ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК004.056
DOI: 10.21822/2073-6185-2024-51-1-68-78 Оригинальная статья/ Original article

CC BY 4.0

Характеристика дефектов безопасности и анализ критичности уязвимостей в программном обеспечении автоматизированных систем органов внутренних дел

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

Резюме. Цель. Целью исследования является теоретический анализ дефектов безопасности и исследование критичности уязвимостей в программных средствах, используемых в современных автоматизированных системах органов внутренних дел. **Метод.** Использован метод системного подхода к рассмотрению сущности проблемы оценивания защищенности программного обеспечения автоматизированных систем органов внутренних дел и критичности его уязвимостей. **Результат.** Представлены результаты анализа теоретических аспектов исследования уязвимостей в программном обеспечении автоматизированных систем. Проанализированы компоненты типичного программного обеспечения, используемого на автоматизированном рабочем месте пользователя современной автоматизированной системы органов внутренних дел, на наличие известных уязвимостей, представленных в Национальной базе уязвимостей США и Банке данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю России, с получением базовых оценок по стандарту Common Vulnerability Scoring System версий 3.0 и 3.1. **Вывод.** Сделаны выводы об уровне критичности выявленных уязвимостей и важности их устранения путем своевременного обновления используемого программного обеспечения на основе выбора его оптимальной по уровню защищенности версии. Намечены основные направления деятельности по проведению количественной оценки уровня защищенности программного обеспечения в автоматизированных системах органов внутренних дел с учетом его уязвимостей в режиме реального времени.

Ключевые слова: автоматизированная система, программное обеспечение, уязвимость, уровень опасности уязвимости, уровень критичности уязвимости, уровень защищенности программного обеспечения, количественная оценка уровня защищенности.

Для цитирования: И.Г. Дровникова, А.Д. Попова. Характеристика дефектов безопасности и анализ критичности уязвимостей в программном обеспечении автоматизированных систем органов внутренних дел. Вестник Дагестанского государственного технического университета. Технические науки. 2024; 51(1):68-78. DOI:10.21822/2073-6185-2024-51-1-68-78

Characterization of security defects and analysis of vulnerability criticality in software for automated systems of internal affairs bodies

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 study is to theoretically analyze security defects and study the criticality of vulnerabilities in software used in modern automated systems of internal affairs agencies. **Method.** A systematic approach method was used to consider the essence of the problem of assessing the security of software of automated systems of internal affairs bodies and the criticality of its vulnerabilities. **Result.** The results of an analysis of theoretical aspects of the study of vulnerabilities in software of automated systems are presented. The components of typical software used in the automated workstation of a user of a modern automated system of internal affairs bodies were analyzed for the presence of known vulnerabilities presented in the US National

Vulnerability Database and the Data Bank of Information Security Threats of the Federal Service for Technical and Export Control of Russia, obtaining basic estimates for standard Common Vulnerability Scoring System versions 3.0 and 3.1. **Conclusion.** Carry out timely updates of the software used based on the selection of its optimal version in terms of security level. The main directions of activity for conducting a quantitative assessment of the level of software security in automated systems of internal affairs bodies are outlined, taking into account its vulnerabilities in real time.

Keywords: automated system, software, vulnerability, vulnerability danger level, vulnerability criticality level, software security level, quantitative assessment of security level

For citation: I.G. Drovnikova, A.D. Popova. Characterization of security defects and analysis of vulnerability criticality in software for automated systems of internal affairs bodies. Herald of Daghestan State Technical University. Technical Sciences. 2024; 51(1):68-78. DOI:10.21822/2073-6185-2024-51-1-68-78

Введение. Важнейшая особенность современных объектов информатизации органов внутренних дел (ОВД) заключается в хранении, обработке и передаче все возрастающих объемов и многообразия разновидностей служебной информации ограниченного распространения, что приводит к лавинообразному увеличению количества и к расширению номенклатуры угроз информационной безопасности. В первую очередь, это касается появления новых видов угроз, связанных с несанкционированным доступом к информационным ресурсам автоматизированных систем (АС) ОВД, отличающихся как несложностью исполнения, так и изощренностью воздействия, подвергающим служебную информацию, циркулирующую на объектах информатизации, нарушению конфиденциальности, целостности или доступности [1].

