реального времени. Для достижения поставленной цели использованы метод системного анализа существующих подходов к оцениванию уровня защищенности программного обеспечения автоматизированных систем, математический аппарат систем массового обслуживания, методы теории графов, теории вероятностей и математической статистики, теории полумарковских процессов. Предложены количественные статический и динамические показатели, позволяющие адекватно оценивать защищенность программного обеспечения в отношении текущих уязвимостей в динамике его функционирования и с учетом имеющихся недостатков эксплуатации на объектах информатизации органов внутренних дел. Разработаны математические модели и алгоритмы аналитического расчета предложенных показателей в режиме реального времени. Перспективы практической реализации рассмотренной методики связаны с разработкой программного комплекса анализа и оценки защищенности программного обеспечения с целью выбора его оптимальной версии в интересах повышения уровня защищенности служебной информации ограниченного распространения, циркулирующей на конкретных объектах информатизации органов внутренних дел.
Ключевые слова: уязвимости в программном обеспечении, защищенность программного обеспечения, количественные показатели защищенности, аналитические модели оценки показателей в режиме реального времени, алгоритмы аналитического расчета показателей.
Для цитирования: ПОПОВА, Арина Д.; ДРОВНИКОВА, Ирина Г. МЕТОДИКА АНАЛИЗА И ОЦЕНКИ УРОВНЯ ЗАЩИЩЕННОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ИСПОЛЬЗУЕМОГО НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ. Безопасность информационных технологий, [S.l.], т. 31, № 2, с. 51–64, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1637. DOI: http://dx.doi.org/10.26583/bit.2024.2.03.

Arina D. Popova[1], Irina G. Drovnikova[2]
Voronezh Institute of the Ministry of the Interior,
Patriots Ave., 53, Voronezh, 394065, Russia
[1]*e-mail: arpva@mail.ru, https://orcid.org/0009-0009-8596-6448*
[2]*e-mail: idrovnikova@mail.ru, https://orcid.org/0000-0001-5265-5875*

The methodology of analysis and assessment of the level of security of the software used at the objects of informatization of internal affairs bodies

Abstract. The purpose of the article is to develop a technique that allows analyzing and quantifying the software protection level used in automated systems of internal affairs agencies in real time. To achieve this goal, the method of system analysis of existing approaches to assessing the protection level of automated systems software, the mathematical apparatus of queuing systems, methods of graph theory, probability theory and mathematical statistics, and the theory of semi-Markov processes were used.

Quantitative static and dynamic indicators are proposed that make it possible to adequately assess the software protection in relation to current vulnerabilities in the dynamics of its functioning and taking into account the existing disadvantages of operation at the facilities of informatization of internal affairs bodies. Mathematical models and algorithms for analytical calculation of the proposed indicators in real time have been developed. The prospects for the practical implementation of the considered technique are related to the development of a software package for analyzing and evaluating the software protection in order to select its optimal version for increasing the protection level of official information of limited distribution circulating at specific informatization facilities of internal affairs bodies.
Keywords: vulnerabilities in software, software security, quantitative indicators of security, analytical models for evaluating indicators in real time, algorithms for analytical calculation of indicators.
For citation: POPOVA, Arina D.; DROVNIKOVA, Irina G. The methodology of analysis and assessment of the level of security of the software used at the objects of informatization of internal affairs bodies. IT Security (Russia), [S.l.], v. 31, no. 2, p. 51–64, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1637. DOI: http://dx.doi.org/10.26583/bit.2024.2.03.

Введение

Реализация процедуры оценивания уровня защищенности используемого программного обеспечения (ПО) имеет определяющее значение при рассмотрении вопроса безопасного функционирования современных автоматизированных систем (АС) органов внутренних дел (ОВД). Это, в свою очередь, предполагает разработку соответствующих показателей защищенности ПО, эксплуатируемого на объектах информатизации ОВД, а также адекватной методики их анализа и количественной оценки.

Результаты анализа существующих в настоящее время подходов к оцениванию уровня защищенности ПО в АС показали, что показатели и методики, предлагаемые в большинстве научных работ, позволяют лишь качественно оценивать защищенность, поскольку они основаны на использовании либо статических аналитических моделей несанкционированного доступа [1, 2], либо статических моделей определения показателей критичности уязвимостей в компонентах ПО [3], что не обеспечивает достаточной точности оценивания. Немногочисленные научные труды, предлагающие количественно оценивать защищенность ПО, используя динамические аналитические модели [4, 5], не в достаточной степени обеспечивают моделирование и определение стохастических параметров и количественных показателей, которые характеризуют изменяющиеся в процессе функционирования (эксплуатационные) свойства безопасности ПО – его эксплуатационную информационную безопасность (ИБ) – применительно к современным объектам информатизации ОВД [6].

Предлагаемая в данной статье методика анализа и оценки уровня защищенности ПО, используемого на объектах информатизации ОВД, включает в себя следующие этапы:

1) разработку показателей защищенности ПО, учитывающих недостатки его эксплуатации в АС ОВД;

2) разработку математических моделей для проведения анализа и количественной оценки изменения показателей защищенности ПО в отношении текущих уязвимостей (типов уязвимостей) в динамике его функционирования в АС ОВД;

3) разработку алгоритмов аналитического расчета показателей защищенности ПО в АС ОВД на основе предложенных моделей.

1. Показатели защищенности программного обеспечения автоматизированных систем органов внутренних дел и аналитические модели их расчета

Система количественных показателей, позволяющих адекватно оценивать реальную защищенность (эксплуатационную ИБ) ПО, характеризующих как статические, так и

динамические свойства защищенности с учетом недостатков его эксплуатации на объектах информатизации ОВД, предложена и обоснована в [7]. При этом в качестве простейшего элемента ИБ ПО АС ОВД рассматривалась уязвимость в используемом ПО (текущие уязвимости определенного типа).

