ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004. 056

DOI: 10.21822/2073-6185-2025-52-2-130-138 Оригинальная статья /Original article

Практические рекомендации по проведению оценки защищенности программного обеспечения и выбору его оптимальной версии для эксплуатации на объектах информатизации органов внутренних дел

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

Резюме. Цель. Целью исследования является разработка практических рекомендаций по проведению количественной оценки защищенности программного обеспечения в режиме реального времени и выбору его наиболее защищенной (оптимальной) версии для эксплуатации на объектах информатизации органов внутренних дел в соответствии с требованиями действующей методической документации ФСТЭК России и с учетом особенностей и недостатков эксплуатации автоматизированных систем органов внутренних дел. **Метод.** Реализован системный подход к рассмотрению сущности проблемы оценивания защищенности программного обеспечения и проведению количественной оценки показателей защищенности. Использованы методы теоретического анализа, синтеза, дедукции. **Результат.** Представлены практические рекомендации по реализации методики анализа и количественной оценки защищенности программного обеспечения с учетом уязвимостей в динамике его функционирования и выбора наиболее защищенной версии для эксплуатации в автоматизированных системах органов внутренних дел. Дополнение существующих методик проведения оценки защищенности представленными практическими рекомендациями позволяет повысить эффективность и качество оценивания программного обеспечения в процессе его жизненного цикла на объектах информатизации органов внутренних дел. **Вывод.** Перспективы использования полученных результатов связаны с разработкой методической документации для проведения оценки состояния технической защиты информации в автоматизированных системах органов внутренних дел с целью обоснования выбора организационных и технических мер обеспечения безопасности служебной информации ограниченного распространения.

Ключевые слова: автоматизированная система органов внутренних дел, программное обеспечение, уязвимости, количественные показатели защищенности, автоматизированная оценка уровня защищенности, режим реального времени

Для цитирования: А.Д. Попова, И.Г. Дровникова. Практические рекомендации по проведению оценки защищенности программного обеспечения и выбору его оптимальной версии для эксплуатации на объектах информатизации органов внутренних дел. Вестник Дагестанского государственного технического университета. Технические науки. 2025;52(2):130-138. DOI:10.21822/2073-6185-2025-52-2-130-138

Practical recommendations for assessing software security and choosing its optimal version for use at facilities of informatization of internal affairs agencies

A.D. Popova, I.G. Drovnikova
Voronezh Institute of the Ministry of Internal Affairs of Russia,
53 Patriotov Str., Voronezh 394065, Russia

Abstract. Objective. The aim of the study is to develop practical recommendations for conducting a quantitative assessment of software security in real time and choosing its optimal version in accordance with the requirements of the FSTEC of Russia and taking into account the features and shortcomings of the operation of automated systems of internal affairs agencies.

Method. A systems approach has been implemented. The methods of theoretical analysis, synthesis, and deduction have been used. **Result.** Practical recommendations are presented for the implementation of the methodology for analyzing and quantitatively assessing the security of software, taking into account vulnerabilities and selecting the most secure version for use in automated systems of internal affairs agencies. Supplementing existing methods with practical recommendations will improve the efficiency and quality of software evaluation at IT facilities of internal affairs agencies. **Conclusion.** Prospects for using the obtained results are associated with the development of methodological documentation for assessing the state of technical information protection in automated systems of the internal affairs agencies in order to justify the choice of organizational and technical measures to ensure the security of restricted service information.

Keywords: automated system of internal affairs bodies, software, vulnerabilities, quantitative indicators of security, automated assessment of the level of security, real-time mode

For citation: A.D. Popova, I.G. Drovnikova. Practical recommendations for assessing software security and choosing its optimal version for use at facilities of informatization of internal affairs agencies. Herald of Daghestan State Technical University. Technical Sciences. 2025; 52(2):130-138. (In Russ) DOI:10.21822/2073-6185-2025-52-2-130-138

Введение. Процесс эксплуатации современных автоматизированных систем (АС) органов внутренних дел (ОВД) характеризуется рядом особенностей и недостатков, подробно рассмотренных в [1-4]. Их анализ показал, что требование обеспечения необходимой степени защищенности служебной информации ограниченного распространения, циркулирующей на объектах информатизации ОВД, может быть в значительной степени реализовано путем применения программных средств, способных безопасно функционировать в условиях растущего числа уязвимостей [5]. Следовательно, используемый программный код должен быть максимально оптимизирован с точки зрения защищенности ПО в процессе его жизненного цикла в АС ОВД.