Постоянное совершенствование злоумышленниками способов деструктивного воздействия, используя уязвимости в программном обеспечении (ПО) АС ОВД, с целью получения доступа к служебной информации ограниченного распространения, а также необходимость быстрого и правомерного реагирования на угрозы ставит в качестве первоочередной решение задачи устранения выявленных уязвимостей и повышения уровня защищенности используемых программных средств. Это, в свою очередь, приводит к необходимости оценивания уровня защищенности ПО в АС ОВД с учетом его уязвимостей.

Для решения обозначенной задачи сформулирована триединая цель обеспечения безопасности ПО объектов информатизации ОВД:

- защита ПО от использования злоумышленниками уязвимостей с целью кражи служебной информации (нарушения конфиденциальности);
- защита ПО от использования злоумышленниками уязвимостей с целью подмены или модификации служебной информации (нарушения целостности);
- защита ПО от использования злоумышленниками уязвимостей с целью нарушения процессов обработки, хранения и передачи служебной информации (нарушения доступности).

Постановка задачи. Реализация указанной цели требует изучения дефектов безопасности и проведения общего анализа критичности уязвимостей в программных средствах, используемых на современных объектах информатизации ОВД.

Это предполагает проработку отдельных аспектов теории оценки защищенности ПО АС ОВД с учетом уязвимостей [2] и проведение анализа типичного ПО, используемого на автоматизированном рабочем месте (АРМ) пользователя современной АС ОВД, на наличие известных уязвимостей, представленных в Национальной базе уязвимостей США (National Vulnerabilities Database – NVD) [3] и банке данных угроз (БДУ) безопасности информации Федеральной службы по техническому и экспортному контролю (ФСТЭК) России [4], с получением базовых оценок по стандарту Common Vulnerability Scoring System (CVSS) [5] V.3.0 [6] и V.3.1 [7], что и является задачей исследования.

Методы исследования. Комплексный характер проблемы оценивания уровня защищенности ПО на объектах информатизации ОВД с учетом его уязвимостей [2] предполагает реализацию системного подхода к рассмотрению сущности проблемы оценивания защищенности ПО АС ОВД и критичности его уязвимостей.

Обсуждение результатов. Согласно [8] ПО – это совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ.

Под безопасным ПО понимается ПО, разработанное с использованием совокупности мер, направленных на предотвращение появления и устранение уязвимостей программы. В соответствии с [8] уязвимость программы рассматривается как ее недостаток, который может быть использован для реализации угроз безопасности информации, а в соответствии с [9] – является свойством программы, обусловливающим возможность реализации угроз безопасности обрабатываемой с ее помощью информации.

В [10] уязвимость трактуется как слабость одного или нескольких активов (то есть всего, что представляет ценность для организации), которая может использоваться одной или несколькими угрозами. В книге Ю.К. Язова, С.В. Соловьева дается определение уязвимости системного и прикладного ПО: она рассматривается как свойство ПО, предоставляющее возможность для реализации угроз безопасности информации, обрабатываемой с использованием данного ПО. При этом подчеркивается, что описание уязвимости представляет собой неотъемлемую составную часть описания угрозы безопасности информации, которая реализуется с использованием данной уязвимости. Отсутствие указания на используемую угрозой уязвимость приводит к неопределенности описания способа реализации угрозы, а, следовательно, и описания самой угрозы [11].

В настоящее время наиболее представительной по составу содержащихся сведений о существующих уязвимостях ПО является база данных CVE (Common Vulnerabilities and Exposures) [12], которая входит в состав NVD [3] и считается единым стандартом идентификации уязвимостей. Для проведения анализа уязвимостей из CVE, их классификации, определения необходимых характеристик и получения численных оценок наиболее широкое применение получил стандарт CVSS, содержащий три группы метрик в виде набора целых чисел 0, 1, …, 10 и векторов с кратким текстовым описанием с используемыми для вывода оценки значениями [5, 13]: базовые метрики (отображают не изменяющиеся со временем и не зависящие от окружения характеристики уязвимости,); временные метрики (отображают изменяющиеся со временем характеристики уязвимости); контекстные метрики (отражают связанные со средой использования характеристики уязвимости). Временные и контекстные метрики не являются обязательными и не влияют на базовую оценку, а служат для ее уточнения.

Востребованным отечественным каталогом уязвимостей ПО служит база данных уязвимостей, входящая в состав БДУ безопасности информации ФСТЭК России [4].