К таким показателям относятся:

1. *Уровень критичности уязвимости в ПО* ($V_{\text{кр у}}$) – статический показатель защищенности ПО – определяется уровнем опасности уязвимости и ее влиянием на процесс функционирования АС ОВД, использующей данное ПО. Расчет $V_{\text{кр у}}$ осуществляется с использованием аналитической статической модели в соответствии с утвержденной Федеральной службой по техническому и экспортному контролю (ФСТЭК) России методикой[1] по формуле:

$$V_{\text{кр у}} = I_{cvss\,\text{у}} \times I_{infr\,\text{у}}, \quad (1)$$

где: $I_{cvss\,\text{у}}$ – показатель уровня опасности уязвимости в ПО – находится путем расчета базовых метрик, метрик угроз, метрик окружения и дополнительных метрик по методике Common Vulnerability Scoring System (CVSS) v.4.0[2,3,4] с использованием online-калькулятора[5] и определяется совокупностью показателей указанных метрик применительно к конкретной АС ОВД;

$I_{infr\,\text{у}}$ – показатель, характеризующий влияние уязвимости в ПО на процесс функционирования АС ОВД, использующей данное ПО – рассчитывается для конкретной системы по формуле:

$$I_{infr\,\text{у}} = k * K + l * L + p * P, \quad (2)$$

где: K – показатель, описывающий тип подверженного уязвимости компонента ПО;

L – показатель, описывающий число уязвимых компонент ПО;

P – показатель, описывающий влияние уязвимого компонента ПО на защищенность периметра АС ОВД;

k, l, p – весовые коэффициенты рассматриваемых показателей.

Определение оценок показателей K, L, P и их весовых коэффициентов, а также результирующего значения $V_{\text{кр у}}$ применительно к конкретной АС ОВД проводится в соответствии с приведенными в Методике[1] таблицами.

Поскольку согласно опубликованной статистике[6] на защищенность ПО существенное влияние оказывают уязвимости высокого и критического уровней критичности, то только их следует рассматривать при расчете остальных показателей защищенности ПО в АС ОВД.

[1]Методический документ ФСТЭК России от 28 октября 2022 г. «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств».

[2]Common Vulnerability Scoring System version 4.0: Specification Document. URL: https://www.first.org/cvss/v4.0/specification-document (дата обращения: 03.04.2024).

[3]Common Vulnerability Scoring System version 4.0: User Guide. URL: https://www.first.org/cvss/v4.0/user-guide (дата обращения: 03.04.2024).

[4]Common Vulnerability Scoring System version 4.0: Examples. URL: https://www.first.org/cvss/v4.0/examples (дата обращения: 03.04.2024).

[5]Common Vulnerability Scoring System Version 4.0: Calculator. URL: https://www.first.org/cvss/calculator/4.0 (дата обращения: 03.04.2024).

[6]Kaspersky Security Bulletin 2023. Статистика | Securelist. URL: http://www.securelist.ru (дата обращения: 04.04.2024).

2. *Коэффициент готовности ПО к безопасной эксплуатации* ($V_{\text{г}}$) – динамический показатель защищенности ПО – представляет собой вероятность $P_{0\text{у}}$ того, что ПО готово к безопасной эксплуатации в отношении уязвимости. Расчет $V_{\text{г}}$ осуществляется на основе аналитической динамической дискретной модели с использованием аппарата систем массового обслуживания (СМО) [8] по формуле:

$$V_{\text{г}} = P_{0\text{у}} = \left(\sum_{n=0}^{M} \frac{(\lambda/\mu)^n}{n!} + \frac{(\lambda/\mu)^{C+1}}{C!\left(C-\frac{\lambda}{\mu}\right)}\right)^{-1}, \quad (3)$$

где: M – число каналов обслуживания (система защиты в АС ОВД представляется как многоканальная СМО);

C – количество обслуживающих приборов, осуществляющих анализ уязвимости в используемом ПО для выявления ее сигнатуры;

λ, μ – интенсивности выявления и устранения уязвимости в ПО (поступления и обслуживания заявки) соответственно ($\lambda = 1/\tau_{\text{ву}}$, $\mu = 1/\tau_{\text{уу}}$, где $\tau_{\text{ву}}$, $\tau_{\text{уу}}$ – времена выявления и устранения уязвимости в ПО).

При разработке модели принято допущение, что $\lambda \leq \mu C$ (то есть рассматриваемая СМО является стационарной), поскольку в противном случае время обслуживания заявки и очередь заявок на обслуживание могут возрасти до бесконечности.

Учитывая, что при реализации угрозы нарушителем (осуществлении атаки), как правило, в определенной последовательности используется некоторая совокупность текущих уязвимостей (типов уязвимостей) в ПО, имеющих высокий или критический уровни критичности, аналитическая модель расчета коэффициента готовности для совокупности уязвимостей $\text{V}_{\text{г}0}$ примет следующий вид:

$$V_{\text{г}0} = P_0 = 1 - \prod_{i=1}^{N}(1 - P_{0\text{у}i}), \quad (4)$$

где: P_0 – вероятность того, что ПО готово к безопасной эксплуатации в отношении совокупности уязвимостей;

N – количество используемых нарушителем текущих уязвимостей в ПО.

3. *Интервальный показатель нарушения защищенности ПО* ($V_{\text{ин у}}$) – динамический показатель защищенности ПО – определяется средним временем наработки на нарушение эксплуатационной ИБ ПО в отношении уязвимости (то есть средним интервалом времени $T_{0\text{у}}$ между выявлениями уязвимости в ПО, средняя интенсивность устранения которой составляет μ). При выполнении условия $T_{0\text{у}} \gg 1/\mu$ расчет $V_{\text{ин у}}$ осуществляется с использованием аналитической динамической дискретной модели по формуле:

$$V_{\text{ин у}} = T_{0\text{у}} = \frac{P_{0\text{у}}}{\mu(1-P_{0\text{у}})}. \quad (5)$$

При использовании нарушителем совокупности текущих уязвимостей в ПО интервальный показатель $V_{\text{ин}0}$ рассчитывается по формуле:

$$V_{\text{ин}0} = T_0 = \frac{P_0}{\mu_0(1-P_0)}, \quad (6)$$

где: T_0 – средний интервал времени между выявлениями уязвимостей в ПО, средняя интенсивность устранения которых (интенсивность восстановления эксплуатационной ИБ ПО) составляет $\mu_0 = 1/\sum_{i=1}^{N} \tau_{\text{уу}i}$.

