ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004. 056

DOI: 10.21822/2073-6185-2025-52-3-116-125 Оригинальная статья /Original article

Организация и методика эксперимента для определения исходных данных при оценивании показателей защищенности программного обеспечения автоматизированных систем органов внутренних дел

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

Резюме. Цель. Целью исследования является разработка методики проведения натурного эксперимента для определения исходных данных, необходимых при оценивании защищенности программного обеспечения, используемого на объектах информатизации органов внутренних дел, в динамике его функционирования. Методика позволяет выявлять потенциально возможные уязвимости высокого и критического уровня критичности в процессе функционирования программного обеспечения, определять значения временных характеристик их эксплуатации, средние значения времен выявления и устранения текущих уязвимостей в программном обеспечении. **Метод.** Использованы методы теории графов, автоматизированного статического анализа программного кода, электронной хронометрии, прямого измерения, анализа статистических данных, сравнения. **Результат.** Получены количественные значения исходных данных, необходимые для проведения оценки комплексного показателя защищенности программного обеспечения автоматизированных систем органов внутренних дел, включающего показатель уровня критичности совокупности уязвимостей в программном обеспечении, показатель временной защищенности программного обеспечения, коэффициент готовности программного обеспечения к безопасному функционированию при наличии уязвимостей, интервальный показатель нарушения защищенности программного обеспечения за счет эксплуатации уязвимости заданного уровня критичности. **Вывод.** Перспективы практической реализации предложенной методики связаны с проведением анализа и точной количественной оценки защищенности используемого программного обеспечения в режиме реального времени на основе разработанного программного комплекса с целью выбора его наиболее защищенной версии в интересах повышения уровня защищенности служебной информации ограниченного распространения, циркулирующей на конкретных объектах информатизации органов внутренних дел.

Ключевые слова: уязвимости в программном обеспечении, временные характеристики эксплуатации уязвимости, среднее время выявления уязвимости, среднее время устранения уязвимости, натурный эксперимент, электронный хронометраж, SAST-анализатор SonarQube

Для цитирования: А.Д. Попова, И.Г. Дровникова, А.Д. Попов. Организация и методика эксперимента для определения исходных данных при оценивании показателей защищенности программного обеспечения автоматизированных систем органов внутренних дел. Вестник Дагестанского государственного технического университета. Технические науки. 2025;52(3): 116-125. DOI:10.21822/2073-6185-2025-52-3-116-125

Organization and methodology of an experiment to determine initial data for assessing software security indicators for automated systems of internal affairs agencies

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

Abstract. Objective. The aim of the article is to develop a methodology for conducting a full-scale experiment to determine the initial data necessary for assessing the security of software

used in the information technology systems of internal affairs agencies, in the dynamics of its operation. The methodology allows for the identification of potential vulnerabilities of high and critical levels of criticality during software operation, determining the values of the time characteristics of their operation, and the average values of the times to identify and eliminate current vulnerabilities in the software. **Method.** To achieve the stated objective, the methods of graph theory, automated static analysis of program code, electronic chronometry, direct measurement, analysis of statistical data, and comparison were used. **Result.** The application of the proposed methodology yielded quantitative values of the initial data required for assessing the comprehensive software security indicator for automated systems of internal affairs agencies. This indicator includes the criticality level of a set of software vulnerabilities, the software security time indicator, the software readiness coefficient for safe operation in the presence of vulnerabilities, and the interval indicator of software security breach due to exploitation of a vulnerability of a given criticality level. **Conclusion.** The prospects for the practical implementation of the proposed methodology are related to the analysis and accurate quantitative assessment of the software security in use in real time based on the developed software package. This is achieved by selecting the most secure version to improve the security of restricted service information circulating at specific information systems of internal affairs agencies.

Keywords: software vulnerabilities, vulnerability exploitation time characteristics, average vulnerability detection time, average vulnerability remediation time, full-scale experiment, electronic timing, SonarQube SAST analyzer

For citation: A.D. Popova, I.G. Drovnikova, A.D. Popov. Organization and methodology of an experiment to determine initial data for assessing software security indicators for automated systems of internal affairs agencies. Herald of Daghestan State Technical University. Technical Sciences.2025;52(3): 116-125. (In Russ) DOI:10.21822/2073-6185-2025-52-3-116-125

Введение. В связи со стремительным ростом информационных технологий (ИТ), применяемых на современных объектах информатизации органов внутренних дел (ОВД), важным направлением деятельности правоохранительных органов является использование безопасного программного обеспечения (ПО) при решении служебных задач [1].

В то же время практика применения программных продуктов, разработанных различными вендорами, в автоматизированных системах (АС) ОВД подтверждает использование многочисленных их версий, в которых существуют и регулярно обнаруживаются новые уязвимости. В этих условиях возрастает актуальность выбора необходимых мер защиты используемого ПО, в том числе выбора наиболее защищенных версий программных продуктов для повышения эффективности защиты служебной информации ограниченного распространения, циркулирующей на объектах информатизации ОВД. Осуществление выбора наиболее защищенных версий ПО приводит к необходимости проведения оценки критичности выявляемых уязвимостей [2] и анализа защищенности используемого ПО в динамике функционирования в АС ОВД, что предполагает определение количественных значений показателей его защищенности с помощью разработанного программного комплекса [3–5].