Отсутствие соответствующих показателей, позволяющих адекватно оценивать изменение реальной защищенности ПО в процессе эксплуатации на объектах информатизации ОВД на основе анализа его уязвимостей (то есть эксплуатационную информационную безопасность (ИБ) ПО) привило к необходимости их разработки. Такого рода показатели, учитывающие возможность изменения во времени вероятностей успешной эксплуатации текущих уязвимостей высокого и критического уровней критичности в ПО и позволяющие количественно оценивать данные изменения в процессе жизненного цикла ПО в АС ОВД, предложены в [4]. Для расчета данных показателей с учетом временного фактора разработаны аналитические модели (статическая, динамические дискретные и динамическая непрерывная) и алгоритмы, которые подробно рассмотрены в [6]. В [7] описан алгоритм функционирования программного комплекса, реализующего предложенные модели и алгоритмы. Представленный программный комплекс, автоматизирующий процессы анализа и оценки защищенности ПО в режиме реального времени с учетом его уязвимостей, позволяет на основе сравнения версий используемого ПО выбрать оптимальную с точки зрения защищенности версию для эксплуатации на объектах информатизации ОВД.

Постановка задачи. Результаты анализа существующих способов оценки уровня защищенности ПО в АС [8 –18], изложенные в [19], показали их практическую непригодность для проведения количественной оценки защищенности ПО в процессе его жизненного цикла в АС ОВД. Это приводит к необходимости разработки предложений, содержащих практические рекомендации по проведению количественной оценки защищенности ПО и выбору оптимальной (наиболее защищенной) его версии для эксплуатации на объектах информатизации ОВД в соответствии с требованиями действующей методической документации Федеральной службы по техническому и экспортному контролю (ФСТЭК) России [20 – 23] с учетом особенностей и недостатков эксплуатации АС ОВД, что и является целью данной статьи.

Методы исследования. Для реализации поставленной цели использованы методы теоретического анализа документации, синтеза, дедукции. В качестве методологической основы исследования применен системный подход как к рассмотрению сущности проблемы оценивания изменения уровня защищенности ПО в отношении текущих уязвимостей в процессе его жизненного цикла в АС ОВД, так и к проведению количественной оценки показателей защищенности ПО.

Обсуждение результатов. Показатель, характеризующий текущее состояние обеспечения безопасности значимых объектов критической информационной инфраструктуры (КИИ) РФ и (или) технической защиты информации (ЗИ), не отнесенной к государственной тайне, а также нормированное значение и порядок расчета данного показателя регламентированы методическим документом «Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», утвержденным ФСТЭК России 2 мая 2024 г. [20]. Данная методика применяется для оценки текущего состояния ЗИ в государственных органах, органах местного самоуправления, организациях, в том числе субъектах КИИ, и степени его соответствия минимально необходимому уровню ЗИ от типовых актуальных угроз безопасности информации. Оценка показателя защищенности информации $K_{ЗИ}$ проводится не реже одного раза в шесть месяцев и полученное его значение является критерием принятия в органе (организации) управленческих решений в части необходимости реализации первоочередных мер по ЗИ от актуальных угроз безопасности информации и их приоритетности.

Порядок и содержание работ по тестированию ПО, в том числе с открытым исходным кодом, предназначенного для устранения уязвимостей в программных, программно-аппаратных средствах (обновления безопасности), которые применяются в информационных системах, информационно-телекоммуникационных сетях, АС управления, в том числе функционирующих на базе информационно-телекоммуникационной инфраструктуры центров обработки данных, регламентируются методическим документом «Методика тестирования обновлений безопасности программных, программно-аппаратных средств», утвержденным ФСТЭК России 28 октября 2022 г. [21]. Данная Методика применяется при принятии операторами информационных систем мер, направленных на устранение указанных уязвимостей в соответствии с требованиями по обеспечению безопасности значимых объектов КИИ Российской Федерации, а также требованиями по ЗИ государственных информационных систем, иными нормативными правовыми актами и методическими документами ФСТЭК России. Поскольку АС ОВД являются государственными информационными системами и, безусловно, относятся к значимым объектам КИИ РФ, то разрабатываемые практические рекомендации по проведению оценки защищенности ПО в АС ОВД, учитывающие особенности и недостатки эксплуатации данных систем, и выбору наиболее защищенной версии для использования на объектах информатизации, не должны противоречить положениям указанных методических документов.