4. *Показатель временной защищенности ПО* ($V_{\text{вз у}}(t)$) – динамический показатель защищенности ПО – позволяет оценивать изменение уровня защищенности ПО в

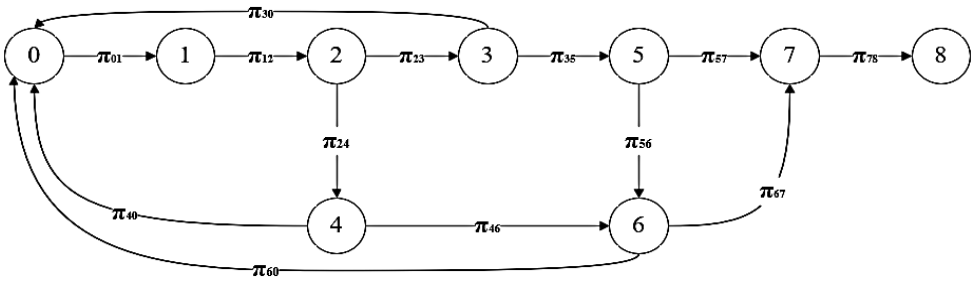
отношении уязвимости в процессе его эксплуатации в АС ОВД (напрямую зависит от времени). Расчет $V_{\text{вз у}}(t)$) осуществляется с использованием аналитической динамической непрерывной модели по формуле:

$$V_{\text{вз у}}(t) = 1 - P_{\text{эу}}(t)|_{\,t \le 1/\mu}, \quad (7)$$

где $P_{\text{эу}}(t)$ – вероятность эксплуатации уязвимости в ПО в течение времени, не превышающего времени восстановления его эксплуатационной ИБ $1/\mu$.

Для моделирования процесса эксплуатации уязвимости в ПО в течение интервала времени $t \le 1/\mu$ с периодичностью $T_{0\text{y}}$ и расчета вероятностно-временных характеристик (ВВХ), описывающих динамику ее эксплуатации в ПО АС ОВД в режиме реального времени, использован математический аппарат полумарковских процессов (ПМП) [9].

Разработка аналитической модели расчета показателя $V_{\text{вз у}}(t)$ основана на применении теории ПМП к графовой модели динамики эксплуатации текущей уязвимости в ПО АС ОВД, представленной на рис. 1, что позволяет осуществлять анализ случайной последовательности смены состояний процесса эксплуатации уязвимости во времени и исследовать данный процесс с определением его ВВХ [10].



0 – штатный режим функционирования ПО;
1 – обнаружение уязвимости в ПО нарушителем;
2 – поиск нарушителем обнаруженной уязвимости среди неустранённых уязвимостей в National Vulnerabilities Database (NVD) и в базе данных уязвимостей банка данных угроз безопасности информации ФСТЭК России;
3 – получение информации об уровне критичности найденной уязвимости;
4 – самостоятельный расчет уровня критичности уязвимости нарушителем;
5 – для уязвимости высокого или критического уровня критичности поиск эксплойта нарушителем;
6 – для уязвимости высокого или критического уровня критичности самостоятельная разработка эксплойта нарушителем;
7 – применение эксплойта;
8 – эксплуатация уязвимости нарушителем.

Рис. 1. Графовая модель процесса эксплуатации уязвимости в ПО АС ОВД

Изображенная модель является взвешенным ориентированным графом, дугам которого присвоены веса π_{ij}, являющиеся мгновенными вероятностями достижения каждого из состояний на этапах процесса эксплуатации уязвимости в ПО АС ОВД.

Для определения вероятности эксплуатации уязвимости и расчета ВВХ, характеризующих динамику ее эксплуатации в ПО АС ОВД, разработана система интегро-дифференциальных уравнений:

$$p_i(t) = \pi_{in} F_i(t) + \sum_{j=1}^{n-1} \pi_{ij} \int_0^t \varphi_i(\tau) p_j(t-\tau) d\tau,\ i = 0..n-1, \quad (8)$$

где: $p_i(t)$ – вероятность достижения ПМП, пребывающем в i-ом состоянии, своего конечного состояния n в течение времени, не превышающего t; $\varphi_i(\tau) = F_i'(\tau)$ – плотность

распределения вероятностей (ПРВ) для случайной величины τ (времени пребывания ПМП в i-ом состоянии); $p_j(t-\tau)$ – вероятность достижения ПМП, пребывающем в i-ом состоянии, состояния j, а затем – конечного состояния n, учитывающая временные задержки переходов ПМП.

Решение представленной системы интегро-дифференциальных уравнений осуществляется путем сведения ее к системе линейных алгебраических уравнений, применяя к обеим частям (8) преобразование Лапласа. Аналитическое решение полученной в результате системы линейных алгебраических уравнений и последующее аналитическое выполнение обратного преобразования Лапласа от дробно-линейных функций с использованием встроенных функций пакета программ MATLAB позволяет определить ВВХ процесса эксплуатации уязвимости в ПО в течение времени восстановления его эксплуатационной ИБ ($\tau_{\text{уу}=} {}^{1}/_{\mu}$), а следовательно, и рассчитать $V_{\text{вз у}}(t)$) по формуле:

$$V_{\text{вз у}}(t) = 1 - L^{-1}[p_0(s)](t)|_{t={}^{1}/_{\mu}}, \quad (9)$$

где $p_0(s)$ – преобразование Лапласа для функции $p_0(t) = P_{\text{эу}}(t)$.

При использовании нарушителем совокупности текущих уязвимостей в ПО аналитическая модель расчета показателя временной защищенности ПО $V_{\text{взо}}(t)$ примет вид:

$$V_{\text{взо}}(t) = 1 - P_{\text{эо}}(t)|_{t={}^{1}/_{\mu_0}} = \prod_{i=1}^{N}(1 - P_{\text{эу}i})|_{t={}^{1}/_{\mu_i}}, \quad (10)$$

где $P_{\text{эо}}(t)$ – вероятность эксплуатации совокупности уязвимостей в ПО в течение времени, не превышающего времени восстановления его эксплуатационной ИБ ${}^{1}/_{\mu_0}$.

Комплексный показатель защищенности ПО в АС ОВД ($V_{\text{зо ПО}}$) рассчитывается путем сведения всех рассмотренных выше показателей защищенности ПО в единый показатель с использованием процедуры агрегирования:

$$V_{\text{зо ПО}}(s) = V_{\text{кро}}(s) \cap V_{\text{го}}(s) \cap V_{\text{ино}}(s) \cap V_{\text{взо}}(s,t), \quad (11)$$

где s – стратегия обеспечения защищенности ПО в процессе его функционирования в АС ОВД из множества допустимых значений S.