Находящиеся в открытом доступе стандарты CVE и CVSS вместе с БДУ ФСТЭК России могут быть использованы для получения предварительной информации об уязвимостях ПО АС ОВД. В [14] рассматривается понятие степени опасности уязвимости информационной системы, в соответствии с которым можно ввести понятие уровня опасности уязвимости ПО АС как меры (сравнительной величины), которая характеризует подверженность ПО уязвимости, а также влияние данной уязвимости на нарушение свойств безопасности информации, обрабатываемой в АС с использованием данного ПО (нарушение ее конфиденциальности, целостности и доступности).

Согласно [15] уровень критичности уязвимости ПО АС следует рассматривать как показатель, характеризующий уровень опасности уязвимости и ее влияние на функционирование АС, использующей данное ПО. По сути критичность уязвимости ПО – это совокупность ее основных технических характеристик, некая числовая оценка, позволяющая определить серьезность данной уязвимости в сравнении с другими [2]. Необходимость оценивания уровня критичности уязвимостей ПО связана с принятием операторами АС обоснован-

ного решения о необходимости устранения выявленных уязвимостей, основываясь на результатах их анализа [15]. В соответствии с [14] уязвимости в ПО классифицируются следующим образом по месту (источнику) их возникновения:

1) уязвимости в общесистемном ПО:

− уязвимости операционных систем (ОС) (файловых систем, режимов загрузки, связанные с наличием средств разработки и отладки ПО, механизмов управления процессами и др.);

− уязвимости систем управления базами данных (СУБД) (серверной и клиентской частей СУБД, специального инструментария, исполняемых объектов баз данных (хранимые процедуры, триггеры) и др.);

− уязвимости иных типов общесистемного ПО;

2) уязвимости в прикладном ПО – уязвимости офисных пакетов программ и иных типов прикладного ПО (наличие средств разработки мобильного кода, недостатки механизмов контроля исполнения мобильного кода, ошибки программирования, наличие функциональных возможностей, способных оказать влияние на средства защиты информации и др.);

3) уязвимости в специальном ПО – уязвимости ПО, разработанного для решения специфических задач конкретной АС (ошибки программирования, наличие функциональных возможностей, способных оказать влияние на средства защиты информации, недостатки механизмов разграничения доступа к объектам специального ПО и др.).

В [16] описан состав типичного ПО, используемого на АРМ пользователя современной АС ОВД. Рассмотрим каждый из компонентов описанного ПО на наличие известных уязвимостей, представленных в NVD [3] и БДУ безопасности информации ФСТЭК России [4]:

1) BIOS материнской платы версии UEFI. Для рассматриваемой версии BIOS не выявлено опубликованной информации о наличии каких-либо неустраненных уязвимостей;

2) ОС Astra Linux. В представленной ОС выявлено значительное количество уязвимостей, информация об устранении которых отсутствует. Выделим отдельные из последних таких уязвимостей [4] (табл.1).

Таблица 1. Уязвимости ОС Astra Linux
Table 1. Astra Linux OS vulnerabilities

№ пп	Идентификатор Identifier	Краткое описание Brief Description	Базовая оценка CVSS V.3.0 Base Rating	Уровень опасности Danger level
1	BDU:2023-00001	Уязвимость ядра операционной системы Linux, позволяющая нарушителю получить базовый адрес Kernel ASLR и получить доступ к памяти ядра/ Operating system kernel vulnerability	6,5	средний average
2	BDU:2023-00352	BDU:2023-00352. Уязвимость функции scsi_ioctl (drivers/scsi/scsi_ioctl.c) ядра операционной системы Linux, позволяющая нарушителю повысить свои привилегии/ Vulnerability of the scsi_ioctl function (drivers/scsi/scsi_ioctl.c) of the operating system kernel	5,9	средний average
3	BDU:2023-01277	Уязвимость функции setup_async_work() (fs/ksmbd/smb2pdu.c) подсистеме SMB ядра операционной системы Linux, позволяющая нарушителю вызвать отказ в обслуживании/ Vulnerability of the setup_async_work() function (fs/ksmbd/smb2pdu.c) in the SMB subsystem of the Linux operating system kernel	6,5	средний average
4	BDU:2023-01801	Уязвимость функции hci_conn_hash_flush() в модуле net/bluetooth/hci_conn.c операционной системы Linux, позволяющая нарушителю повысить свои привилегии/ Vulnerability of the hci_conn_hash_flush() function in the net/bluetooth/hci_conn.c module of the Linux	7,8	высокий high