Поскольку согласно опубликованной статистике [6–9] на защищенность ПО существенное влияние оказывают уязвимости высокого и критического уровня критичности, то лишь их будем рассматривать при проведении натурного эксперимента с целью определения исходных данных для расчета показателей защищенности ПО АС ОВД.

В соответствии с поставленной целью сформулированы основные задачи натурного эксперимента:

- выявление потенциально возможных уязвимостей высокого и критического уровня критичности в процессе функционирования ПО в АС ОВД;
- определение значений временных характеристик эксплуатации текущих уязвимостей высокого и критического уровня критичности в ПО (τ_{ij});
- определение средних значений времен выявления ($\overline{\tau_{\text{ву},n}}$) и устранения ($\overline{\tau_{\text{ву},n}}$) уязвимости высокого и критического уровня критичности в ПО.

Методы исследования. Для решения поставленных задач натурного эксперимента использованы методы теории графов, автоматизированного статического анализа программного кода на основе применения SAST-анализатора SonarQube, прямого измерения в виде электронной хронометрии с использованием встроенных инструментов ПО, анализа статистических данных, сравнения. В качестве методологической основы исследования применен системный подход к определению значений временных характеристик эксплуатации уязвимостей и средних значений времен их выявления и устранения в ПО АС ОВД.

Обсуждение результатов. Методика проведения натурного эксперимента включала в себя три основных этапа.

На первом этапе эксперимента был развернут имитационный стенд АС ОВД, необходимый для воспроизведения сценария реализации злоумышленником угрозы несанкционированного доступа (НСД) к информации путем эксплуатации уязвимостей в ПО.

Развертывание проводилось в виде виртуальной локальной вычислительной сети топологии «звезда», где центральным узлом выступал сервер, к которому подключались три виртуальных автоматизированных рабочих места (АРМ) пользователей. Настройка типового АРМ пользователя осуществлялась согласно рекомендациям Департамента информационных технологий связи и защиты информации МВД России. На всех АРМ пользователей устанавливался единый пароль доступа: P@7rs36!, составленный в соответствии с Положением по организации парольной защиты в Федеральной службе по интеллектуальной собственности (уровень стойкости пароля – не ниже среднего) [10].

АРМ пользователей были развернуты на одинаковой аппаратной платформе, имеющий следующие характеристики:

- процессор (Intel Core i3-2100, 3.1 ГГц);
- оперативная память (4 ГБ DDR3);
- жесткий диск (500 ГБ SATA);
- сетевой адаптер (1 Гбит/с).

Состав ПО АРМ пользователя являлся типовым для ОВД:

- операционная система (ОС) Astra Linux 1.7 (64-разрядная);
- системное ПО – классический набор утилит для надежного функционирования ОС: systemd, udev, rsyslog, cron, bash, coreutils, util-linux, менеджер пакетов (APT) и др.;
- прикладное ПО: LibreOffice, Яндекс.Браузер, VipNet client, Kaspersky Anti-Virus и др.

Для имитации деструктивных действий злоумышленника была развернута ОС Kali Linux (x64), включающая в себя следующие инструменты:

- nmap, hping3 – для сканирования сети;
- ohydra, john – для подбора паролей;
- metasploit, msfvenom – для генерации и внедрения эксплойтов;
- burpsuite, sqlmap – для деструктивных воздействий на приложения;
- кастомные bash-скрипты – для автоматизации действий по графу;
- утилиты контроля (htop, tcpdump, iftop).

ОС злоумышленника подключалась к развернутой локальной вычислительной сети через отдельный виртуальный адаптер, обеспечивающий полный сетевой доступ к АС ОВД (за исключением использования NAT или прокси).

На втором этапе натурного эксперимента осуществлялась имитация действий злоумышленника по реализации переходов между состояниями графовой модели процесса эксплуатации текущих уязвимостей в ПО в виде последовательной смены его состояний на примере графовой модели процесса эксплуатации уязвимостей в офисном пакете LibreOffice, обобщенной для уязвимостей типа CVE-2021-25631, CVE-2023-31145 и CVE-2024-304 (рис. 1).