Расчет показателей $V_{\text{кро}}(s)$, $V_{\text{го}}(s)$, $V_{\text{ино}}(s)$, $V_{\text{взо}}(s,t)$ предлагается производить по качественной шкале в виде булево-независимой ($V_{\text{кро}}(s)$) и булево-зависимых ($V_{\text{го}}(s)$, $V_{\text{ино}}(s)$, $V_{\text{взо}}(s,t)$) переменных [11], где:

$$V_{\text{кро}}(s) = \begin{cases} 1, \text{ если } 4{,}5 \le V_{\text{кро}}(s) \le 10{,}0; \\ 0, \text{ если } V_{\text{кро}}(s) < 4{,}5. \end{cases} \quad (12)$$

Поскольку при расчете динамических показателей защищенности ПО в АС ОВД рассматривается совокупность уязвимостей (типов уязвимостей) высокого и критического уровней критичности, то $V_{\text{кро}}(s) = 1$;

$$V_{\text{го}}(s) = \begin{cases} 1, \text{ если } V_{\text{го}}(s) = P_0|_{\tau_{\text{во}} \ge \tau_{\text{уо}}}; \\ 0, \text{ если } V_{\text{го}}(s) = P_0|_{\tau_{\text{во}} < \tau_{\text{уо}}}; \end{cases} \quad (13)$$

$$V_{\text{ино}}(s) = \begin{cases} 1, \text{ если } V_{\text{ино}}(s) = T_0 \ge T_{\text{э}}; \\ 0, \text{ если } V_{\text{ино}}(s) = T_0 < T_{\text{э}}. \end{cases} \quad (14)$$

$$V_{\text{взо}}(s,t) = \begin{cases} 1, \text{ если } P_{\text{эо}}(s,t)|_{t \le \tau_{\text{уо}}} \le P_{\text{пор}}; \\ 0, \text{ если } P_{\text{эо}}(s,t)|_{t \le \tau_{\text{уо}}} > P_{\text{пор}}, \end{cases} \quad (15)$$

где: $\tau_{в0}$ и $\tau_{у0}$ – времена выявления и устранения совокупности текущих уязвимостей соответственно;

$T_э$ – длительность наработки ПО на отказ при его регулярной эксплуатации в АС ОВД [6];

$P_{пор}$ – заданный порог вероятности, определяемый экспериментально.

В оценке защищенности ПО в АС ОВД реализуется совокупность рассмотренных показателей, не противоречащих концепциям рационального поведения системы (концепциям пригодности, оптимальности, адаптивизации) [12]:

– в соответствии с *концепцией пригодности* любая стратегия $s \in S$ является рациональной, если при ее реализации обоснованные целевые требования принимают значения не ниже (не выше) некоторого приемлемого уровня:

$$4{,}5 \le V_{кр0}(s_{пр}) \le 10,\ s_{пр} \in S; \tag{16}$$

$$V_{г0}(s_{пр}) = P_0(s_{пр})|_{\tau_{в0} \ge \tau_{у0}},\ s_{пр} \in S; \tag{17}$$

$$V_{ин0}(s_{пр}) = T_0(s_{пр}) \ge T_э,\ s_{пр} \in S; \tag{18}$$

$$P_{э0}(s_{пр}, t)|_{t \le \tau_{у0}} \le P_{пор} \text{ или } V_{вз0}(s_{пр}, t)|_{t \le \tau_{у0}} \ge V_{пор},\ s_{пр} \in S, \tag{19}$$

где $V_{пор} = 1 - P_{пор}$.

Поскольку при агрегировании в комплексный показатель рассмотренных показателей защищенности ПО АС ОВД первостепенную роль играет показатель $V_{вз\,0}(t)$ – напрямую зависимый от времени и отражающий изменение защищенности ПО в процессе его эксплуатации в АС ОВД [7], то далее рассмотрим концепции оптимальности и адаптивизации применительно к данному показателю:

– в соответствии с *концепцией оптимальности* рациональной является та стратегия $s_{опт}$ из заданного ограниченного множества пригодных $S_{пр}$, реализация которой обеспечивает максимальный эффект в операции, проводимой системой:

$$V_{вз0}(s_{опт}, t)|_{t \le \tau_{у0}} = \max V_{вз0}(s_{пр}, t)|_{t \le \tau_{у0}},\ s_{опт} \in S_{пр}; \tag{20}$$

– в соответствии с *концепцией адаптивизации* предполагается возможность оперативного реагирования на поступающую текущую информацию в ходе реализации процесса. Следовательно, концепция направлена на создание наиболее гибкой стратегии $s_{ад}(t)$ из множества оптимальных $S_{опт}$, учитывающей динамические свойства защищенности ПО в АС ОВД:

$$V_{вз0}\left(s_{ад}(t)\right)|_{t \le \tau_{у0}} = V_{вз0}(S_{опт}(t), 1)|_{t \le \tau_{у0}},\ s_{ад} \in S_{опт}. \tag{21}$$

Очевидно, что каждый последующий показатель временной защищенности ПО представляет собой подмножество множества стратегий предыдущего, что обеспечивает возможность выбора наилучшей стратегии с учетом требуемой степени достижения цели обеспечения защищенности ПО в процессе его эксплуатации на объекте информатизации ОВД.

2. Алгоритмы аналитического расчета показателей защищенности программного обеспечения в динамике его функционирования в автоматизированных системах органов внутренних дел

Оценивание защищенности ПО, эксплуатируемого на объектах информатизации ОВД, предполагает разработку соответствующих алгоритмов аналитического расчета показателей защищенности ПО на основе рассмотренных моделей.

Поскольку оценивание защищенности ПО в процессе его эксплуатации в АС ОВД является сложным математическим процессом, требующим для своего осуществления минимизации временных и вычислительных ресурсов, то для реализации в виде алгоритма разработанной аналитической модели расчета показателя временной защищенности ПО в процессе его эксплуатации в АС ОВД выбрана универсальная система автоматизации математических и научно-технических расчетов MATLAB, обладающая неоспоримыми преимуществами перед множеством других ориентируемых на численные расчеты специализированных программных пакетов [13, 14].

Алгоритм аналитического расчета комплексного показателя защищенности ПО в АС ОВД представлен на рис. 2. Работу данного алгоритма можно описать следующим образом.

Блок 1. Формирование исходных данных для расчета уровня критичности уязвимостей в ПО АС ОВД ($V_{\text{кр0}}$):

– 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)[7];

– 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 Методике[8].

Блок 2. Расчет показателя $V_{\text{кр0}}$ (блок Start 1) (рис. 3):

Блок 2.1. Ввод сформированных исходных данных для расчета $V_{\text{кр0}}$.

