ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056
DOI: 10.21822/2073-6185-2023-50-4-85-92 Оригинальная статья /Original article

Способы оценки уровня защищенности программного обеспечения автоматизированных систем органов внутренних дел и направления их совершенствования

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

Резюме. Цель. Целью статьи является анализ существующих способов и процедур, используемых для оценивания уровня защищенности программного обеспечения автоматизированных систем, на основе исследования научной литературы, международных и отраслевых стандартов РФ по информационной безопасности автоматизированных систем, руководящих и методических документов Федеральной службы по техническому и экспортному контролю России, а также ведомственных приказов по вопросам защиты информации от несанкционированного доступа на объектах информатизации органов внутренних дел. **Метод.** Для достижения поставленной цели использован метод системного анализа подходов, применяемых при оценивании уровня защищенности программного обеспечения в автоматизированных системах. **Результат.** Представлены результаты анализа основных подходов к оцениванию уровня защищенности программного обеспечения в автоматизированных системах. Обоснована целесообразность объединения рассмотренных подходов для проведения количественной оценки уровня защищенности программного обеспечения на объектах информатизации органов внутренних дел в режиме реального времени с учетом уязвимостей в используемых программных средствах. **Вывод.** Полученные результаты могут быть использованы для формирования показателей уровня защищенности программного обеспечения в автоматизированных системах органов внутренних дел и разработки методики их расчета с учетом фактора времени.

Ключевые слова: автоматизированная система, программное обеспечение, уязвимость, критичность уязвимости, уровень защищенности, оценка уровня защищенности

Для цитирования: И.Г. Дровникова, А.Д. Попова. 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

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

Abstract. Objective. The purpose of the article is to analyze existing methods and procedures used to assess the level of software security of automated systems, based on a study of scientific literature, international and industry standards of the Russian Federation on information security of automated systems, guidelines and methodological documents of the Federal Service for Technical and Export Control Russia, as well as departmental orders on the protection of information from unauthorized access at informatization facilities of internal affairs bodies. **Method.** To achieve this goal, the method of system analysis of approaches used in assessing the level of software security in automated systems was used. **Result.** The results of an analysis of the main approaches

to assessing the level of software security in automated systems are presented. The expediency of combining the considered approaches to carry out a quantitative assessment of the level of software security at informatization facilities of internal affairs bodies in real time, taking into account vulnerabilities in the software used, is substantiated. **Conclusion.** The results obtained can be used to generate indicators of the level of software security in automated systems of internal affairs bodies and to develop methods for their calculation taking into account the time factor.

Keywords: automated system, software, vulnerability, vulnerability criticality, security level, security level assessment

For citation: I.G. Drovnikova, A.D. Popova. Methods for assessing the level of security of software of automated systems of internal affairs bodies and directions for their improvement. Herald of Daghestan State Technical University. Technical Sciences. 2023; 50(4):85-92. DOI:10.21822/2073-6185-2023-50-4-85-92

Введение. Заметной тенденцией последних лет в сфере информатизации органов внутренних дел (ОВД) является возрастание числа угроз безопасности информации (БИ), реализуемых посредством несанкционированного доступа (НСД) к информационным ресурсам автоматизированных систем (АС) путем эксплуатации уязвимостей в используемом программном обеспечении (ПО). Это подвергает служебную информацию ограниченного распространения, хранящуюся и обрабатываемую в АС ОВД, нарушению ее конфиденциальности, целостности или доступности.

Основные причины, обуславливающие данную тенденцию, целесообразно объединить в два блока:

1) увеличение количества обрабатываемой служебной информации ограниченного распространения, расширение ее номенклатуры, усложнение технологического цикла обработки и др. влекут за собой разнообразие и усложнение и программных средств, используемых на современных объектах информатизации правоохранительных органов, необходимых для удовлетворения возрастающих потребностей ОВД. Это, в свою очередь, приводит к росту числа потенциальных уязвимостей в ПО и, следовательно, – к необходимости решения задачи повышения уровня защищенности используемых программных средств;

2) действующие нормативные правовые акты, регламентирующие требования к защите информации (ЗИ) в современных АС ОВД, не учитывают, как вновь появляющиеся разновидности потенциально опасных уязвимостей в ПО, так и расширяющиеся возможности угроз БИ по эксплуатации уже известных уязвимостей. Это приводит к необходимости доработки имеющихся нормативных правовых актов по ЗИ на объектах информатизации ОВД в направлении проведения оценки уровня защищенности используемого ПО с учетом его уязвимостей для выбора безопасной версии ПО в соответствии с требованиями современной международной и отечественной нормативной документации, регламентирующей разработку и эксплуатацию АС, а также приказов МВД России.