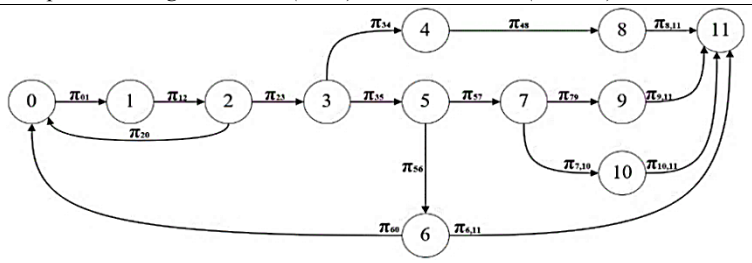

Рис. 1 - Графовая обобщенная для группы уязвимостей модель процесса эксплуатации уязвимостей типа CVE-2021-25631, CVE-2023-31145 и CVE-2024-3044 в офисном пакете LibreOffice ПО АС ОВД
Fig. 1 - A generalized graph model for the exploitation process of vulnerabilities of the CVE-2021-25631, CVE-2023-31145, and CVE-2024-3044 types in the LibreOffice office suite of the AS OVD software

0 – исходное состояние, злоумышленник в готовности к действиям, связанным с подготовкой и проведением атаки на АС ОВД;
1 – выявлено ПО в составе АС ОВД (с вероятностью π_{01});
2 – осуществлен поиск по базам данных уязвимостей ПО и выявлены (с вероятностью π_{12}) (или не выявлены (с вероятностью π_{20})) уязвимости типа CVE-2021-25631, CVE-2023-31145 и CVE-2024-3044 в ПО АС ОВД, подлежащей атаке;
3 – определен объект доступа для выполнения несанкционированного действия в ходе атаки (файл с данными или программой) и определено наличие ограничений на получение доступа к объекту (с вероятностью π_{23});
4 – выявлено отсутствие ограничений на доступ к объекту доступа и возможность использования для него штатных средств ОС (с вероятностью π_{34});
5 – выявлено наличие ограничений доступа к объекту и возможностей преодоления этих ограничений с использованием вредоносной программы, эксплойта, подбора пароля в ходе атаки и др. (с вероятностью π_{35})
6 – доступ к объекту доступа путем подбора пароля получен (с вероятностью π_{56}) (или не получен (с вероятностью π_{60}));
7 – подготовлен эксплойт для эксплуатации уязвимости или вредоносная программа для получения доступа к объекту доступа (с вероятностью π_{57});
8 – получен доступ к объекту доступа с применением штатных средств ОС и выполнения несанкционированного действия (копирования, модификации, уничтожения и др.) (с вероятностью π_{48});
9 – вредоносная программа для получения доступа к объекту доступа путем изменения учетной записи и получения привилегий доступа внедрена и запущена (с вероятностью π_{79});
10 – получен доступ к объекту доступа и запущен эксплойт для реализации несанкционированного действия (с вероятностью $\pi_{7,10}$);
11 – несанкционированное действие выполнено, угроза реализована (с вероятностями $\pi_{6,11}, \pi_{8,11}, \pi_{9,11}, \pi_{10,11}$)

Проведем подробный анализ действий злоумышленника по эксплуатации уязвимостей в ПО АС ОВД в соответствии с представленной моделью.

В исходном состоянии злоумышленник находится в полной готовности к действиям, связанным с подготовкой и осуществлением деструктивного воздействия на АС ОВД (состояние 0).

Далее производится активная разведка злоумышленником целевой ОС при помощи сканирования с целью выявления установленного ПО и сетевых сервисов. Для проведения сканирования используются встроенные инструменты ОС Kali Linux (состояние 1).

После составления полной карты состава ПО и его версий начинается этап поиска уязвимостей в версиях ПО среди уязвимостей, представленных в известных базах данных (БД) (состояние 2). Злоумышленник сопоставляет обнаруженные версии ПО с БД уязвимостей, включая национальные и международные справочники CVE.

Для поиска по БД уязвимостей в ПО АС ОВД выбран метод, основанный на автоматизированном статическом анализе программного кода – Static Application Security Testing (SAST) [11] с использованием платформы SonarQube. Данный выбор обосновывался доступностью, функциональностью, качеством проверки и возможностью внедрения

отчетов в перспективную разработку комплекса программ.

Для уточнения информации и выявления наличия (либо отсутствия) дополнительных векторов атаки злоумышленник возвращается к первоначальному этапу разведки, проводя более глубокое сканирование системы. Это может позволить ему обнаружить скрытые порты или особенности в конфигурации, которые могут быть использованы для осуществления НСД к служебной информации в АС ОВД.

После сбора информации о системе начинается этап определения целевых объектов доступа и наличия ограничений на получение доступа к ним. Злоумышленник анализирует файловую систему в поисках критически важных данных, конфиденциальной информации или системных компонентов, к которым может быть осуществлен НСД. Одновременно с этим проводится анализ существующих механизмов защиты (состояние 3).

Если проведенный анализ показывает, что ограничения на доступ к целевым объектам отсутствуют и доступ к ним может быть осуществлен с использованием штатных средств ОС (состояние 4), то злоумышленник получает такой доступ и переходит к немедленной реализации атаки (состояние 8).