Блок 2.2. Расчет I_{cvss0} с использованием online-калькулятора[9].

Блок 2.3. Расчет I_{infr0} по формуле (2).

Блок 2.4. Расчет $V_{\text{кр0}}$ по формуле (1).

Блок 2.5. Вывод результатов расчета $V_{\text{кр0}}$.

Блок 3. Формирование исходных данных для расчета коэффициента готовности ПО АС ОВД к безопасной эксплуатации ($V_{\text{г0}}$): числа каналов обслуживания (M), количества обслуживающих приборов (C), количества используемых нарушителем текущих уязвимостей в ПО (N), времен выявления и устранения текущих уязвимостей в ПО ($\tau_{\text{вy}i}$, $\tau_{\text{yy}i}$, $i = 1..N$).

[7]Common Vulnerability Scoring System version 4.0: Specification Document. URL: https://www.first.org/cvss/v4.0/specification-document (дата обращения: 03.04.2024).

[8]Методический документ ФСТЭК России от 28 октября 2022 г. «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств».

[9]Common Vulnerability Scoring System Version 4.0: Calculator. URL: https://www.first.org/cvss/calculator/4.0 (дата обращения: 03.04.2024).

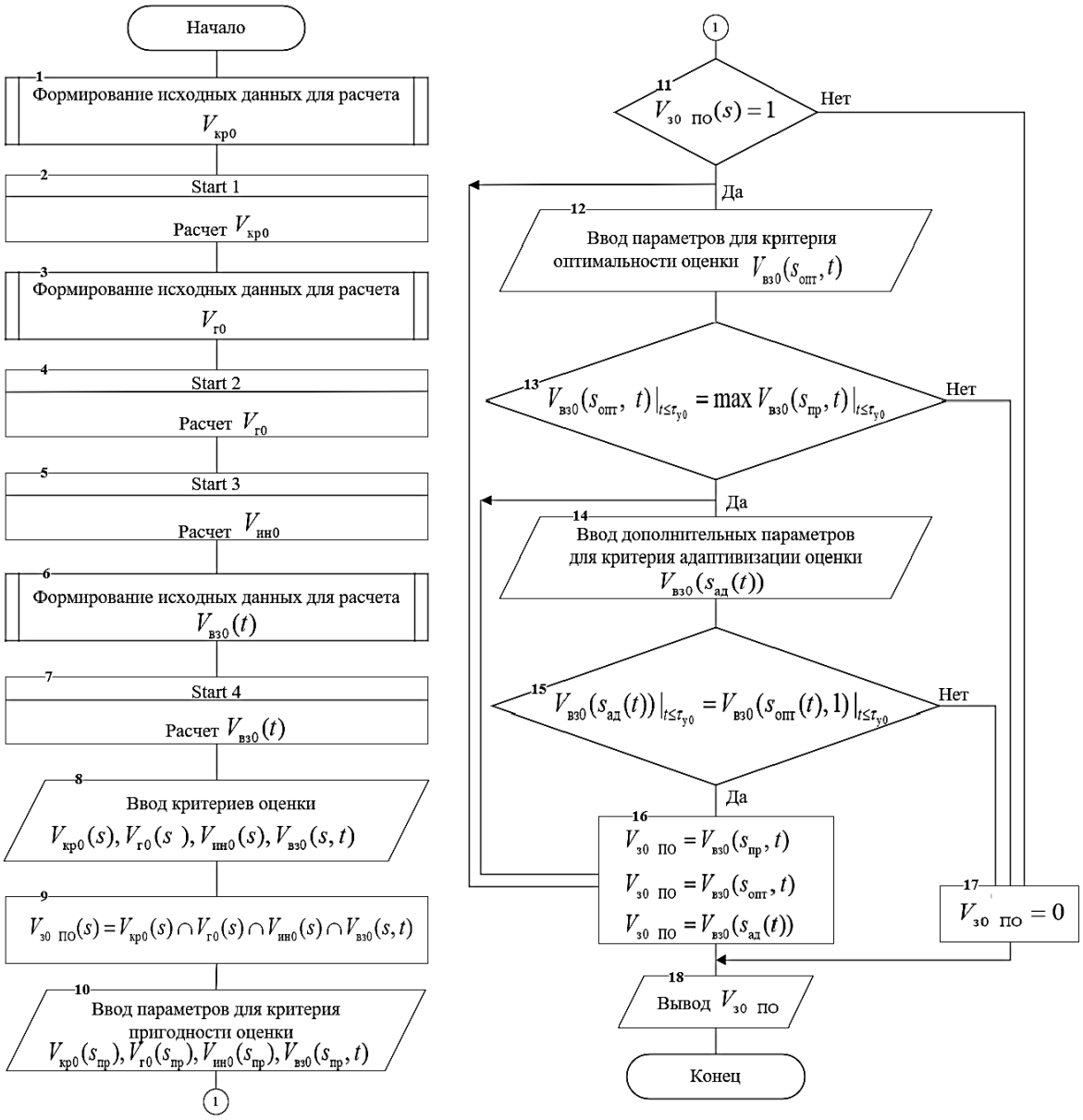


Рис. 2. Алгоритм аналитического расчета комплексного показателя защищенности ПО в АС ОВД

Блок 4. Расчет показателя $V_{г0}$ (блок Start 2) (рис. 4):

Блок 4.1. Ввод сформированных исходных данных для расчета $V_{г0}$.

Блок 4.2. Организация цикла с параметром i для расчета $V_{г0}$.

Блок 4.3. Расчет интенсивностей выявления и устранения текущих уязвимостей в ПО по формулам $\lambda_i = {}^{1}/_{\tau_{вуi}}$, $\mu_i = {}^{1}/_{\tau_{ууi}}$.

Блок 4.4. Организация цикла с параметром n для расчета P_{0yi}.

Блок 4.5. Расчет P_{0yi} по формуле (3).

Блок 4.6. Расчет $V_{г0}$ по формуле (4).

Блок 4.7. Вывод результатов расчета $V_{г0}$.

Блок 5. Расчет интервального показателя нарушения защищенности ПО в АС ОВД ($V_{ин0}$) (блок Start 3) (рис. 5):

Блок 5.1. Организация цикла с параметром i для расчета μ_0.