Постановка задачи. На основе вышеизложенного актуальной задачей является не только выявление, классификация и анализ неустраненных (текущих) уязвимостей в компонентах ПО современных АС ОВД с точки зрения их критичности с учетом фактора времени, но также изучение существующих способов и процедур оценки уровня защищенности ПО АС с целью определения направлений их совершенствования применительно к объектам информатизации ОВД с учетом уязвимостей в используемом ПО.

Результаты проведенного анализа послужат основой для определения системы показателей и разработки методики количественной оценки уровня защищенности ПО в АС ОВД в режиме реального времени, а также формирования предложений по их использованию для оптимизации версионного выбора ПО при разработке нормативно-правовой документации, связанной с обеспечением безопасности информационных технологий на объектах информатизации ОВД [1–7].

Методы исследования. Методологической основой исследования является системный

анализ подходов, применяемых при оценивании уровня защищенности ПО, используемого на объектах информатизации. Согласно [8] защищенность (security) ПО рассматривается как одна из подхарактеристик функциональных возможностей (functionality), которые, в свою очередь, являются характеристикой качества (quality) ПО. В соответствии с [9] защищенность ПО – это совокупность свойств ПО, характеризующая его способность предотвращать НСД, случайный или преднамеренный, к программам и данным, а также степень удобства и полноты обнаружения результатов такого доступа или действий по разрушению программ и данных. Следовательно, уровень защищенности ПО в АС ОВД может быть оценен не только относительно совокупности тех задач, выполняемых ее ПО, которые заранее определены и декларированы для конкретной системы, но и относительно всего комплекса сформулированных для нее задач. При оценивании уровня защищенности ПО в настоящее время на практике применяются четыре основные подхода, позволяющие лишь частичного устранить обозначенную условность, однако ни один из походов не позволяет ее устранить в полной мере, что можно объяснить относительностью, присущей самому понятию «защищенность» [8, 9].

Обсуждение результатов. В табл. 1 представлены результаты анализа четырех наиболее популярных подходов (оценочного, экспертно-балльного, расчетного, вероятностного), используемых в настоящее время при оценивании уровня защищенности ПО в АС, которые позволяют констатировать отсутствие среди авторов единства в способах их реализации.

Таблица 1.Основные подходы, используемые при оценивании уровня защищенности ПО в АС
Table 1. Main approaches used in assessing the level of software security in an automated system

№ п/п	Характеристика подхода Characteristics of the approach	Способ реализации подхода How to implement the approach
1	Оценочный – основан на установлении соответствия уровня защищенности ПО в АС сформулированным требованиям Estimated – based on establishing compliance of the software security level in the AS with those formulated requirements	Требования по защищенности ПО формулируются в виде перечня механизмов ЗИ, которые должны быть реализованы в ПО для соответствия использующей его АС определенному уровню (классу) защищенности [10, 11] Requirements for software security are formulated in the form of a list of security mechanisms
		Требования по защищенности ПО формулируются в виде перечня функций, которые должны реализоваться ПО для достижения определенного уровня (класса) защищенности информации в АС, использующей данное ПО [12, 13] Software security requirements are formulated as a list of functions
2	Экспертно-балльный – основан на сочетании экспертного и балльного (табличного) методов оценки Expert-scoring – based on a combination of expert and scoring (tabular) assessment methods	Результаты опроса специалистов-экспертов обрабатываются и представляются в формате балльной оценки, которая интерпретируется в виде суждений об уровне защищенности ПО в АС [14–16] The results of the survey of expert specialists are processed and presented in a scoring format, which is interpreted in the form of judgments about the level of software security in the AS
3	Расчетный – основан на анализе ПО в АС на критичность уязвимостей Calculated - based on analysis of software in the AS for criticality vulnerabilities	На основе определения показателей критичности известных уязвимостей в компонентах ПО рассчитывается вероятность неэксплуатации их нарушителем, интерпретируемая в виде суждений об уровне защищенности ПО в АС [17–19] Calculated the probability of non-exploitation by the violator, interpreted in the form of judgments about the level of software security in the AS [17–19]
4	Вероятностный – основан на математическом моделировании процесса функционирования ПО в АС Probabilistic – based on mathematical modeling of the functioning process Software in AS	Для оценивания защищенности ПО в АС используются математические методы и модели, с помощью которых определяются соответствующие показатели и критерии [14, 15, 20–22, 24] Mathematical methods and models are used

Сущность *первого подхода (оценочного)* заключается в формировании требований по защищенности ПО в АС, выполнение которых будет свидетельствовать о безопасности используемых программных средств [10–13]. Целью обеспечения безопасности ПО, используемого в АС, при этом станет выполнение условий, позволяющих достигнуть сформулированных требований. В этом случае уровень защищенности ПО следует рассматривать как меру приближения к заданным условиям.