Однако в большинстве случаев система защиты информации от НСД, используемая в АС ОВД, предполагает наличие определенных ограничений доступа. В такой ситуации злоумышленник сталкивается с необходимостью преодоления защитных механизмов путем подбора учетных данных, использования эксплойтов для известных уязвимостей или разработки специализированного вредоносного кода для обхода системы защиты (состояние 5).

В случае выявления ограничений доступа злоумышленник готовит соответствующие средства для их преодоления. Один из возможных путей – это подбор паролей к учетным записям с доступом к целевым объектам. С использованием специализированных инструментов и словарей проводится атака методом перебора, которая может позволить получить существующие учетные данные от системы (состояние 6).

Альтернативный подход предполагает подготовку эксплойтов или вредоносного ПО для эксплуатации выявленных в ПО уязвимостей. Злоумышленник адаптирует существующие эксплойты или разрабатывает новые вредоносные программы и подготавливает инфраструктуру для получения доступа к целевым объектам путем внедрения кода (состояние 7).

Существуют различные способы поиска эксплойтов для уязвимостей в ПО [12]: поиск эксплойтов в автономном режиме с помощью SearchSploit, использование предоставляемой компанией Packet Storm актуальной информации о новостях безопасности и уязвимостях, использование архива эксплойтов SecurityFocus, использование Online-библиотеки эксплойтов.

В связи с трудоемкостью процесса поиска эксплойтов выбран последний из рассмотренных способов поиска – в Online-библиотеке эксплойтов с использованием БД Exploit Database (ExploitDB) [13]. Exploit DB предоставляет архивную копию всего размещенного кода эксплойтов, в ОС Kali Linux архив поставляется в пакете explotdb по умолчанию. Вредоносный код может быть спроектирован для изменения учетных записей, повышения привилегий или получения постоянного доступа к системе. После успешного запуска вредоносной программы злоумышленник получает расширенные права доступа к целевым объектам (состояние 9).

Использование подготовленных средств предполагает запуск эксплойтов для эксплуатации уязвимостей в ПО в режиме реального времени. Это позволяет злоумышленнику получать прямой доступ к целевым объектам системы и выполнять запланированные несанкционированные действия без необходимости прохождения стандартных процедур аутентификации (состояние 10).

После получения различными способами доступа к целевым объектам выполняется несанкционированное действие. Данный этап может включать копирование конфиденциальных данных, их модификацию, уничтожение или любые другие несанкционированные действия с информацией в АС ОВД (состояние 11).

В табл. 1 представлены инструменты, используемые злоумышленником для реализации вредоносных функций при эксплуатации уязвимостей в исследуемом ПО в соответствии с рассматриваемой графовой моделью.

Таблица 1. Описание действий злоумышленника и инструментов для их выполнения в процессе эксплуатации уязвимостей в офисном пакете LibreOffice

Table 1. Description of the attacker's actions and tools for performing them during the exploitation of vulnerabilities in the LibreOffice office suite

№ пп	Переходы Transitions	Используемые инструменты Tools	Вредоносные функции, реализуемые злоумышленником Malicious functions implemented by the attacker
1	π_{01} **0→1**	`nmap c time`	Сканирование портов и определение сервисов на целевой ОС Astra Linux. Использовались флаги -sV -O для определения версий ПО, функционирующего под управлением ОС
2	π_{12} **1 → 2**	`stdout + stopwatch`	Автоматизированный статический анализ программного кода и выявление потенциально возможных уязвимостей высокого и критического уровня критичности в LibreOffice с использованием SAST-анализатора SonarQube
3	π_{23} **2 → 3**	`enum4linux + smbclient`	Определение сетевых ресурсов и объектов доступа. Анализ ограничений доступа к критическим файлам и директориям
4	π_{20} **2 → 0**	`nmap -p- + nikto`	Повторное расширенное сканирование всех портов и веб-сервисов для поиска скрытых векторов атаки
5	π_{34} **3 → 4**	`cat + ls -la`	Проверка доступа к целевым объектам через стандартные команды. Быстрый доступ без дополнительных привилегий
6	π_{35} **3 → 5**	`hydra + medusa`	Выявление ограничений доступа и подготовка к подбору учетных данных. Тестирование различных сервисов на уязвимости
7	π_{56} **5 → 6**	`hydra`	Подбор учетных данных для SSH/FTP сервисов (3247 попыток, 18 попыток/с)
8	π_{57} **5 → 7**	`msfvenom + time`	Поиск эксплойта для выявленной уязвимости в ExploitDB и его генерация. Быстрая подготовка payload для дальнейшего использования
9	π_{48} **4 → 8**	`scp + time`	Использование стандартных средств копирования для реализации НСД к целевым объектам
10	π_{79} **7 → 9**	`scp + crontab`	Внедрение вредоносной программы через копирование и настройка автозапуска через планировщика задач
11	$\pi_{6,11}$ **6 → 11**	`ssh + rm -rf`	Немедленное выполнение деструктивных действий через полученный легитимный доступ. Удаление критических файлов
12	π_{60} **6 → 0**	`ssh + nmap`	Повторная разведка системы с использованием полученных учетных данных для поиска новых векторов атаки
13	$\pi_{8,11}$ **8 → 11**	`find, cat + shred`	Выполнение несанкционированных действий через стандартные средства: чтение данных и их последующее уничтожение
14	$\pi_{9,11}$ **9 → 11**	`reverse shell + commands`	Использование внедренной вредоносной программы для получения привилегий и выполнения деструктивных действий
15	$\pi_{7,10}$ **7 → 10**	msfconsole + time	Запуск подготовленного эксплойта через Metasploit Framework для эксплуатации уязвимости
16	$\pi_{10,11}$ **10 → 11**	`exploit execution + commands`	Выполнение несанкционированных действий через эксплойт: повышение привилегий и уничтожение данных