№ пп	Идентификатор Identifier	Краткое описание Brief Description	Базовая оценка CVSS V.3.0 Base Rating	Уровень опасности Danger level
		operating system,		
5	BDU:2023-02516	Уязвимость функции mtd_div_by_eb() в модуле include/linux/mtd/mtd.h ядра операционной системы Linux, позволяющая нарушителю вызвать отказ в обслуживании или, возможно, оказать иное воздействие/ Vulnerability of the mtd_div_by_eb() function in the include/linux/mtd/mtd.h module of the Linux operating system kernel	5,5	средний average
6	BDU:2023-03165	Уязвимость реализации сетевого протокола безопасности MACsec ядра операционной системы Linux, позволяющая нарушителю получить доступ к защищаемой информации или нарушить целостность данных/ Vulnerability in the implementation of the MACsec network security protocol in the Linux operating system kernel,	8,0	высокий high
7	BDU:2023-03435	Уязвимость функции ravb_remove() в модуле drivers/net/ethernet/renesas/ ravb_main. с драйвера сетевых устройств Renesas ядра операционной системы Linux в функции ravb_remove(), позволяющая нарушителю оказать воздействие на конфиденциальность, целостность и доступность защищаемой информации/ Vulnerability of the ravb_remove() function in the drivers/net/ethernet/renesas/ravb_main module. from the Renesas network device driver of the Linux operating system kernel in the ravb_remove() function,	7,6	высокий high

3) драйвера чипсета, звуковой карты и др. [3]:

– CVE-2022-42455. Уязвимость драйвера ASUS EC Tool (он же d.sys) 1beb15c90dcf7a5234ed077833a0a3e900969b60be1d04fcebce0a9f8994bdbb, подписанного ASUS и поставляемого с несколькими программными продуктами ASUS, содержащего несколько обработчиков IOCTL, которые обеспечивают необработанный доступ к портам ввода-вывода и MSRS для чтения и записи через непривилегированные вызовы IOCTL. Локальные пользователи могут получать привилегии (базовая оценка CVSS V.3.1 составляет 7,8; высокий уровень опасности);

4) набор прикладных программ:

а) пакет офисных программ LibreOffice. Содержит множество выявленных уязвимостей, последние из которых представлены в табл. 2 [3].

Таблица 2. Уязвимости пакета программ LibreOffice
Table 2. Vulnerabilities of the LibreOffice software package

№ пп	Идентификатор Identifier	Краткое описание Brief Description	Базовая оценка CVSS V.3.0 Base Rating	Уровень опасности Danger level
1	CVE-2023-0950	Уязвимость индекса массива в компоненте электронных таблиц Document Foundation LibreOffice, позволяющая злоумышленнику создать документ электронной таблицы, который при загрузке приводит к недостаточному заполнению индекса массива, вызывая риск выполнения произвольного кода/ Array index vulnerability in Document Foundation LibreOffice spreadsheet component	7,8	**высокий high**
2	CVE-2023-1183	Уязвимость пакета LibreOffice, позволяющая	5,5	средний

№ пп	Идентификатор Identifier	Краткое описание Brief Description	Базовая оценка CVSS V.3.0 Base Rating	Уровень опасности Danger level
		злоумышленнику создать odb, содержащий файл «база данных/сценарий», с помощью команды SCRIPT, в которой содержимое файла может быть записано в новый файл, местоположение которого определено злоумышленником/ A vulnerability in LibreOffice that allows an attacker to create an odb containing a database/script file		average
3	CVE-2023-2255	Уязвимость реализации неправильного контроля доступа в компонентах редактора Document Foundation LibreOffice, позволяющая злоумышленнику создать документ, приводящий к загрузке внешних ссылок без запроса разрешения пользователя/ Improper access control implementation vulnerability in Document Foundation LibreOffice editor components	5,3	средний average
4	CVE-2023-26435	Уязвимость позволяет вызывать ссылки на файловую систему и сеть, используя локальный экземпляр LibreOffice и обработанные документы ODT, что позволяет злоумышленнику обнаружить топологию сети и службы с ограниченным доступом, а также включить локальные файлы с правами на чтение пользователя системы open-xchange/ The vulnerability allows you to call links to the file system and network using a local instance	5,0	средний average
5	CVE-2023-31145	Отраженная уязвимость XSS с полным обходом политики безопасности контента в установках Nextcloud с использованием для совместной работы онлайн-офисного пакета Collabora Online, основанного на технологии LibreOffice. Позволяет злоумышленнику выполнить тривиальную атаку на захват учетной записи, что может привести к несанкционированному доступу к конфиденциальной информации и данным, а также к возможности совершать действия от имени пользователя/ Reflected XSS vulnerability with full content security policy bypass in Nextcloud installations using Collabora Online online office collaboration suite	6,1	средний average

