Для цитирования: *Ю.М. Баркалов, И.Г. Дровникова, А.М. Каднова, Е.С. Овчинникова, Е.А. Рогозин. Анализ архитектуры и особенностей функционирования автоматизированных систем органов внутренних дел в защищенном исполнении. Вестник Дагестанского государственного технического университета. Технические науки. 2020; 47(2): 40-51. DOI:10.21822/2073-6185-2020-47-2-40-51*
For citation: *Yu. M. Barkalov, I. G. Drovnikova, A. M. Kadnova, E. S. Ovchinnikova, E. A. Rogozin. Analysis of the architecture and functions of protected automated systems installed at internal affairs facilities. Herald of Daghestan State Technical University. Technical Sciences. 2020; 47 (2): 40-51. (In Russ.) DOI:10.21822/2073-6185-2020-47-2-40-51*

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ
COMPUTER SCIENCE, COMPUTER ENGINEERING AND MANAGEMENT

УДК 004.056
DOI: 10.21822/2073-6185-2020-47-2-40-51

АНАЛИЗ АРХИТЕКТУРЫ И ОСОБЕННОСТЕЙ ФУНКЦИОНИРОВАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Ю.М. Баркалов, И.Г. Дровникова, А.М. Каднова, Е.С. Овчинникова, Е.А. Рогозин
Воронежский институт Министерства внутренних дел России,
394065, г. Воронеж, пр. Патриотов,53, Россия

Резюме. Цель. *Одной из ключевых задач теории и практики защиты информации является анализ процесса функционирования защищенных автоматизированных систем при их эксплуатации на объектах информатизации органов внутренних дел. С целью идентификации потенциальных угроз конфиденциальному информационному ресурсу и их источников, оценки опасности реализации угроз и формирования на этой основе перечня актуальных угроз и их модели для конкретной автоматизированной системы на объекте информатизации органа внутренних дел необходимо проанализировать состав и архитектуру автоматизированных систем, выявить ключевые особенности их функционирования в защищенном исполнении на объектах информатизации органов внутренних дел, определить уязвимости программно-аппаратного обеспечения систем.* ***Метод.*** *Методом решения данной задачи является всесторонний анализ процесса функционирования защищенных автоматизированных систем при их эксплуатации на объектах информатизации органов внутренних дел.* ***Результат.*** *На основе анализа нормативно-методической и научной литературы, посвященной защите информации в автоматизированных системах, ведомственной документации МВД России, регламентирующей требования по защите информации на объектах информатизации органов внутренних дел, определены типовые структура и архитектура защищенной автоматизированной системы органов внутренних дел, выявлены потенциальные каналы реализации угроз, имеющих определяющее значение для ее функционирования, — сетевых атак. По результатам опроса экспертов в области обеспечения информационной безопасности проведены анализ, классификация и систематизация уязвимостей компонентов и программного обеспечения автоматизированной системы на объекте информатизации органов внутренних дел с точки зрения реализации сетевых атак.* ***Вывод.*** *Результаты проведенного исследования могут быть использованы в процессе проектирования и эксплуатации средств и систем информационной безопасности на объектах информатизации ОВД в целях повышения их защищенности.*

Ключевые слова: *автоматизированная система, уязвимость, угроза, несанкционированный доступ, сетевая атака, защита информации*

ANALYSIS OF THE ARCHITECTURE AND FUNCTIONS OF PROTECTED AUTOMATED SYSTEMS INSTALLED AT INTERNAL AFFAIRS FACILITIES

Yu. M. Barkalov, I.G. Drovnikova, A.M. Kadnova, E.S. Ovchinnikova, E.A. Rogozin
Voronezh Institute of the Ministry of Internal Affairs of Russia,
53 Patriotov St., Voronezh 394065, Russia

Abstract: Aim. *One of the key objectives of the theory and practice of information security is to analyse the functioning of protected automated systems, particularly those operated at computerized facilities of internal affairs bodies. In order to identify potential threats to resources of confidential information, to assess the risk of threat implementation, as well as to form a list of potential threats to automated systems installed at computerized facilities of internal affairs bodies, it is necessary to analyse the composition and architecture of automated systems, identify the features of their protected functioning and determine the vulnerability of software and hardware systems.* ***Methods.*** *A comprehensive analysis of the functioning of protected automated systems during their operation at computerized facilities of internal affairs bodies was conducted.* ***Results.*** *Following an analysis of normative documentation and research publications in the field of protecting information in automated systems, departmental records of the Ministry of Internal Affairs of the Russian Federation, regulations for the protection of information at computerized facilities of internal affairs bodies, the structure and architecture of a protected automated system were defined. Potential threats to the functioning of such a system, including cyber attacks, were identified. On the basis of a survey among experts in the field of information security, the vulnerability (in term of cyber attacks) of the software components of an automated system installed at computerized facilities of internal affairs bodies was analysed.* ***Conclusion.*** *The results can be used in the process of designing and operating information security tools and systems installed at computerized facilities of internal affairs bodies for the purpose of improving their security.*