На третьем этапе натурного эксперимента определялись значения временных характеристик эксплуатации уязвимостей высокого и критического уровня критичности в версиях LibreOffice с использованием встроенной в ОС Astra Linux утилиты «time», позволяющей измерять длительность выполнения команды или скрипта, а также утилиты «time», встроенной в ряд указанных в табл.1 инструментов, используемых для реализации злоумышленником вредоносных функций в соответствии с рассматриваемой графовой моделью.

С учетом того, что офисный пакет LibreOffice используется на объектах информатизации ОВД, начиная с 2020 г., для проверки эффективности рассмотренной выше методики определения значений временных характеристик эксплуатации уязвимостей в процессе функционирования ПО АС ОВД были выбраны девять версий LibreOffice, обновления которых выпущены в 2020–2024 годах.

Согласно [14, 15] достаточное для определения временных характеристик количество итераций экспериментов L определялось по формуле:

$$L = \frac{t_\varphi{}^2 \sigma^2}{\varepsilon^2}, \quad (1)$$

где: t_φ – квантиль нормального распределения вероятностей порядка $\varphi = \frac{1+Q}{2}$ (данные из таблицы Лапласа); $\sigma = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \bar{x})^2}{n-1}}$ – среднеквадратичное отклонение (x_i – i-ый элемент выборки, $\bar{x}$ – выборочное среднее, n – объем первоначальной выборки); Q – достоверность оценки (уровень доверия), ε – заданная точность решения.

Расчет L производился для достоверности $Q = 0{,}95$. По таблице Лапласа определено, что для $Q = 0{,}95$ квантиль нормального распределения вероятностей t_φ = 1,645. Установлено, что при $n = 20$ для определения временных характеристик с точностью $\varepsilon = 0{,}05$ достаточно осуществить 100 итераций экспериментов.

В табл. 2 приведены значения временных характеристик эксплуатации уязвимостей τ_{01}–$\tau_{10,11}$ для рассматриваемых версий Libre Office, рассчитанные в соответствии с описанной выше методикой. Проведенный натурный эксперимент демонстрирует реализацию реалистичного сценария процесса эксплуатации уязвимостей в офисном пакете LibreOffice ПО АС ОВД, где злоумышленник последовательно переходит от разведки к осуществлению деструктивных воздействий. В случае успешного прохождения злоумышленником всех описанных выше этапов несанкционированное действие считается выполненным, угроза безопасности информации – реализованной.

Табл. 2 показывает, что наибольшее время потребовалось злоумышленнику для осуществления переходов 1→2 (статический анализ программного кода) и 5→ 6 (подбор пароля), последнее подчеркивает важность использования сложных паролей как защитного механизма в АС ОВД. Заметна тенденция к увеличению времени τ_{12} проведения автоматизированного статического анализа программного кода с использованием SAST-анализатора SonarQube и выявления потенциально возможных уязвимостей высокого и критического уровня критичности с каждой новой версией LibreOffice.

Данный факт можно объяснить добавлением в офисный пакет различных функций, упрощающих работу в данной среде, с выпуском обновлений, что приводит к увеличению числа строк программного кода, а, значит и к возрастанию времени, затрачиваемого на сканирование используемого ПО.

Табл. 2 также позволяет проследить незначительное увеличение временных характеристик и на других этапах процесса эксплуатации уязвимости для различных версий LibreOffice. Проанализирована публикуемая в открытой печати статистика по выявлению и устранению уязвимостей в процессе функционирования ПО в АС ОВД, что дало возможность определить средние значения времен выявления и устранения уязвимости высокого и критического уровня критичности в рассматриваемом ПО.

На основе анализа представленных в [16,17] результатов исследования, проведенного за период времени с апреля 2022 года по июнь 2023 года, не противоречащих результатам анализа существующей статистики за 2022–2024 годы [6–9, 16], заданы средние значения времен выявления ($\overline{\tau_{\text{ву},n}}$) и устранения ($\overline{\tau_{\text{уу},n}}$) текущей уязвимости высокого и критического уровня критичности в процессе функционирования ПО в АС ОВД: $\overline{\tau_{\text{ву},n}}$~7,53 мин., $\overline{\tau_{\text{уу},n}}$)~77,79 мин. Значения показателей могут быть использованы в качестве исходных данных для проведения дальнейших исследований.