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

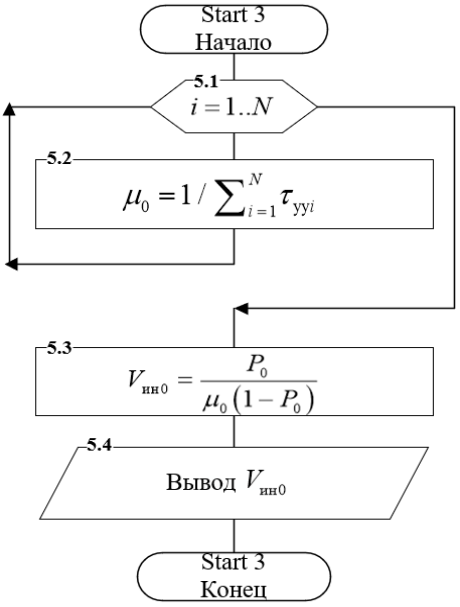


Рис. 5. Алгоритм аналитического расчета интервального показателя нарушения защищенности ПО в АС ОВД

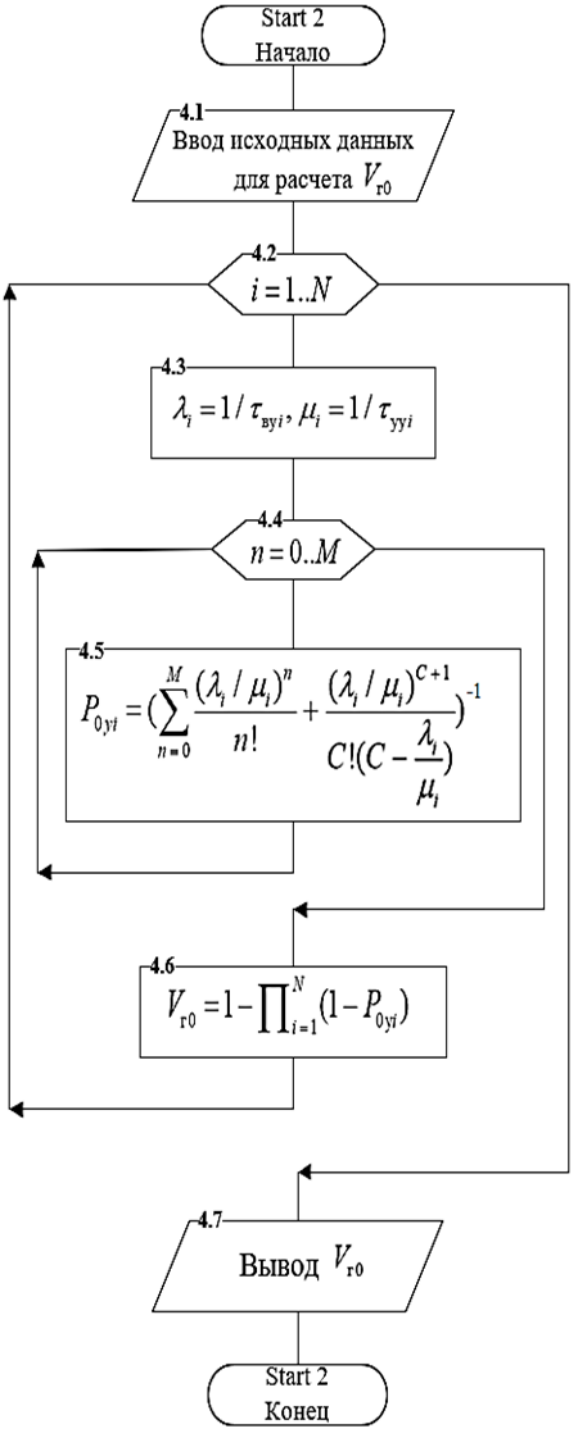


Рис. 4. Алгоритм аналитического расчета коэффициента готовности ПО АС ОВД к безопасной эксплуатации

Блок 5.2. Расчет μ_0 по формуле $\mu_0 = {1}/{\sum_{i=1}^{N} \tau_{\text{уу}i}}$.

Блок 5.3. Расчет $V_{\text{ин0}}$ по формуле (6).

Блок 5.4. Вывод результатов расчета $V_{\text{ин0}}$.

Блок 6. (рис. 1). Формирование исходных данных для расчета показателя временной защищенности ПО в АС ОВД ($V_{\text{взо}}(t)$):

– 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).

Блок 7. (рис. 1). Расчет показателя $V_{\text{взо}}(t)$ в программной среде MATLAB R2020b (блок Start 4) (рис. 6):

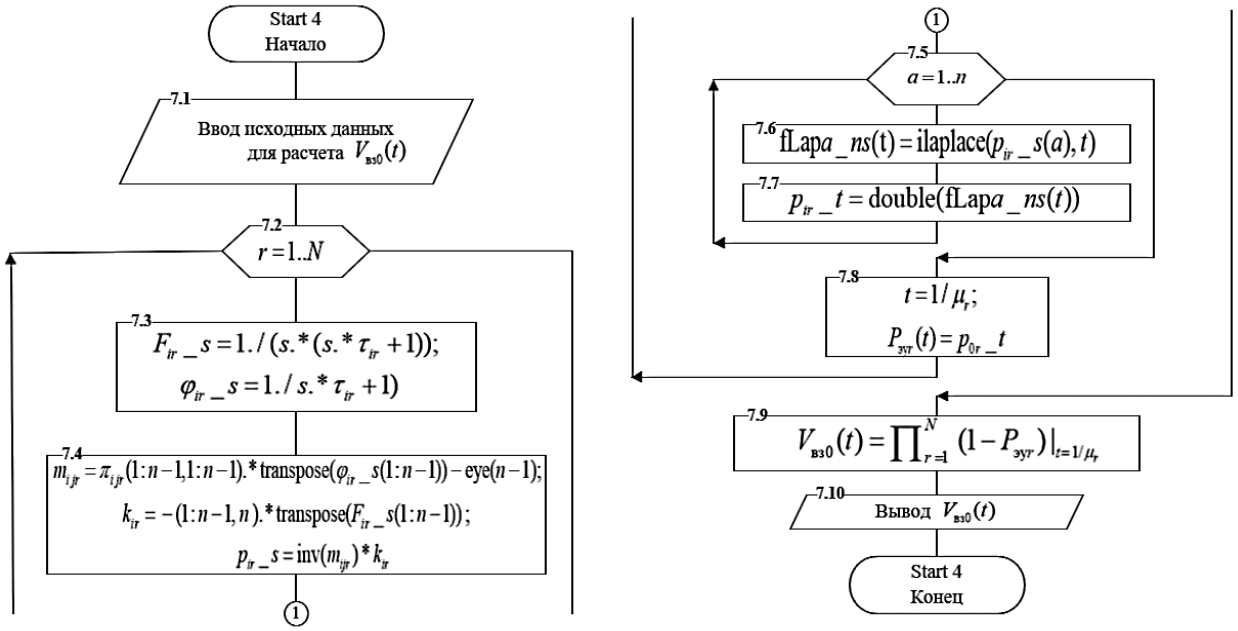


Рис. 6. Алгоритм аналитического расчета показателя временной защищенности ПО в АС ОВД

Блок 7.1. Ввод сформированных исходных данных для расчета $V_{\text{взо}}(t)$.