Keywords: *automated system, vulnerability, threat, unauthorized access, cyber attack, information protection*

Введение. Для повышения производительности и оперативности выполняемых работ в сфере информационных технологий (ИТ) на объектах информатизации органов внутренних дел (ОВД) в настоящее время функционируют автоматизированные системы (АС) ОВД — системы, состоящие из персонала и комплекса средств автоматизации его деятельности, реализующие ИТ выполнения установленных функций [1]. АС ОВД представляют собой сложные по структуре системы критического применения, выход из строя которых ведет к значительным информационным и финансовым потерям [2-4]. Функционирование данных систем осуществляется с учетом решения множества актуальных задач по обеспечению их информационной безопасности (ИБ), сводящихся к трем основным группам: предотвращение и пресечение нарушений целостности, предотвращение и пресечение нарушений доступности, предотвращение и пресечение нарушений конфиденциальности информации в АС ОВД [5-7].

Необходимость решения указанных задач связана с обнаружением внештатных ситуаций в режиме функционирования АС ОВД в защищенном исполнении, причинами которых могут быть ошибки, возникающие в процессе проектирования, эксплуатации, администрирования, в случаях сбоях технических и программных средств, в связи с нарушением режима доступа на объект информатизации ОВД, при недостаточной квалификации пользователей - сотрудников различных подразделений [8]. Это приводит к увеличению вероятности нарушения ИБ АС ОВД, что способствует облегчению получения злоумышленниками информации конфиденциального характера. Поэтому исследования в данной области приобретают чрезвычайную важность и актуальность для объектов информатизации ОВД.

Постановка задачи. В процессе эксплуатации современных АС ОВД существенное внимание уделяется, как защите от преднамеренного воздействия на информацию штатных пользо-

вателей, так и защите технологической информации, от которой в полной мере зависит устойчивое функционирование прикладного программного обеспечения (ПО) или самой системы по ее прямому функциональному назначению (обработка, хранение и передача конфиденциальной информации) [9].

Нарушения целостности, доступности и конфиденциальности информации в АС ОВД возникают в результате реализации угроз безопасности информации, под которыми в [5, 10] понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность утечки, хищения, утраты, уничтожения, искажения, модификации, подделки, копирования, блокирования информации и несанкционированного доступа (НСД) к ней.

В приказе МВД России от 14.03.2012 № 169 «Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года» среди основных направлений ее обеспечения указываются: разработка новых и совершенствование существующих способов, методов и средств выявления, оценки, прогнозирования, нейтрализации и ликвидации угроз безопасности информации на объектах информатизации ОВД; проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки. Излагаемый в Концепции комплекс организационно-технических мероприятий, направленных на обеспечение ИБ ОВД, включает в себя разработку модели угроз информационно-телекоммуникационных систем ОВД [5].

Таким образом, анализ состава и архитектуры АС ОВД, выделение ключевых особенностей их функционирования в защищенном исполнении, выявление уязвимостей программно-аппаратного обеспечения, идентификация возможных угроз информационному ресурсу и их источников, оценивание опасности реализации угроз позволят сформировать перечень актуальных угроз и разработать их модель для данной АС ОВД [11-13].

Указанные этапы, в полной мере согласующиеся с требованиями системного подхода к анализу угроз безопасности информации в АС, изложенными в [9, 14, 15], позволят не только выявить основные направления ЗИ в АС ОВД, повысить обоснованность принятия решений по защите информации (ЗИ), но и раскрыть дальнейшие перспективы формализации и оперативного управления процессами ЗИ, разработки АС поддержки принятия решений по ЗИ на объектах информатизации ОВД и т.д.

Методы исследования. Типовая структура защищенной АС ОВД в виде сложной иерархической разветвленной информационно-телекоммуникационной сети представлена на рис. 1 [16, 17].