Таблица. 2. Результаты расчета временных характеристик эксплуатации уязвимостей в ПО
Table 2. Results of calculating the time characteristics of exploitation of vulnerabilities in software

№ пп	Версии ПО Software versions	Количество уязвимостей в ПО Number of software vulnerabilities	Количество уязвимостей высокого и критического уровня критичности Number of vulnerabilities of high and critical severity	Временные характеристики эксплуатации уязвимости в ПО τ_{ij}, с Temporal characteristics of exploitation of a vulnerability in software τij, s							
1	LO № 6.4	21	7	τ_{01}	τ_{12}	τ_{23}	τ_{20}	τ_{34}	τ_{35}	τ_{56}	τ_{57}
				105	182	96	126	38	53	205	18
				τ_{48}	τ_{79}	$\tau_{6,11}$	τ_{60}	$\tau_{8,11}$	$\tau_{9,11}$	$\tau_{7,10}$	$\tau_{10,11}$
				55	24	44	89	68	33	20	47
2	LO № 7.0	15	4	τ_{01}	τ_{12}	τ_{23}	τ_{20}	τ_{34}	τ_{35}	τ_{56}	τ_{57}
				105	190	96	126	38	54	206	18
				τ_{48}	τ_{79}	$\tau_{6,11}$	τ_{60}	$\tau_{8,11}$	$\tau_{9,11}$	$\tau_{7,10}$	$\tau_{10,11}$
				55	24	45	90	68	33	21	48
3	LO № 7.1	22	5	τ_{01}	τ_{12}	τ_{23}	τ_{20}	τ_{34}	τ_{35}	τ_{56}	τ_{57}
				105	193	96	126	39	54	207	19
				τ_{48}	τ_{79}	$\tau_{6,11}$	τ_{60}	$\tau_{8,11}$	$\tau_{9,11}$	$\tau_{7,10}$	$\tau_{10,11}$
				55	25	45	90	69	34	21	48
4	LO № 7.2	17	3	τ_{01}	τ_{12}	τ_{23}	τ_{20}	τ_{34}	τ_{35}	τ_{56}	τ_{57}
				105	195	96	127	39	55	206	18
				τ_{48}	τ_{79}	$\tau_{6,11}$	τ_{60}	$\tau_{8,11}$	$\tau_{9,11}$	$\tau_{7,10}$	$\tau_{10,11}$
				56	25	46	90	69	34	22	49
5	LO № 7.3	24	3	τ_{01}	τ_{12}	τ_{23}	τ_{20}	τ_{34}	τ_{35}	τ_{56}	τ_{57}
				105	196	96	127	38	56	207	19
				τ_{48}	τ_{79}	$\tau_{6,11}$	τ_{60}	$\tau_{8,11}$	$\tau_{9,11}$	$\tau_{7,10}$	$\tau_{10,11}$
				56	28	46	90	70	35	22	49
6	LO № 7.4	20	6	τ_{01}	τ_{12}	τ_{23}	τ_{20}	τ_{34}	τ_{35}	τ_{56}	τ_{57}
				105	198	96	127	39	57	209	19
				τ_{48}	τ_{79}	$\tau_{6,11}$	τ_{60}	$\tau_{8,11}$	$\tau_{9,11}$	$\tau_{7,10}$	$\tau_{10,11}$
				57	28	48	91	70	35	22	50
7	LO № 7.5	19	3	τ_{01}	τ_{12}	τ_{23}	τ_{20}	τ_{34}	τ_{35}	τ_{56}	τ_{57}
				105	199	96	127	39	57	209	19
				τ_{48}	τ_{79}	$\tau_{6,11}$	τ_{60}	$\tau_{8,11}$	$\tau_{9,11}$	$\tau_{7,10}$	$\tau_{10,11}$
				58	29	48	90	71	36	23	50
8	LO № 7.6	25	5	τ_{01}	τ_{12}	τ_{23}	τ_{20}	τ_{34}	τ_{35}	τ_{56}	τ_{57}
				105	201	96	127	38	58	210	18
				τ_{48}	τ_{79}	$\tau_{6,11}$	τ_{60}	$\tau_{8,11}$	$\tau_{9,11}$	$\tau_{7,10}$	$\tau_{10,11}$
				58	29	49	92	72	37	24	52
9	LO № 24.2	10	3	τ_{01}	τ_{12}	τ_{23}	τ_{20}	τ_{34}	τ_{35}	τ_{56}	τ_{57}
				105	206	96	128	39	60	212	19
				τ_{48}	τ_{79}	$\tau_{6,11}$	τ_{60}	$\tau_{8,11}$	$\tau_{9,11}$	$\tau_{7,10}$	$\tau_{10,11}$
				60	31	52	93	75	39	24	53