Оценочный подход может быть реализован в двух вариантах, но наиболее популярным в настоящее время является его «функциональный» вариант. В соответствии с ним требования по защищенности ПО в АС формулируются в виде перечня функций, реализация которых ПО необходима для достижения требуемого уровня защищенности информации в АС, использующей данное ПО [12, 13]. При этом уровень защищенности ПО, как правило, устанавливается экспертным путем декларативно (в качестве указанных уровней могут быть рассмотрены классы защищенности АС, использующей данное ПО). ПО считается безопасным в случае выполнения им всех функций, соответствующих заданному классу защищенности АС («функций безопасности») [14, 15].

Существенным недостатком «функционального» варианта применительно к объектам информатизации ОВД можно считать «бинарность» проводимой оценки, когда не оцениваются конкретные функции безопасности, а лишь констатируется сам факт использования опасного либо безопасного ПО при реализации данных функций сертифицированными программными средствами [21]. В результате понятие «защищенность» подменяется понятием «достаточность», что не служит мерой приближения к поставленной цели защиты информации в АС ОВД, использующей данное ПО [14].

Второй подход (экспертно-балльный), применяемый при оценивании уровня защищенности ПО в АС, состоит том, что факту обеспечения защищенности ПО ставится в соответствие ряд суждений специалистов-экспертов с использованием качественной шкалы, переводимой затем в балльную шкалу [14–16]. Находится сумма (либо произведение) набранных баллов, при превышении которой (которым) заданного порога принимается решение о достаточности уровня защищенности используемого ПО. Поскольку каждому полученному значению суммы (либо произведения) ставится в соответствие определенное суждение об уровне защищенности ПО, то указанную сумму (либо произведение) баллов следует рассматривать в качестве меры безопасности используемого ПО [14, 15].

Очевидным недостатком указанного подхода применительно к оцениванию уровня защищенности ПО, используемого в АС ОВД, является его недостаточная точность, что обусловлено участием экспертов в процессе оценивания.

Более подробно остановимся на *третьем (расчетном) подходе*, используемом при оценивании уровня защищенности ПО в АС, изложенном в [18, 19], поскольку на сегодняшний день он является новым, развивающимся.

Сущность данного подхода состоит в проведении комплексной оценки уровня защищенности ПО в АС путем расчета и сведения в матрицу массива показателей критичности известных уязвимостей в компонентах ПО с использованием Методики оценки уровня критичности уязвимостей программных, программно-аппаратных средств, разработанной ФСТЭК России [17] на основе стандарта CVSS (Common Vulnerability Scoring System) [23]. Определение элемента матрицы, имеющего максимальное значение в столбце n, указывает на критичность уязвимости в n-ом компоненте ПО АС, а элемента с максимальным значением в матрице в целом – на критичность уязвимости всего ПО, используемого в АС [19]. Связь полученных количественных величин с качественной оценкой уровня критичности уязвимости представлена таблицей, содержащейся в [17].

Поскольку рассчитанный показатель количественной оценки критичности уязвимости в ПО АС нормирован, автором [18, 19] предложена формула (1) для оценивания защищенности ПО в АС, определяющая вероятность неэксплуатации данной уязвимости нарушителем (вероятность эксплуатации уязвимости тем выше, чем выше ее критичность):

$$P_н = \left(1 - \frac{V_{кр}}{10}\right), \quad (1)$$

где: $V_{кр}$ – максимальный показатель критичности уязвимости по всем компонентам ПО АС.

Для перевода количественной оценки в качественную предложена таблица значений (табл. 2), аналогичная таблице, содержащейся в [17].