б) браузер Mozila Firefox. Не выявлено опубликованной информации о наличии каких-либо неустраненных уязвимостей;

в) Adobe Acrobat Reader. Выделим некоторые из последних выявленных уязвимостей [3] (табл. 3).

Таблица 3. Уязвимости программы Adobe Acrobat Reader
Table 3. Adobe Acrobat Reader vulnerabilities

№ пп	Идентификатор Identifier	Краткое описание Brief Description	Базовая оценка CVSS V.3.0 Base Rating	Уровень опасности Danger level
1	CVE-2023-29299	Уязвимость ненадежного пути поиска, которая может привести к отказу в обслуживании приложения (подвержен Adobe Acrobat Reader версий 23.003.20244 и более ранних, 20.005.30467 и более ранних). Злоумышленник может воспользоваться этой уязвимостью, если для параметра	4,7	средний average

№ пп	Идентификатор Identifier	Краткое описание Brief Description	Базовая оценка CVSS V.3.0 Base Rating	Уровень опасности Danger level
		PowerShell Set-ExecutionPolicy по умолчанию установлено значение Unrestricted, что повышает сложность атаки. Для решения проблемы и открытия вредоносного файла необходимо взаимодействие с пользователем/ An untrusted search path vulnerability that could lead to an application denial of service (affected by Adobe Acrobat Reader versions 23.003.20244 and earlier, 20.005.30467 and earlier).		
2	CVE-2023-29303	Уязвимость Use After Free, которая может привести к раскрытию конфиденциальной памяти (подвержен Adobe Acrobat Reader версий 23.003.20244 и более ранних, 20.005.30467 и более ранних). Злоумышленник может использовать эту уязвимость для обхода средств защиты, таких как ASLR. Для решения проблемы и открытия вредоносного файла необходимо взаимодействие с пользователем/ Use After Free vulnerability that can lead to disclosure of confidential memory (affected by Adobe Acrobat Reader versions 23.003.20244 and earlier, 20.005.30467 and earlier).	5,5	средний average
3	CVE-2023-29320	Уязвимость, связанная с нарушением принципов безопасного проектирования, которая может привести к выполнению произвольного кода в контексте текущего пользователя в обход функции внесения в черный список API (подвержен Adobe Acrobat Reader версий 23.003.20244 и более ранних, 20.005.30467 и более ранних). Для решения проблемы и открытия вредоносного файла необходимо взаимодействие с пользователем/ Secure Design Vulnerability	7,8	высокий high
4	CVE-2023-38226	Уязвимость доступа по неинициализированному указателю, которая может привести к выполнению произвольного кода в контексте текущего пользователя (подвержен Adobe Acrobat Reader версий 23.003.20244 и более ранних, 20.005.30467 и более ранних). Для решения проблемы и открытия вредоносного файла необходимо взаимодействие с пользователем/ Uninitialized pointer access vulnerability	7,8	высокий
5	CVE-2023-38228	Уязвимость «Использовать бесплатно», которая может привести к выполнению произвольного кода в контексте текущего пользователя (подвержен Adobe Acrobat Reader версий 23.003.20244 и более ранних, 20.005.30467 и более ранних). Для решения проблемы и открытия вредоносного файла необходимо взаимодействие с пользователем/ Free to use vulnerability that could lead to arbitrary code execution in the context of the current user	7,8	высокий high
6	CVE-2023-38230	Уязвимость «После использования», которая может привести к раскрытию конфиденциальной памяти (подвержен Adobe Acrobat Reader версий 23.003.20244 и более ранних, 20.005.30467 и более ранних). Злоумышленник может использовать эту уязвимость для обхода средств защиты, таких как ASLR. Для решения	5,5	средний average