Вывод. Рассмотрена организация и предложена методика проведения натурного эксперимента, позволяющего выявить потенциально возможные уязвимости ПО в процессе функционирования в АС ОВД, исследовать этапы и определить значения временных характеристик их эксплуатации на основе применения SAST-анализатора SonarQube и встроенных в ПО утилит. Полученные в результате реализации методики количество потенциально возможных уязвимостей высокого и критического уровня критичности в версиях ПО (на примере версий офисного пакета LibreOffice), значения временных характеристик их эксплуатации, а также заданные средние значения времени выявления и устранения уязвимости высокого и критического уровня критичности в ПО следует использовать в качестве исходных данных при проведении точной количественной оценки комплексного

показателя защищенности программного продукта в режиме реального времени и автоматизированного выбора наиболее защищенной его версии для использования в АС ОВД.

Библиографический список:

1. ГОСТ Р 56939-2024. Защита информации. Разработка безопасного программного обеспечения. Общие требования : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 24 октября 2024 г. № 1504-ст : дата введения 2024-12-20. – Москва : Стандартинформ, 2024. – 29 с.
2. Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств:методический документ от 28 октября 2022 г. // ФСТЭК России [Электронный ресурс]. https://fstec.ru/dokumenty/vse-dokumenty/ spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g-2 (дата обращения: 20.04.2025).
3. Попова А.Д. Разработка программного комплекса анализа и оценки защищенности программного обеспечения автоматизированных систем органов внутренних дел / А. Д. Попова, И. Г. Дровникова // Вестник Воронежского института ФСИН России. – 2025. – № 1. – С. 102–109.
4. Свидетельство о государственной регистрации программы для ЭВМ № 2025662021. Российская Федерация. «Программный комплекс анализа и оценки защищенности программного обеспечения автоматизированных систем органов внутренних дел»: № 2025662021: заявл. 28.04.2025 :опубл. 16.05.2025 / А.Д. Попова, Д. В. Поддубнов, И. Г. Дровникова ; правообладатели : Попова Арина Дмитриевна, Поддубнов Данила Викторович, Дровникова Ирина Григорьевна.
5. Попова А.Д. Результаты экспериментального исследования защищенности программного обеспечения автоматизированных систем органов внутренних дел/А. Д. Попова, И. Г. Дровникова // Вестник Воронежского института МВД России. – 2025. – № 2. – С. 9–20.
6. Актуальные киберугрозы: I квартал 2024 года [Электронный ресурс]. https://www.ptsecurity.com/ ru-ru/research/analytics/cybersecurity-threatscape-2024-q1/ (дата обращения: 04.08.2024).
7. Эксплойты и уязвимости в первом квартале 2024 года // Securelist by Kaspersky [Электронный ресурс]. – URL : https://securelist.ru/vulnerability-report-q1-2024/109484/ (дата обращения: 07.05.2024).
8. Kaspersky Security Bulletin 2023/Статистика [Электр. ресурс]. URL: https:// www.itb.spb.ru/time-to-live-news/informatsionnaya-bulletin_2023_statistika/(date of application: 04.04.2024).
9. Security Week 2420: эксплуатация уязвимостей в ПО // Kaspersky_Lab [Электр.ресурс]. – URL : https://habr.com/ru/companies/kaspersky/articles/814065/ (date of application: 14.06.2025).
10. https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=633381#nbQp5sUnqmXfbuF6 (дата обращения: 12.06.2025) Об утверждении Положения по организации парольной защиты в Федеральной службе по интеллектуальной собственности : приказ Роспатента от 14.07.2015 г. № 97 // КонсультантПлюс [Электронный ресурс].
11. Static Application Security Testing (SAST) [Электронный ресурс]. – URL : https://docs.gitlab.com/ ee/user/application_security/sast/ (date of application: 06.07.2025).
12. Поиск эксплойтов для любой уязвимости [Электронный ресурс]. – URL : https://www.itsecforu.ru/2022/02/21/поиск-эксплойтов-для-любой-уязвимости/ (дата обращения: 14.12.2024).
13. URL : https://www.how-to/top-10-exploit-databases-for-finding-vulnerabilities-0189314/ (date of application: 14.09.2024). Top 10 Exploit Databases or Finding Vulnerabilities [Электронный ресурс].
14. Советов Б.Я. Моделирование систем / Б.Я. Советов, С.А. Яковлев. – 3-е издание, переработанное и дополненное. – Москва : Высшая школа, 2001. – 343 с.
15. Советов Б.Я. Моделирование систем. Практикум/ Б.Я. Советов, С.А. Яковлев. – 4-е издание, переработанное и дополненное. – Москва : Юрайт, 2014. – 295 с.
16. Как изменилась работа с уязвимостями в 2022 году // Positive technologies [Электронный ресурс]. – URL : https://www.ptsecurity.com/ru-ru/research/analytics/kak-izmenilas-rabota-s-uyazvimostyami-v-2022-godu/ (дата обращения: 16.10.2023).
17. Shift Left: красивый отчет или реальность? [Электронный ресурс] – URL : https://habr.com/ru/companies/swordfish_security/articles/747638/ (date of application: 11.06.2025).