В соответствии с [20] проведение оценки показателя защищенности ПО в АС ОВД ($K_{З\,ПО}$) должно включать:

– сбор и анализ необходимых для оценивания исходных данных (акты, протоколы, отчеты и другие документы, составленные по результатам государственного контроля, внутреннего контроля и внешней оценки соответствия в области ЗИ; внутренние организационно-распорядительные документы по ЗИ; эксплуатационную документацию на средства ЗИ; результаты проведения инвентаризации объектов информатизации ОВД; результаты опроса сотрудников по обеспечению ИБ АС ОВД; результаты анализа применения отдельных программных, программно-аппаратных средств АС ОВД; результаты работы инструментальных средств анализа и оценки защищенности ПО на объектах информатизации ОВД и (или) мониторинга его ИБ);

– проведение оценки частных показателей безопасности ПО K_{nm}, характеризующих

реализацию отдельных мер по обеспечению защищенности ПО от актуальных угроз безопасности информации на объекте информатизации ОВД (n – номер группы частных показателей безопасности, m – номер показателя в группе частных показателей безопасности);

– расчет значения показателя $K_{З\,ПО}$ по формуле (1)

$$K_{З\,ПО} = (K_{11} + K_{12} + K_{13})R_1 + (K_{21} + K_{22} + \ldots + K_{2m})R_2 + (K_{31} + K_{32} + \ldots + K_{3m})R_3 + +(K_{41} + K_{42} + \ldots + K_{4m})R_4,$$

где R_n – весовой коэффициент частных показателей безопасности ПО, отнесенных к -ой группе, $n = 1..4$, и его сравнение с нормированным значением ($K_{З\,ПО} = 1$).

В [20] представлены критерии оценки показателя защищенности ПО, произведенной по 4-м основным группам частных показателей безопасности:организация и управление, защита пользователей, защита информационных систем, мониторинг ИБ и реагирование (табл. 1).

Таблица 1. Оценка состояния обеспечения ИБ ПО в АС ОВД
Table 1. Assessment of the state of information security software in the ATS AS

Значение $K_{З\,ПО}$ Meaning	**Характеристика текущего состояния защищенности ПО Characteristics of the current state of software security**
$K_{З\,ПО} \leq 0{,}75$	Уровень состояния защищенности ПО – критический «красный»: минимальный уровень защиты от типовых актуальных угроз безопасности информации не обеспечен, существует реальная возможность реализации угроз/ Software security status level is critical "red"
$0{,}75 < K_{З\,ПО} < 1$	Уровень состояния защищенности ПО – низкий «оранжевый»: минимальный уровень защиты от типовых актуальных угроз безопасности информации не обеспечен, существуют предпосылки реализации угроз/ Software security status level is low "orange"
$K_{З\,ПО} = 1$	Уровень состояния защищенности ПО – минимальный базовый «зеленый»: минимальный уровень защиты от типовых актуальных угроз безопасности информации обеспечен Software security status level – minimum basic “green”

Необходимо отметить, что при рассмотрении группы частных показателей безопасности «Защита информационных систем» в [20] не учитывается значительное количество уязвимостей в ПО АС ОВД критического уровня опасности. При этом в случае соблюдения всех указанных в Методике требований уровень состояния защищенности ПО в АС ОВД будет низким («оранжевым»), что в соответствии с [20] требует разработки плана реализации мероприятий по достижению следующего уровня состояния защищенности ПО от актуальных угроз. Кроме того, данная оценка допускает отсутствие проверки вложений на наличие вредоносного ПО и централизованного управления средствами антивирусной защиты (на ~ 20 % пользовательских устройств).

В результате значительное количество устройств, обладающих огромным числом неустраненных уязвимостей в ПО, в том числе и критических, окажутся неучтенными, что может послужить причиной существенного сбоя в работе АС ОВД. Следовательно, необходимо проведение регулярного тестирования обновлений безопасности с учетом уязвимостей критического уровня критичности в используемом ПО.

Согласно [21] тестированию подлежат обновления безопасности, направленные на устранение уязвимостей, уровень критичности которых должен определяться в соответствии с требованиями методического документа «Методика оценки уровня критичности уязвимостей программных и программно-аппаратных средств», утвержденного ФСТЭК России 28 октября 2022 г. [22].