№ пп	Идентификатор Identifier	Краткое описание Brief Description	Базовая оценка CVSS V.3.0 Base Rating	Уровень опасности Danger level
		проблемы и открытия вредоносного файла необходимо взаимодействие с пользователем/ After Exploit vulnerability that could lead to sensitive memory disclosure (affected by Adobe Acrobat Reader versions 23.003.20244 and earlier, 20.005.30467 and earlier)		
7	CVE-2023-38232	Уязвимость для чтения за пределами доступа, которая может привести к раскрытию конфиденциальной памяти (подвержен Adobe Acrobat Reader версий 23.003.20244 и более ранних, 20.005.30467 и более ранних). Злоумышленник может использовать эту уязвимость для обхода средств защиты, таких как ASLR. Для решения проблемы и открытия вредоносного файла необходимо взаимодействие с пользователем/ Out-of-bounds read vulnerability that could lead to sensitive memory disclosure	5,5	средний average
8	CVE-2023-38233	Уязвимость записи за пределы допустимых значений, которая может привести к выполнению произвольного кода в контексте текущего пользователя (подвержен Adobe Acrobat Reader версий 23.003.20244 и более ранних, 20.005.30467 и более ранних). Для решения проблемы и открытия вредоносного файла необходимо взаимодействие с пользователем/ An out-of-bounds write vulnerability that could lead to arbitrary code execution in the context of the current user	7,8	высокий high

г) Qpdfview. Не выявлено опубликованной информации о наличии каких-либо неустраненных уязвимостей;

д) VipNet. К последним уязвимостям, информация об устранении которых отсутствует, относятся уязвимости, представленные в табл.4 [4].

Таблица 4. Уязвимости VipNet
Table 4. VipNet vulnerabilities

№ пп	Идентификатор Identifier	Краткое описание Brief Description	Базовая оценка CVSS V.3.0 Base Rating	Уровень опасности Danger level
1	BDU:2022-03008	Уязвимость функционала проверки файлов обновлений программно-аппаратного комплекса защиты информации ViPNet Client, позволяющая нарушителю установить вредоносное программное обеспечение/ Vulnerability in the functionality for checking update files of the ViPNet Client information security software and hardware system	8,8	высокий high
2	BDU:2022-03009	Уязвимость программно-аппаратного комплекса защиты информации ViPNet Client, позволяющая нарушителю выполнить произвольный код путем возможности подмены динамической библиотеки/ Vulnerability of the ViPNet Client information security software and hardware system,	7,8	высокий high

е) Криптопро [3]:

– CVE-2022-34301**. Уязвимость** в загрузчиках защищенных дисков CryptoPro, выпущенных до 2022-06-01. Злоумышленник может использовать этот загрузчик для обхода

или вмешательства в систему безопасной загрузки. Чтобы загрузить и выполнить произвольный код на этапе предварительной загрузки, злоумышленнику необходимо заменить существующий подписанный загрузчик, используемый в данный момент, этим загрузчиком. Для загрузки с внешнего носителя требуется доступ к системному разделу EFI (базовая оценка CVSS V.3.1 составляет 6,7; средний уровень опасности);

ж) антивирус «Kaspersky» [3]:

– CVE-2022-27534**.** Уязвимость в модуле анализа данных антивирусных продуктов Касперского для дома и Kaspersky Endpoint Security с антивирусными базами, выпущенных до 12 марта 2022 года, которая потенциально позволяла злоумышленнику выполнять произвольный код (базовая оценка CVSS V.3.1 составляет 9,8; **критический** уровень опасности).

Зная значения оценок уровня опасности уязвимостей компонентов ПО АС ОВД могут быть определены оценки уровня их критичности. В соответствии с [15] уровень критичности (V) уязвимости ПО в АС рассчитывается по формуле:

$$V = I_{cvss} \times I_{infr}, \quad (1)$$

где: I_{cvss} – показатель уровня опасности уязвимости (находится путем расчета базовых, временных и контекстных метрик по методике CVSS V.3.0 или V.3.1 [6, 7] применительно к конкретной АС с использованием калькулятора [17, 18] и определяется совокупностью показателей этих метрик);

I_{infr} – показатель, характеризующий влияние уязвимости ПО на процесс функционирования АС, использующей это ПО. Рассчитывается для конкретной АС в соответствии с таблицей, приведенной в [15], по формуле:

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

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

L – показатель, описывающий число уязвимых компонентов ПО;

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

k, l, p – весовые коэффициенты рассматриваемых показателей.