References:

1. GOST R 56939-2024. Information Security. Development of Secure Software. General Requirements: official publication: approved and put into effect by Order of the Federal Agency for Technical Regulation and Metrology dated October 24, 2024;1504-st: effective date: December 20, 2024. Moscow: Standartinform, 2024:29 p.
2. Methodology for Assessing the Criticality of Vulnerabilities in Software and Hardware: methodological document dated October 28, 2022.FSTEC of Russia [Electronic resource]. – Available at: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g-2 (Accessed: 20.04.2025).
3. Popova, A.D. “Development of a software package for analyzing and assessing the security of software in automated systems of internal affairs agencies” A.D. Popova, I.G. Drovnikova // Bulletin of the Voronezh

Institute of the Federal Penitentiary Service of Russia. 2025:102–109.
4. Certificate of state registration of a computer program No. 2025662021. Russian Federation. "Software Package for Analysis and Assessment of Software Security of Automated Systems of Internal Affairs Bodies": No. 2025662021: declared 28.04.2025: published 16.05.2025 / A.D. Popova, D.V. Poddubnov, I.G. Drovnikova; copyright holders: Arina Dmitrievna Popova, Danila Viktorovich Poddubnov, Irina Grigoryevna Drovnikova.
5. A.D. Popova. Results of an Experimental Study of Software Security of Automated Systems of Internal Affairs Bodies. A.D. Popova, I.G. Drovnikova. *Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia*. 2025;2: 9-20.
6. Current Cyber Threats: Q1 2024 [Electronic resource]. https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2024-q1/ (date of access: 04.08.2024).
7. Exploits and Vulnerabilities in Q1 2024 // Securelist by Kaspersky [Electronic resource]. – URL: https://securelist.ru/vulnerability-report-q1-2024/109484/ (date of access: 07.05.2024).
8. Kaspersky Security Bulletin 2023/ Statistics | Securelist [Electronic resource]. – URL: https:// www.itb.spb.ru/time-to-live-news/informatsionnaya-bulletin_2023_statistika/ (date of application: 04.04.2024).
9. Security Week 2420: Exploitation of Vulnerabilities in Software // Kaspersky_Lab [Electronic resource]. – URL: https://habr.com/ru/companies/kaspersky/articles/814065/ (date of application: 14.06.2025).
10. URL: ttps://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=633381#nbQp5sUnqmXfbuF6 (date of access: 12.06.2025). On approval of the Regulation on the organization of password protection in the Federal Service for Intellectual Property: order of Rospatent dated 14.07.2015 No. 97 // ConsultantPlus [Electronic resource].
11. Static Application Security Testing (SAST) [Electronic resource]. – URL: https://docs.gitlab.com/ee/user/application_security/sast/ (date of application: 06.07.2025).
12. Search for exploits for any vulnerability [Electronic resource]. – URL: https://www.itsecforu.ru/2022/02/21/poisk-eksploytov-dlya-lyuboy-uyazvimosti/ (date of access: 14.12.2024).
13. Top 10 Exploit Databases or Finding Vulnerabilities [Electronic resource]. https://www.how-to/top-10-exploit-databases-for-finding-vulnerabilities-0189314/ (date of application: September 14, 2024).
14. Sovetov, B.Ya. System Modeling. B.Ya. Sovetov, S.A. Yakovlev. –3rd edition, revised and supplemented. Moscow: Vysshaya Shkola, 2001:343 p.
15. Sovetov, B.Ya. System Modeling. Workshop. B.Ya. Sovetov, S.A. Yakovlev. 4th edition, revised and supplemented. Moscow: Yurait, 2014:295 p.
16. How Vulnerability Management Changed in 2022 // Positive Technologies [Electronic resource]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/kak-izmenilas-rabota-s-uyazvimostyami-v-2022-godu/ (Accessed: October 16, 2023).
17. URL: https://habr.com/ru/companies/swordfish_security/articles/747638/ (Application Date: June 11, 2025). Shift Left: A Nice Report or Reality? [Electronic resource]

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

Антон Дмитриевич Попов, кандидат технических наук, доцент, доцент кафедры автоматизированных информационных систем органов внутренних дел; anton.holmes@mail.ru

Information about the 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; idrovnikova@mail.ru

Anton D. Popov, Cand. Sci. (Eng.), Assoc. Prof., Assoc. Prof., Department of Automated Information Systems of Internal Affairs Bodies; anton.holmes@mail.ru

Конфликт интересов/Conflict of interest.

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

Поступила в редакцию/Received 19.06.2025.

Одобрена после рецензирования/Reviced 12.07.2025.

Принята в печать/Accepted for publication 20.08.2025.