Тестирование обновлений безопасности проводится с целью своевременного выявления в них потенциально опасных функциональных возможностей, незадекларированных разработчиком программных, программно-аппаратных средств, и включает следующие этапы:

1) Этап подготовки к проведению тестирования – получение обновлений безопасности и подготовка среды тестирования (исследовательского стенда, тестовой зоны АС, функционирующей в штатном режиме АС ОВД).

2) Этап проведения тестирования – выполнение тестов Т001 – Т006 (табл. 2).

Таблица 2. Характеристика этапа проведения тестирования обновлений безопасности
Table 2. Characteristics of the stage of testing security updates

Название теста **Test name**	**Содержание и условия выполнения теста** **Contents and conditions of execution and testing**
Т001 – сверка идентичности identity verification	Заключается в получении обновлений безопасности из различных источников и (или) различными способами, расчете и сравнении их контрольных сумм. Проводится, если имеется возможность получать обновления безопасности из различных источников и (или) различными способами/ receiving security updates
Т002 – проверка подлинности authenticity Check	Заключается в распаковке файлов обновлений безопасности и определении критериев проверки их подлинности. Проводится, если имеются предоставляемые разработчиком обновления штатных средств проверки подлинности файлов обновлений безопасности, а также если до установки файлов в среде функционирования исследователь может получать их в распакованном (расшифрованном) виде/ unpacking update files
Т003 – антивирусный контроль Antivirus Control	Заключается в выявлении вредоносных компьютерных программ (вирусов) в исследуемых обновлениях безопасности с использованием средств антивирусной защиты. Проводится, если имеются не менее двух средств антивирусной защиты разных разработчиков/ detection of malicious computer programs
Т004 – поиск опасных конструкций Search for Dangerous Constructions	Заключается в поиске опасных конструкций в обновлениях безопасности с применением YARA-правил, индикаторов компрометации и др., контекстном поиске политических баннеров, лозунгов и другой противоправной информации в обновлениях безопасности. Проводится, если до или после установки файлов обновлений в среде функционирования у исследователя имеется возможность получать их в распакованном виде/ search for dangerous structures
Т005 – мониторинг активности Activity Monitoring	Заключается в получении и анализе сведений о поведении обновляемых программных, программно-аппаратных средств в результате их взаимодействия со средой функционирования или другими программами, а также анализе сведений о взаимодействии компонентов обновляемых программных, программно-аппаратных средств. Проводится, если имеется возможность установки необходимых инструментов в среде тестирования обновляемого программного, программно-аппаратного средства/ analysis of information about updated programs
Т006 – ручной анализ Manual Analysis	Заключается в анализе логики работы, исследовании компонентов обновлений безопасности с помощью трассировщиков и отладчиков, проверке присутствия ключевой информации в обновлениях безопасности, использовании статического и динамического анализа. Проводится, если по результатам выполнения тестов: выявлены различия в обновлениях безопасности, полученных разными способами и (или) из разных источников; обнаружены признаки вредоносной активности в файлах обновлений безопасности в результате антивирусного контроля или мониторинга их активности в среде функционирования; неуспешно пройден тест подлинности файлов обновлений безопасности; выявлены опасные конструкции/ analysis of the logic of the update components

– Этап оформления результатов тестирования – подготовка отчета тестирования обновлений безопасности, включающего: наименования обновлений безопасности; сведения о местах размещения обновлений безопасности, контрольных суммах, дате их выпуска, разработчике, версиях ПО; сведения об уязвимостях, на устранение которых направлены обновления безопасности; наименования проведенных тестов; результаты тестирования (успешно/не успешно); описание результатов тестирования, включая средства проведения тестирования, среду тестирования, выявленные признаки недекларированных возможностей, описания проведенных тестов.

Отчеты тестирования обновлений безопасности направляются на адрес электронной почты webmaster@bdu.fstec.ru, где после проведения верификации полученные результаты тестирования размещаются оператором в Банке данных угроз безопасности информации ФСТЭК России в течение одного рабочего дня. В соответствии с [21] решение об установке протестированных обновлений безопасности должен принимать оператор АС ОВД с учетом результатов тестирования и оценки нарушения функционирования системы от установки таких обновлений. Учитывая результаты проведенных исследований [4, 6, 7, 24]

предлагается расширить содержание основных этапов реализации рассмотренной Методики [21] применительно к объектам информатизации ОВД и разработать практические рекомендации по проведению оценки защищенности ПО в процессе его жизненного цикла и выбору наиболее защищенной (оптимальной) версии для эксплуатации в АС ОВД, изложенные в табл. 3.