Проведенный анализ типичного ПО, используемого на АРМ пользователя современной АС ОВД, на наличие известных уязвимостей, представленных в NVD и БДУ безопасности информации ФСТЭК Росси, с получением базовых оценок CVSS V.3.0 [6, 17] и CVSS V.3.1 [7, 18] показал, что основные компоненты рассматриваемого ПО подвержены значительному числу неустраненных уязвимостей с высоким и даже критическим уровнем опасности. Это может привести к получению оценок «высокий» и «критический» при определении уровня критичности рассматриваемых уязвимостей ПО в случае проведения расчетов применительно к конкретной АС ОВД.

Наиболее эффективным способом устранения таких уязвимостей является своевременное обновление ПО, используемого на объектах информатизации ОВД. При промедлении в обновлении ПО может стать доступным значительное число уязвимостей с высоким и критическим уровнем критичности. В этом случае требуется быстрое их устранение путем принятия соответствующих организационных (компенсирующих) мер (в течение 24 часов – для уязвимостей, имеющий критический уровень критичности; в течение 7 дней – для уязвимостей, имеющих высокий уровень критичности) [15] по причине непрерывного выявления новых уязвимостей в компонентах используемого ПО АС ОВД. Выбор компенсирующих мер по защите информации осуществляет оператор системы, учитывая как архитектуру и особенности функционирования АС ОВД, так и способы эксплуатации уязвимостей в используемом ПО. Реализация своевременного обновления ПО, используемого на объектах информатизации ОВД, должна осуществляться на основе выбора его безопасной, наиболее защищенной (оптимальной по уровню защищенности) версии, что приводит к необходимости проведения количественной оценки уровня защищенности ПО в АС ОВД с учетом его

уязвимостей в режиме реального времени.

Вывод. Комплексность проблемы оценивания уровня защищенности ПО в АС ОВД с учетом его уязвимостей предполагает реализацию системного подхода. Это требует проведения более детального анализа ряда аспектов, связанных с оценкой уровня критичности уязвимостей и возможности их эксплуатации в используемых программных средствах, что определяет следующие основные направления деятельности:

- системное рассмотрение сущности проблемы оценивания защищенности ПО АС ОВД и критичности его уязвимостей;
- разработка системы показателей уровня защищенности ПО АС ОВД, учитывающих фактор времени;
- системное использование методов моделирования исследуемых процессов расчета показателей уровня защищенности ПО АС ОВД;
- разработка методики количественной оценки уровня защищенности ПО АС ОВД, основанной на анализе критичности его уязвимостей в режиме реального времени;
- разработка и верификация программного комплекса анализа и оценки уровня защищенности ПО АС ОВД с учетом уязвимостей;
- разработка предложений по использованию разработанных методики и программного комплекса при проведении оценки уровня защищенности ПО и оптимизации его версионного выбора для объектов информатизации ОВД.

Библиографический список:

1. Ефимов А. О. Меры защиты планшетных компьютеров, осуществляющих обработку конфиденциальной информации, от несанкционированного доступа / А.О. Ефимов, Т. В. Мещерякова, Е. А. Рогозин // Вестник Воронежского института МВД России. – 2023. – № 2. – С. 31–38.
2. 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.
3. National Vulnerability Database. Nist [Электронный ресурс]. – Режим доступа : https://nvd.nist.gov/ (дата обращения: 29.01.2024).
4. Банк данных угроз безопасности информации. Уязвимости // ФСТЭК России [Электронный ресурс]. – Режим доступа : https://bdu.fstec.ru/vul (дата обращения: 30.01.2024).
5. Common Vulnerability Scoring System (CVSS-SIG) [Электронный ресурс]. – Режим доступа : https://www.first.org/cvss (дата обращения: 12.02.2024).
6. Common Vulnerability Scoring System version 3.0. Specification Document. Revision 0 [Электронный ресурс]. – Режим доступа : https://cvss-v3-specification_r0.pdf (дата обращения: 12.02.2024).
7. Common Vulnerability Scoring System version 3.1. Specification Document. Revision 1 [Электронный ресурс]. – Режим доступа : https://cvss-v31-specification_r1.pdf (дата обращения: 12.02.2024).
8. ГОСТ Р 56939-2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования. – Москва : Стандартинформ, 2016. – 24 с.
9. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Москва : Стандартинформ, 2008. – 15 с.
10. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. – Москва : Стандартинформ, 2007. – 33 с.
11. Язов Ю. К. Защита информации в информационных системах от несанкционированного доступа : учебное пособие / Ю. К. Язов, С. В. Соловьев. – Воронеж : Кварта, 2015. – 440 с.
12. Common Vulnerabilities and Exposures (CVE) [Электронный ресурс]. – Режим доступа : https://en.wikichip.org/wiki/cve (дата обращения: 12.02.2024).
13. Полное руководство по общему стандарту оценки уязвимостей версии 2. Вычисление оценки [Электронный ресурс]. – Режим доступа : https://www.securitylab.ru/ analytics/356476.php (дата обращения: 30.01.2024).
14. ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. – Москва : Стандартинформ, 2015. – 12 с.
15. 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: 29.01.2024).