Блок 7.2. Организация цикла с параметром r для расчета $V_{\text{взо}}(t)$.

Блок 7.3. Вычисление F_{ir}_s и φ_{ir}_s посредством аналитического выполнения прямого преобразования Лапласа функций $F_{ir}(t)$ и $\varphi_{ir}(\tau)$ для экспоненциального распределения вероятности и плотности вероятности. С этой целью применяются известные табличные функции образов Лапласа от экспоненциальных функций: $F_{ir} = 1./(s.*(s.*\tau_{ir}+1))$; $\varphi_{ir} = 1./(s.*\tau_{ir}+1)$.

Блок 7.4. Создание и вычисление матриц m_{ijr} и k_{ir} путем использования матрицы

вероятностей переходов между состояниями процесса π_{ijr} и проведения транспонирования φ_{ir}_s и F_{ir}_s. Применение метода обратной матрицы MATLAB для нахождения матрицы p_{ir}_s с помощью оператора inv вычисления обратной матрицы от матрицы m_{ijr}.

Блок 7.5. Организация цикла с параметром a для вычисления значений функций вероятностей переходов ПМП из различных состояний в конечное поглощающее состояние fLap$a_ns(t)$ и p_{ir}_t, определяющих ВВХ процесса эксплуатации уязвимости в ПО.

Блок 7.6. Расчет fLap$a_ns(t)$ посредством аналитического выполнения обратного преобразования Лапласа $p_{ir}\_s(a)$ с использованием встроенной функции MATLAB – ilaplace.

Блок 7.7. Вычисление численного значения p_{ir}_t с использованием стандартной функции MATLAB – double (преобразует значение к двойной точности).

Блок 7.8. Вычисление значения p_{0r}_t в точке $t = {}^{1}/_{\mu_r}$ согласно формуле (9).

Блок 7.9. Вычисление значения $V_{\text{взо}}(t)$ в соответствии с формулой (10).

Блок 7.10. Вывод результатов расчета $V_{\text{взо}}(t)$.

Блок 8. (рис. 1). Ввод критериев оценки $V_{\text{кро}}(s)$, $V_{\text{го}}(s)$, $V_{\text{ино}}(s)$, $V_{\text{взо}}(s,t)$ в соответствии с формулами (12) – (15).

Блок 9. (рис. 1). Расчет $V_{\text{зо ПО}}(s)$ – конъюнкции показателей $V_{\text{кро}}(s)$, $V_{\text{го}}(s)$, $V_{\text{ино}}(s)$, $V_{\text{взо}}(s,t)$ в соответствии с формулой (11).

Блок 10. Ввод параметров для критерия пригодности оценки $V_{\text{кро}}(s_{\text{пр}})$, $V_{\text{го}}(s_{\text{пр}})$, $V_{\text{ино}}(s_{\text{пр}})$, $V_{\text{взо}}(s_{\text{пр}},t)$ в соответствии с формулами (16) – (19).

Блок 11. Проверка выполнения условий по критерию пригодности, то есть $V_{\text{зо ПО}}(s) = 1$. При выполнении условия реализуется переход к блоку 12, при его достаточности – к блоку 16, при невыполнении – к блоку 17.

Блок 12. Ввод параметров для критерия оптимальности оценки $V_{\text{взо}}(s_{\text{опт}},t)$ согласно формуле (20).

Блок 13. Проверка выполнения условия по критерию оптимальности. При выполнении условия реализуется переход к блоку 14, при его достаточности – к блоку 16, при невыполнении – к блоку 17.

Блок 14. Ввод дополнительных параметров для критерия адаптивизации оценки $V_{\text{взо}}(s_{\text{ад}}(t))$ согласно формуле (21).

Блок 15. Проверка выполнения условия по критерию адаптивизации. При выполнении условия реализуется переход к блоку 16, при невыполнении – к блоку 17.

Блок 16. При выполнении условий (16) – (21) комплексный показатель защищенности ПО ($V_{\text{зо ПО}}$) оценивается по формуле (10).

Блок 17. При невыполнении условий (16) – (21) значение комплексного показателя защищенности ПО равно нулю ($V_{\text{зо ПО}} = 0$).

Блок 18. Вывод найденного значения комплексного показателя защищенности ПО в АС ОВД ($V_{\text{зо ПО}}$) – результата работы алгоритма, представленного на рис. 2.

Заключение

В данной статье рассмотрена методика анализа и оценки уровня защищенности ПО, используемого на объектах информатизации ОВД. Предложен комплекс показателей защищенности, учитывающих имеющиеся недостатки эксплуатации ПО в динамике его функционирования в АС ОВД, математические модели и алгоритмы их количественной оценки в отношении текущих уязвимостей в ПО в режиме реального времени.

Планируемая в дальнейшем практическая реализация разработанных моделей и алгоритмов 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.