Таблица 2. Соответствие оценок защищенности ПО в АС
Table 2. Correspondence of software security ratings in the AS

№ пп	Количественная оценка Quantitative assessment	Качественная оценка Qualitative assessment
1	$P_н < 0{,}15$	Низкий/ Short
2	$0{,}15 \le P_н < 0{,}45$	Средний/Average
3	$0{,}45 \le P_н < 0{,}7$	Выше среднего/Above average
4	$0{,}7 \le P_н \le 1{,}0$	Высокий/High

Основным недостатком рассмотренного подхода применительно к объектам информатизации ОВД является отсутствие учета временного фактора при расчете вероятности эксплуатации (неэксплуатации) нарушителем уязвимости в используемом ПО.

Указанных выше недостатков лишен *четвертый (вероятностный) подход*, используемый при оценивании уровня защищенности ПО в АС, основанный на математическом моделировании процессов эксплуатации уязвимостей в используемых программных средствах. В рамках данного подхода применяются различные критерии и показатели защищенности, методики их расчета, а также критерии оптимальности [14, 15, 20–22, 24]. Рассматриваемый подход может быть использован для описания случайных событий, в частности, на основе определения их вероятностно-временных характеристик (ВВХ).

Поскольку эксплуатация уязвимости в ПО АС представляет собой сложный динамический процесс, то для его описания в настоящее время широко применяются модели, построенные на теории марковских и полумарковских процессов, сетях Петри-Маркова [15, 24], что дает возможность определять ВВХ процесса эксплуатации уязвимости и проводить количественную оценку уровня защищенности ПО, используемого в АС ОВД, в режиме реального времени.

Существует множество мнений о приоритетности рассмотренных подходов, однако правильным, на наш взгляд, выходом для устранения отмеченных их недостатков является комплексное использование различных подходов к оцениванию уровня защищенности ПО на объектах информатизации ОВД.

Для оценивания уровня защищенности ПО в АС ОВД предлагается использовать расчетно-вероятностный подход, основанный на анализе ПО на критичность уязвимостей и математическом моделировании процесса эксплуатации уязвимостей в используемых программных средствах для определения их ВВХ.

Вывод. В статье приведены результаты анализа существующих в настоящее время подходов к оцениванию уровня защищенности ПО в АС с целью определения направлений совершенствования используемых методов и процедур оценивания применительно к объектам информатизации ОВД.

Результаты проведенного анализа показали целесообразность объединения существующих подходов и использования расчетно-вероятностного подхода в качестве основы для определения системы показателей уровня защищенности ПО в АС ОВД и разработки методики их расчета с учетом фактора времени.

Перспективы использования данных показателей и методики связаны с формированием предложений, содержащих практические рекомендации по проведению количественной оценки уровня защищенности ПО в АС ОВД в режиме реального времени и выбора его оптимальной версии в интересах повышения уровня защищенности служебной информации ограниченного распространения, циркулирующей и на объектах информатизации ОВД.

Библиографический список:

1. ГОСТ Р 56939-2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования. – Москва : Стандартинформ, 2016. – 24 с.
2. 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.
3. ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. – Москва : ИПК Издательство стандартов, 2003. – 12 с.
4. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей : Руководящий документ от 4 июня 1999 г. № 114 // ФСТЭК России [Электронный ресурс]. – Режим доступа : https://fstec.ru/ dokumenty/vse-dokumenty/ spetsialnye-normativnye-dokumenty/ rukovodyashchij-dokument-ot-4-iyunya-1999-g-n-114 (дата обращения: 30.10.2023).
5. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий : Руководящий документ от 19 июня 2002 г. № 187 // ФСТЭК России [Электронный ресурс]. – Режим доступа : https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye- dokumenty/ rukovodyashchij-dokument-ot-19-iyunya-2002-g-n-187 (дата обращения: 30.10.2023).
6. Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации : приказ МВД России от 6 июля 2012 г. № 678 (в ред. приказов МВД России от 15.07.2013 № 538, 20.04.2015 № 447, 07.12.2016 № 807) [Электронный ресурс]. – Режим доступа : https://base.garant.ru/70230320/?ysclid=lmdv18b 7g0759105782 (дата обращения: 05.11.2023).
7. 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: 05.11.2023).
8. 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 05.11.2023).
9. ГОСТ 28806-89. Качество программных средств. Термины и определения [Электронный ресурс]. – Режим доступа : http://www.kimmeria.nw.ru/standart/glosys/gost_28806_90.pdf (дата обращения: 03.11.2023).
10. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации : Руководящий документ от 25 июля 1997 г. № 383 // ФСТЭК России [Электронный ресурс]. – Режим доступа : http://fstec. ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g (дата обращения: 06.11.2023).
11. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации : Руководящий документ : решение Председателя Гостехкомиссии России от 30 марта 1992 г. от 30 марта 1992 г. № 384 // ФСТЭК России [Электронный ресурс]. – Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/ 114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g (дата обращения: 05.11.2023).
12. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2: Функциональные компоненты безопасности [Электронный ресурс]. – Режим доступа : https://files.stroyinf.ru/ Data2/1/4293774/4293774728.pdf (дата обращения: 28.10.2023).
13. ISO/IEC 17000:2004. Conformity assessment. Dictionary and General principles [Электронный ресурс]. – Режим доступа : https://pqm-online.com/assets/files/ lib/std/iso_17000-2004.pdf (дата обращения: 06.11.2023).
14. Радько Н. М. Проникновения в операционную среду компьютера: модели злоумышленного удаленного доступа: учебное пособие / Н. М. Радько, Ю. К. Язов, Н. Н. Корнеева. – Воронеж : Воронежский государственный технический университет, 2013. – 265 с.
15. 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.
16. ISO/IEC 27002:2005-2013. Information technology. Security method. Practical rules of information security management [Электронный ресурс]. – Режим доступа : http://docs.cntd.ru/document/gost-r-iso-mek-17799-2005 (дата обращения 06.11.2023).
17. 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: 05.11.2023).
18. К вопросу оценки защищенности автоматизированных систем по критичности их уязвимостей / А. О. Ефимов [и др.] // Вестник воронежского института ФСИН России. – 2023. – № 2. – С. 50–54.
19. 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.
20. Попов А. Д. Модели и алгоритмы оценки эффективности систем защиты информации от несанкционированного доступа с учетом их временных характеристик в автоматизированных системах органов внутренних дел : 05.13.19 диссертация на соискание ученой степени кандидата технических наук / Попов Антон Дмитриевич. – Воронеж, 2018. – 163 с.
21. Бацких А. В. Модели оценки эффективности функционирования модифицированных подсистем управления доступом к информации в автоматизированных системах органов внутренних дел : 2.3.6. диссертация на соискание ученой степени кандидата технических наук / Бацких Анна Вадимовна. – Воронеж, 2022. – 190 с.
22. Золотых Е. С. Модели оценки опасности реализации сетевых атак в автоматизированных системах органов внутренних дел : 2.3.6. диссертация на соискание ученой степени кандидата технических наук / Золотых Елена Сергеевна. – Воронеж, 2022. – 220 с.
23. Common Vulnerability Scoring System version 3.1. Specification Document. Revision 1 [Электронный ресурс]. – Режим доступа : https:// cvss-v31-specification_r1.pdf (дата обращения: 30.10.2023).
24. 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.

References

1. GOST R 56939-2016. Data protection. Secure software development. *General requirements.* Moscow: Standardinform, 2016; 24. (In Russ)
2. GOST R ISO/IEC 25051-2017. Information Technology. System and software engineering. Requirements and quality assessment of systems and software. Moscow: Standardin-form, 2017; 32. (In Russ)
3. GOST R 51188-98. Data protection. Testing software for the presence of computer viruses. Model manual. – Moscow: IPK Publishing House of Standards, 2003; 12. (In Russ)
4. Protection against unauthorized access to information. Part 1. Information security software. Classification according to the level of control over the absence of undeclared capabilities: Guiding document dated June 4, 1999 No. 114 //FSTEC of Russia [Electronic resource]. – Access mode: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-4-iyunya-1999-g-n-114 (date of access: 10/30/2023). (In Russ)
5. Information technology security. Criteria for assessing the security of information technologies: Guiding document dated June 19, 2002;187 FSTEC of Russia [Electronic resource]. Access mode: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-19-iyunya-2002-g-n-187 (date of access: 10/30/2023). (In Russ)
6. On approval of the Instructions for organizing the protection of personal data contained in information systems of internal affairs bodies of the Russian Federation: order of the Ministry of Internal Affairs of Russia dated July 6, 2012 No. 678 (as amended by orders of the Ministry of Internal Affairs of Russia dated July 15, 2013 No. 538, 20.04. 2015 No. 447, 07.12.2016 No. 807) [Electronic resource]. Access mode: https://base.garant.ru/70230320/?ysclid=lmdv18b7g0759105782 (access date: 11/05/2023). (In Russ)
7. 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 (access date: 11/05/2023). (In Russ)
8. 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 05.11.2023). (In Russ)
9. GOST 28806-89. Quality of software. Terms and definitions [Electronic resource]. Access mode: http://www.kimmeria.nw.ru/standart/glosys/gost_28806_90.pdf (access date: 11/03/2023). (In Russ)
10. Computer facilities. Protection against unauthorized access to information. Indicators of security against unauthorized access to information: Guiding document dated July 25, 1997 No. 383 // FSTEC of Russia [Electronic resource]. Access mode: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997- g (date of access: 11/06/2023). (In Russ)
11. Automated systems. Protection against unauthorized access to information. Classification of automated