16. 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.
17. БДУ-CVSS v3 Calculator [Электронный ресурс]. – Режим доступа : https://bdu.fstec.ru/calc3 (дата обращения: 12.02.2024).
18. БДУ-CVSS v31 Calculator [Электронный ресурс]. – Режим доступа : https://bdu.fstec.ru/calc31 (дата обращения: 12.02.2024).

References

1. Efimov A. O. Measures to protect tablet computers processing confidential information from unauthorized access /A.O. Efimov, T. V. Meshcheryakova, E. A. Rogozin. *Bulletin of the Voronezh Institute Ministry of Internal Affairs of Russia*. 2023; 2:31–38.
2. Efimov A. O. Conceptual basis for assessing the level of security of automated systems based on their vulnerability / A. O. Efimov, I. Livshits,T. V. Meshcheryakova, E. A. Rogozin. *Information technology security = IT Security.* 2023; 30(2): 63–79.
3. National Vulnerability Database. Nist [El. res.]. Access mode: https://nvd.nist.gov/ (date of access: 01/29/2024).
4. Data bank of information security threats. Vulnerabilities // FSTEC of Russia [Electronic resource]. – Access mode: https://bdu.fstec.ru/vul (date of access: 01/30/2024).
5. Common Vulnerability Scoring System (CVSS-SIG) [Electronic resource]. – Access mode: https://www.first.org/cvss (access date: 02/12/2024).
6. Common Vulnerability Scoring System version 3.0. Specification Document.Revision 0 [Electronic resource]. – Access mode: https://cvss-v3-specification_r0.pdf (access date: 02/12/2024).
7. Common Vulnerability Scoring System version 3.1. Specification Document.Revision 1 [Electronic resource]. – Access mode: https://cvss-v31-specification_r1.pdf (access date: 02.12.2024).
8. GOST R 56939-2016. Data protection. Secure software development. General requirements. – Moscow: Standardinform, 2016; 24.
9. GOST R 50922-2006. Data protection. Basic terms and definitions. Moscow: Standartinform, 2008; 15.
10. GOST R ISO/IEC 13335-1-2006. Information technology. Methods and means of ensuring security. Part 1. Concept and models of security management of information and telecommunication technologies. – Moscow: Standartinform, 2007; 33.
11. Yazov Yu. K. Protection of information in information systems from unauthorized access: textbook / Yu. K. Yazov, S. V. Solovyov. Voronezh: Kvarta, 2015; 440 .
12. Common Vulnerabilities and Exposures (CVE) [Electronic resource]. – Access mode: https://en.wikichip.org/wiki/cve (access date: 02.12.2024).
13. A Complete Guide to the Common Vulnerability Assessment Standard Version 2. Calculating the Score [El. resource]. – Access mode: https://www.securitylab.ru/analytics/356476.php (access date: 01/30/2024).
14. GOST R 56546-2015. Data protection. Vulnerabilities of information systems. Classification of information system vulnerabilities. – Moscow: Standartinform, 2015;12 .
15. 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: 01/29/2024).
16. 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 Cand. of Technical Sci. / Elena Sergeevna Zolotykh. – Voronezh, 2022; 220.
17. BDU-CVSS v3 Calculator [El.res.]. Access mode: https://bdu.fstec.ru/calc3 (date of access: 02.12.2024).
18. BDU-CVSS v31 Calculator [El.res.]. Access mode: https://bdu.fstec.ru/calc31 (date of access: 02.12.2024).

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 29.12.2023.

Одобрена после рецензирования/ Reviced 21.01.2024.

Принята в печать/ Accepted for publication 21.01.2024.