СПИСОК ЛИТЕРАТУРЫ:

1. Радько Н.М. Проникновения в операционную среду компьютера: модели злоумышленного удаленного доступа. Н.М. Радько, Ю.К. Язов, Н.Н. Корнеева. Воронеж: Воронежский государственный технический университет, 2013. – 265 с.
2. Язов Ю.К. Методология оценки эффективности защиты информации в информационных системах от несанкционированного доступа: монография. Ю.К. Язов, С.В. Соловьев. – Санкт-Петербург: Наукоемкие технологии, 2023. – 258 с.
3. Ефимов, Алексей О. и др. Концептуальные основы оценки уровня защищенности автоматизированных систем на основе их уязвимости. Безопасность информационных технологий, [S.l.], т. 30, № 2, с. 63–79, 2023. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2023.2.04.
4. Язов Ю.К. Сети Петри-Маркова и их применение для моделирования процессов реализации угроз безопасности информации в информационных системах: монография. Ю.К. Язов, А.В. Анищенко. Воронеж: Кварта, 2020. – 173 с.
5. Щеглов К.А. Математические модели и методы формального проектирования систем защиты информационных систем. К.А. Щеглов, А.Ю. Щеглов. Санкт-Петербург: СПбГУ ИТМО, 2014. – 83 с.
6. Дровникова И.Г., Попова А.Д. Способы оценки уровня защищенности программного обеспечения автоматизированных систем органов внутренних дел и направления их совершенствования. Вестник Дагестанского государственного технического университета. Технические науки. 2023;50(4):85-92. DOI: 10.21822/2073-6185-2023-50-4-85-92. – EDN: LDTFDM.
7. 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. URL: https://ВИ.МВД.РФ/Nauka/nauchnij-zhurnal-vestni/Vestnik_1_2024.pdf (дата обращения: 18.04.2024).
8. 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.
9. Королюк В.С. Полумарковские процессы и их приложения. В.С. Королюк, А.Ф. Турбин. Киев: Наукова думка, 1976. – 184 с.
10. Краснов А.Ю. Статистические методы в инженерных исследованиях. А.Ю. Краснов. Санкт-Петербург: Университет ИТМО, 2022. – 119 с.
11. Качаева Г.И., Попов А.Д., Рогозин Е.А. Показатели эффективности функционирования при разработке систем защиты информации от несанкционированного доступа в автоматизированных информационных системах. Вестник Дагестанского государственного технического университета. Технические науки. 2018;45(1):147–159. DOI: https://doi.org/10.21822/2073-6185-2018-45-1-147-159.
12. Бородачев С.М. Теория принятия решений. С.М. Бородачев. Екатеринбург: Издательство Уральского университета, 2014. – 124 с.
13. Леонов Г.А., Кузнецов Н.В., Кудряшова Е.В., Кузнецова О.А. (2011). Современные методы символьных вычислений: ляпуновские величины и 16-я проблема Гильберта. Труды СПИИРАН, 1(16), с. 5–36. DOI: https://doi.org/10.15622/sp.16.1.
14. Бубнов В.П., Еремин А.С., Сергеев С.А. (2015). Особенности программной реализации численно-аналитического метода расчёта моделей нестационарных систем обслуживания. Труды СПИИРАН, 1(38), с. 218–232. DOI: https://doi.org/10.15622/sp.38.12.

REFERENCES:

[1] Radko N.M. Penetration into the computer-operating environment: models of malicious remote access. N.M. Radko, Yu.K. Yazov, N.N. Korneeva. Voronezh: Voronezh State Technical University, 2013. – 265 p. (in Russian).
[2] Yazov Yu.K. Methodology for evaluating the effectiveness of information protection in information systems from unauthorized access: monograph. Yu.K. Yazov, S.V. Solovyov. St. Petersburg: High-tech technologies, 2023. – 258 p. (in Russian).
[3] Efimov, Aleksey O. et al. Conceptual foundations for assessing the level of security of automated systems based

on their vulnerability. IT Security (Russia), [S.l.], v. 30, no. 2, p. 63–79, 2023. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2023.2.04 (in Russian).

[4] Yazov Yu.K. Petri-Markov networks and their application for modeling the processes of implementing information security threats in information systems: monograph. Yu.K. Yazov, A.V. Anishchenko. Voronezh: Kvart, 2020. – 173 p. (in Russian).

[5] Shcheglov K.A. Mathematical models and methods of formal design of information systems protection systems. K.A. Shcheglov, A.Yu. Shcheglov. St. Petersburg: St. Petersburg State University ITMO, 2014. – 83 p. (in Russian).

[6] Drovnikova I.G., Popova A.D. Methods for assessing the level of security of software of automated systems of internal affairs bodies and directions for their improvement. Herald of Dagestan State Technical University. Technical Sciences. 2023;50(4):85-92. DOI: 10.21822/2073-6185-2023-50-4-85-92. (in Russian). – EDN: LDTFDM.

[7] Drovnikova I.G. Indicators of the security of software used at the objects of informatization of internal affairs bodies. I.G. Drovnikova, A.D. Popova.Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia. 2024, no. 1, p. 50–59. URL: https://ВИ.МВД.РФ/Nauka/nauchnij-zhurnal-vestni/Vestnik_1_2024.pdf (accessed: 18.04.2024) (in Russian).

[8] Pleskunov M.A. Theory of queuing: a textbook for university students studying at UGN 01.00.00 "Mathematics and Mechanics". M.A. Pleskunov; 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 Press, 2022. – 264 p. – ISBN 978-5-7996-3539-8. – EDN RSQUKA (in Russian).

[9] Korolyuk V.S. Semimarkov processes and their applications. V.S. Korolyuk, A.F. Turbin. Kiev: Naukova dumka, 1976. – 184 p. (in Russian).

[10] Krasnov A.Y. Statistical methods in engineering research. A.Y. Krasnov. St. Petersburg: ITMO University, 2022. – 119 p. (in Russian).

[11] Kachaeva G.I., Popov A.D., Rogozin E.A. Functional performance indicators during systems development to protect information from unauthorised access. Herald of Dagestan State Technical University. Technical Sciences. 2018;45(1):147-159. DOI: https://doi.org/10.21822/2073-6185-2018-45-1-147-159 (in Russian).

[12] Borodachev S.M. Theory of decision-making. S.M. Borodachev. Yekaterinburg: Ural University Press, 2014. – 124 p. (in Russian).

[13] Leonov G., Kuznetsov N., Kudryashova E., Kuznetsova O. (2011). Modern symbolic computation methods: Lyapunov quantities and 16th Hilbert problem. SPIIRAS Proceedings, 1(16), p. 5–36. DOI: https://doi.org/10.15622/sp.16.1 (in Russian).

[14] Bubnov V., Eremin A., & Sergeev, S. (2015). Program Implementation of the Numerical-Analytical Method for Computation of Non-Stationary Service System Models. SPIIRAS Proceedings, 1(38), p. 218–232. DOI: https://doi.org/10.15622/sp.38.12 (in Russian).

Поступила в редакцию – 28 апреля 2024 г. Окончательный вариант – 01 июня 2024 г.
Received – April 28, 2024. The final version – June 01, 2024.