systems and requirements for information protection: Guiding document: decision of the Chairman of the State Technical Commission of Russia dated March 30, 1992 dated March 30, 1992 No. 384 // FSTEC of Russia [Electronic resource]. Access mode: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992- g (date of access: 05.11.2023). (In Russ)

12. GOST R ISO/IEC 15408-2-2013. Information technology. Methods and means of ensuring security. Criteria for assessing the security of information technologies. Part 2: Functional security components [Electronic resource]. Access mode: https://files.stroyinf.ru/Data2/1/4293774/4293774728.pdf (date of access: 10/28/2023). (In Russ)
13. ISO/IEC 17000:2004. Conformity assessment. Dictionary and General principles [Electronic resource]. Access mode: https://pqm-online.com/assets/files/lib/std/iso_17000-2004.pdf (access date: 11/06/2023). (In Russ)
14. Radko N. M. Penetrations into the computer operating environment: models of malicious remote access: textbook. N. M. Radko, Yu. K. Yazov, N. N. Korneeva. Voronezh: Voronezh State Technical University, 2013; 265. (In Russ)
15. Yazov Yu. K., Solovyov S. V. Methodology for assessing the effectiveness of information protection in information systems from unauthorized access: monograph. St. Petersburg: High technology, 2023; 258. (In Russ)
16. ISO/IEC 27002:2005-2013. Information technology. Security method. Practical rules of information security management [Electronic resource]. Access mode: http://docs.cntd.ru/document/gost-r-iso-mek-17799-2005 (access date 06.11.2023). (In Russ)
17. 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: 05.11.2023). (In Russ)
18. On the issue of assessing the security of automated systems based on the criticality of their vulnerabilities. A. O. Efimov [et al.] *Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia*. 2023; 2: 50–54. (In Russ)
19. 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)
20. Popov A. D. Models and algorithms for assessing the effectiveness of information protection systems from unauthorized access, taking into account their time characteristics in automated systems of internal affairs bodies: 05.13.19 dissertation for the scientific degree of Candidate of Technical Sciences / Popov Anton Dmitrievich. Voronezh, 2018; 163. (In Russ)
21. Batskikh A.V. Models for assessing the effectiveness of the functioning of modified subsystems for managing access to information in automated systems of internal affairs bodies: 2.3.6. dissertation for the degree of candidate of technical sciences / Batskikh Anna Vadimovna. Voronezh, 2022; 190. (In Russ)
22. Zolotykh E. S. Models for assessing the danger of implementing network attacks in automated systems of internal affairs bodies: 2.3.6. dissertation for the degree of candidate of technical sciences / Elena Sergeevna Zolotykh. Voronezh, 2022; 220. (In Russ)
23. Common Vulnerability Scoring System version 3.1. Specification Document. Revision 1 [Electronic resource]. Access mode: https:// cvss-v31-specification_r1.pdf (access date: 10/30/2023). (In Russ)
24. Yazov Yu. K. Petri-Markov networks and their application for modeling the processes of implementing threats to information security in information systems: monograph. Yu. K. Yazov, A. V. Anishchenko. – Voronezh: Kvarta, 2020; 173. (In Russ)

Сведения об авторах:

Дровникова Ирина Григорьевна**,** доктор технических наук, доцент, профессор кафедры автоматизированных информационных систем органов внутренних дел; idrovnikova@mail.ru

Попова Арина Дмитриевна, адъюнкт кафедры автоматизированных информационных систем органов внутренних дел; arnpva@mail.ru

Information about the authors:

Irina G. Drovnikova, Dr. Sci.(Eng.), Assoc. Prof., Prof., Department of Automated Information Systems of Internal Affairs Bodies; 1idrovnikova@mail.ru

Arina D. Popova, Adjunct, Department of Automated Information Systems of Internal Affairs Bodies; arnpva@mail.ru

Конфликт интересов/Conflict of interest.

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

Поступила в редакцию/ Received 06.11.2023.

Одобрена после рецензирования/ Reviced 21.11.2023.

Принята в печать/ Accepted for publication 21.11.2023.