Таблица 3. Практические рекомендации по реализации методики анализа, оценки защищенности и выбора оптимальной версии ПО для эксплуатации в АС ОВД

Table 3. Practical recommendations for the implementation of the methodology for analysis, security assessment and selection of the optimal version of software for operation in the ATS AS

№ этапа Stage number	Название этапа Stage name	Содержание этапа Stage content
1	Подготовка к проведению тестирования Preparing for testing	Получение версий используемого ПО. Подготовка среды тестирования – функционирующей в штатном режиме АС ОВД
2	Проведение тестирования Conducting testing	Формирование исходных данных для проведения тестирования каждой версии ПО [24]: Определение исходных данных для расчета статического показателя защищенности ПО $V_{\text{кр0}}$ – уровня критичности уязвимостей в версии ПО. Определение исходных данных для расчета динамического показателя защищенности ПО $V_{\text{г0}}$ – коэффициента готовности версии ПО к безопасной эксплуатации в отношении уязвимостей. Определение исходных данных для расчета динамического показателя защищенности ПО $V_{\text{ин0}}$ – интервального показателя нарушения защищенности версии ПО. Определение исходных данных для расчета динамического показателя защищенности ПО $V_{\text{взо}}(t)$ – показателя временной защищенности версии ПО)
		Автоматизированное оценивание показателей защищенности каждой версии ПО (с использованием разработанного программного комплекса) [4, 6]: Расчет уровня критичности уязвимостей в версии ПО ($V_{\text{кр0}}$) на основе аналитической статической модели. Расчет коэффициента готовности версии ПО к безопасной эксплуатации ($V_{\text{г0}}$) в отношении уязвимостей на основе аналитической динамической дискретной модели. Расчет интервального показателя нарушения защищенности версии ПО ($V_{\text{ин0}}$) на основе аналитической динамической дискретной модели. Расчет показателя временной защищенности версии ПО ($V_{\text{взо}}(t)$) на основе аналитической динамической непрерывной модели. Расчет комплексного показателя защищенности версии ПО ($V_{\text{зо ПО}}$). Автоматизированное сравнение версий ПО и выбор наиболее защищенной его версии (с использованием разработанного программного комплекса) [7]
3	Оформление результатов тестирования Registration of test results	Составление отчета тестирования: Наименования версий используемого ПО. Сведения об уязвимостях в версиях ПО. Описание результатов тестирования (сведения о значениях комплексных показателей защищенности версий ПО). Наименование оптимальной (наиболее защищенной) версии ПО

Вывод. Результаты верификации предложенной методики анализа, оценки защищенности и выбора наиболее защищенной (оптимальной) версии ПО с использованием разработанного программного комплекса подтвердили ее эффективность. Полученные результаты дают основание констатировать, что дополнение утвержденных ФСТЭК России Методик [20, 21] представленными практическими рекомендациями по проведению количественной оценки защищенности ПО в режиме реального времени и выбору наиболее защищенной (оптимальной) его версии для эксплуатации в АС ОВД позволит повысить эффективность и качество оценивания с учетом уязвимостей в процессе жизненного цикла ПО на объектах информатизации ОВД.

Представленные в статье предложения, содержащие практические рекомендации по применению разработанных моделей, алгоритмов и программного комплекса при проведении количественной оценки защищенности ПО, учитывая особенности и недостатки эксплуатации АС ОВД, могут быть использованы при разработке методической документации для оценивания состояния технической защиты информации на объектах информатизации ОВД. Перспективы проведения такой оценки связаны с обоснованием выбора организационных и технических мер обеспечения безопасности служебной информации ограниченного распространения, циркулирующей в АС ОВД.

Библиографический список:

1. Золотых Е.С. Модели оценки опасности реализации сетевых атак в автоматизированных системах органов внутренних дел:дис. канд. техн. наук:2.3.6. Золотых Елена Сергеевна. Воронеж, 2022. 220 с.
2. Бацких А.В. Модели оценки эффективности функционирования модифицированных подсистем управления доступом к информации в автоматизированных системах органов внутренних дел: 2.3.6. дисс. канд. техн. наук/Бацких Анна Вадимовна. Воронеж, 2022. – 190 с.
3. 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 дис. канд. техн. наук/ Попов Антон Дмитриевич. Воронеж, 2018. 163 с.
4. 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.
5. Щеглов А.Ю. Элементы теории эксплуатационной информационной безопасности: учебное пособие / А. Ю. Щеглов. – Санкт-Петербург: СПбГУ ИТМО, 2014. – 59 с.
6. 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.
7. Попова А.Д. Алгоритм функционирования программного комплекса анализа и оценки защищенности программного обеспечения автоматизированных систем органов внутренних дел//Вестник Дагестанского государственного технического университета. Технические науки.2024.Т.51(2).С.128–136.
8. ГОСТ РИСО/МЭК 25051-2017 Информационные технологии. Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения. М.:Стандартинформ, 2017. 32 с.
9. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий:Руководящий документ от 19 июня 2002 г. № 187 // ФСТЭК России [Эл. ресурс]. – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-19-iyunya-2002-g-n-187 (дата обращения: 30.10.2024).
10. ГОСТ Р ИСО/МЭК 9126-93. Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению [Эл.ресурс]. – Режим доступа : http://docs.cntd.ru/document/gost-r-iso-mek-9126-93 (дата обращения 05.11.2024).
11. ISO/IEC 17000:2004. Conformity assessment. Dictionary and General principles [Эл. ресурс]. – Режим доступа : https://pqm-online.com/assets/files/lib/std/ iso17000-2004.pdf (дата обращения: 06.11.2024).
12. ISO/IEC 27002:2005-2013 Information technology. Security method. Practical rules of information security management [Эл. рес.]. http://docs.cntd.ru/document/gost-r-iso-mek-17799-2005(дата об.06.11.2024).
13. Ефимов А.О., И.И. Лившиц, Т.В. Мещерякова, Е. А. Рогозин. Концептуальные основы оценки уровня защищенности автоматизированных систем на основе их уязвимости// Безопасность информационных технологий = IT Security. – Том 30. – № 2(2023). – С. 63–79.
14. 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.
15. Радько Н.М., Ю.К. Язов, Н.Н. Корнеева. Проникновения в операционную среду компьютера: модели злоумышленного удаленного доступа: учеб. пособ. Воронеж: Воронежский государственный технический университет, 2013. – 265 с.
16. Язов Ю.К., С.В. Соловьев. Методология оценки эффективности защиты информации в информационных системах от несанкционированного доступа:монография. Санкт-Петербург:Наукоемкие технологии, 2023. – 258 с.
17. Язов Ю.К., А.В. Анищенко. Сети Петри-Маркова и их применение для моделирования процессов реализации угроз безопасности информации в информационных системах:монография. – Воронеж : Кварта, 2020. – 173 с.
18. Common Vulnerability Scoring System version 4.0: User Guid–e [Электронный ресурс]. – Режим доступа: https://www.first.org/cvss/v4.0/user-guide (дата обращения: 15.11.2024).
19. 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.

20. Методика оценки показателя состояния технической защиты информации и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации : методический документ от 2 мая 2024 г. // ФСТЭК России [Электронный ресурс]. – Режим доступа : https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-2-maya-2024-g (дата обращения: 25.11.2024).
21. 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-2 (дата обращения: 25.11.2024).
22. 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: 20.11.2024).
23. Руководство по организации процесса управления уязвимостями в органе (организации) : методический документ от 17 мая 2023г.ФСТЭК России [Эл.ресурс].https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-17-maya-2023-g (дата обращения: 25.11.2024).
24. Попова А.Д. Методика эксперимента для оценивания защищенности программного обеспечения автоматизированных систем органов внутренних дел/А.Д. Попова, А.Д. Попов, И.Г. Дровникова // Безопасность информационных технологий = IT Security. – Том 32. – № 1(2025). – С. 95–111.

References:

1. Zolotykh E.S.Models for assessing the danger of implementing network attacks in automated systems of internal affairs bodies:dis.Cand.of Techn.Scie.2.3.6.Zolotykh Elena Sergeevna.Voronezh, 2022:220(In Russ).
2. Batskikh A. V. Models for assessing the effectiveness of modified information access control subsystems in automated systems of internal affairs bodies: dis. 2.3.6. Cand. of Techn. Scie. Batskikh Anna Vadimovna. - Voronezh, 2022: 190 p. (In Russ).
3. 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 dis. Cand. of Technical Scie.Popov Anton Dmitrievich. Voronezh, 2018:163 p. (In Russ).
4. Drovnikova I. G. Security indicators of software used at the information technology facilities of the internal affairs bodies / I. G. Drovnikova, A. D. Popova. *Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia*. 2024;1:50–59. (In Russ).
5. Shcheglov A.Yu. Elements of the theory of operational information security: a tutorial / A. Yu. Shcheglov. – St. Petersburg: SPbSU ITMO, 2014: 59 p. (In Russ).
6. Popova A. D. Methodology for analyzing and assessing the security level of software used at the information technology facilities of the internal affairs bodies /A. D. Popova, I. G. Drovnikova. *Information technology security = IT Security*. 2024; 31(2):51–64. (In Russ).
7. Popova A.D. Algorithm for the functioning of the software package for analyzing and assessing the security of software of automated systems of internal affairs bodies. *Herald of the Daghestan State Technical University. Technical Sciences.* 2024; 51(2):128–136. (In Russ).
8. GOST R ISO/IEC 25051-2017. Information technology. Systems and software engineering. Requirements and quality assessment of systems and software. – Moscow: Standartinform, 2017: 32 p. (In Russ).
9. Information technology security. Criteria for assessing the security of information technology: Guidance document of June 19, 2002, No. 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 (accessed: 10/30/2024). (In Russ).
10. GOST R ISO / IEC 9126-93. Information technology. Software product evaluation. Quality characteristics and guidelines for their application [Electronic resource]. - Access mode: http://docs.cntd.ru/document/gost-r-iso-mek-9126-93 (accessed 11/05/2024). (In Russ).
11. ISO/IEC 17000:2004. Conformity assessment. Dictionary and General principles [Electronic resource]. – Access mode: https://pqm-online.com/assets/files/lib/std/iso17000-2004.pdf (accessed: 06.11.2024).
12. ISO/IEC 27002:2005-2013. Information technology. Security method. Practical rules of information security management[El.resource].:http://docs.cntd.ru/document/gost-r-iso-mek-17799-2005(06.11.2024).
13. Efimov A.O. Conceptual foundations 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).
14. 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).
15. Radko N.M. Penetrations into the computer operating environment: models of malicious remote access: tutorial/N.M. Radko, Yu.K. Yazov, N.N. Korneeva. Voronezh:Voronezh State Technical University, 2013; p.

16. Yazov Yu. K., S.V. Soloviev. Methodology for assessing the effectiveness of information protection in information systems from unauthorized access: monograph. St. Petersburg: Science-intensive technologies, 2023;258 p. (In Russ).
17. Yazov Yu.K., A.V. Anishchenko. Petri-Markov networks and their application for modeling the processes of implementing information security threats in information systems: oronezh:Kvarta, 2020;173(In Russ).
18. Common Vulnerability Scoring System version 4.0: User Guid–e [Electronic resource]. – Access mode: https://www.first.org/cvss/v4.0/user-guide (date of access: 15.11.2024). (In Russ).
19. 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).
20. Methodology for assessing the indicator of the state of technical protection of information and ensuring the security of significant objects of the critical information infrastructure of the Russian Federation: methodological document of May 2, 2024//FSTEC of Russia [Electronic resource]. - Access mode: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-2-maya-2024-g (date of access: 11/25/2024). (In Russ).
21. Methodology for testing security updates for software, firmware and hardware: methodological document of 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: 25.11.2024). (In Russ).
22. Methodology for assessing the criticality level 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: 20.11.2024). (In Russ).
23. Guidelines for organizing the vulnerability management process in a body (organization): methodological document dated May 17,2023. FSTEC of Russia [Electronic resource]. Access mode: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-17-maya-2023-g (accessed: 11/25/2024). (In Russ).
24. Popova A.D., A.D. Popov, I.G. Drovnikova. Experimental methodology for assessing the security of software of automated systems of internal affairs bodies. *Information Technology Security = IT Security.* 2025; 32(1):95-111. (In Russ).

Сведения об авторах:

Арина Дмитриевна Попова, адъюнкт; arnpva@mail.ru

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

Information about authors:

Arina D. Popova, adjunct; arnpva@mail.ru

Irina G. Drovnikova, Dr. Sci.(Eng.), Prof., Prof., Department of Automated Information Systems of Internal Affairs Bodies; idrovniko-va@mail.ru

Конфликт интересов/Conflict of interest.

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

Поступила в редакцию/ Received 17.04. 2025.

Одобрена после рецензирования/ Reviced 22.05.2025.

Принята в печать/ Accepted for publication 02.06.2025.