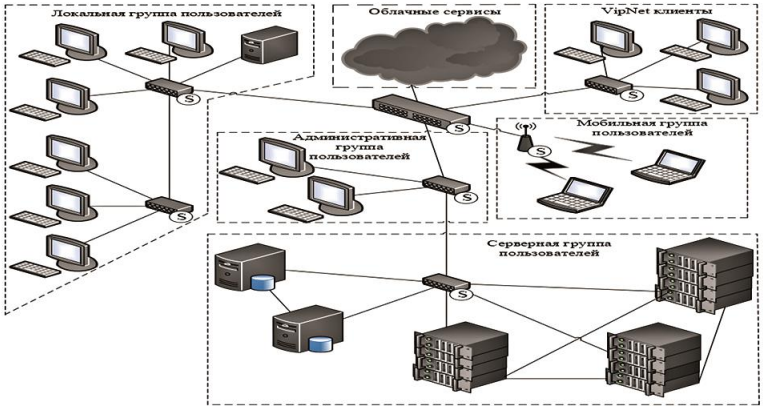

Рис.1.Типовая структура защищенной АС ОВД
Fig. 1 Typical structure of a protected ATS AS

Одной из важнейших характеристик АС ОВД, как и любой информационно-телекоммуникационной системы, является базовая сетевая технология, лежащая в основе ее построения, совокупность (стек) протоколов межсетевого взаимодействия, структура сети, состав и размещение коммуникационных элементов.

Функционирование большинства защищенных АС ОВД осуществляется с учетом исполь-

зования в них технологии межсетевого взаимодействия, реализованной в Internet, и четырехуровневого стека протоколов TCP/IP, популярность которого для АС ОВД обусловлена рядом его свойств [18].

В то же время открытость и масштабируемость TCP/IP порождает его плохую управляемость. Основным недостатком протокола является его недостаточная защищенность от подделки и прослушивания пакетов, что делает возможной реализацию злоумышленниками деструктивных действий в отношении АС на объектах информатизации ОВД.

Соответствие уровней стека протоколов TCP/IP уровням модели OSI (семиуровневой эталонной коммуникационной модели «Взаимодействие открытых систем» (Open System Interconnection), в России в соответствии с ГОСТ Р ИСО/МЭК 7498-1-99 [19] ее называют ЭМВОС («Эталонная модель взаимодействия открытых систем») с распределением некоторых основных протоколов межсетевого взаимодействия по уровням показано на рис.2.

Процесс функционирования защищенных АС ОВД основан, как правило, на использовании клиент-серверной архитектуры взаимодействия, построенного по технологии «Тонкий клиент» в сети Ethernet.

Проведенный теоретический анализ [17, 20, 21] позволил определить ключевые особенности функционирования АС ОВД в защищенном исполнении, которые представлены в [8]. Из всего комплекса угроз безопасности информации по способу их реализации в АС ОВД особо выделяются угрозы, связанные с НСД, под которым согласно [22] следует понимать доступ к служебной информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или АС.

<table>
<tr><td>7
6</td><td>WWW, Gopher, WAIS</td><td>SNMP</td><td>FTP</td><td>Telnet</td><td>TFTP</td><td>SMTP</td><td>I–прикладной applied</td></tr>
<tr><td>5
4</td><td colspan="3">TCP</td><td colspan="3">UDP</td><td>II –транспортный transport</td></tr>
<tr><td>3</td><td>IP</td><td>ICMP</td><td>RIP</td><td colspan="2">OSPF</td><td>ARP</td><td>III-сетевой network</td></tr>
<tr><td>2
1</td><td colspan="6">не регламентируется: Ethernet, Gigabit Ethernet, Token Ring, PPP, FDDI, X.25, SLIP, frame relay ...</td><td>IV-канальный channel</td></tr>
<tr><td>Уровни модели OSI
OSI Model Layers</td><td colspan="6">Протоколы Protocols</td><td>Уровни стека TCP/IP
stack levels</td></tr>
</table>

Рис. 2. Соответствие уровней стека протоколов TCP/IP и модели OSI
Fig. 2. Correspondence between the layers of the TCP / IP protocol stack and the OSI model

При рассмотрении вопроса функционирования АС ОВД в защищенном исполнении определяющее значение имеют информационные угрозы НСД, которые реализуются через удаленное взаимодействие с объектом воздействия (сетевые атаки) [9, 15, 18].

Согласно [18] под сетевой (удаленной) атакой на АС ОВД будем понимать действие или совокупность действий, направленных на реализацию угрозы удаленного (с использованием протоколов сетевого взаимодействия) доступа к технологической информации или информации пользователя в компьютерной сети.

Причины успеха сетевых атак кроются в наличии уязвимостей АС ОВД, под которыми в [10] понимаются свойства АС, обусловливающие возможность реализации угроз безопасности обрабатываемой в ней информации, то есть некие характеристики системы, делающие возможным существование данных атак. Поэтому создание таксономии уязвимостей представляется весьма важной задачей, решение которой позволит выработать принципы построения

защищенного взаимодействия в АС на объектах информатизации ОВД.

Обсуждение результатов. На рис. 3 приведены типовая аппаратура и потенциальные каналы реализации сетевых атак в АС на объекте информатизации ОВД, построенные на основе анализа открытой научно-технической литературы по проблеме ИБ АС ОВД [8, 16, 17, 23, 24].

В соответствии с рис. 3 в табл.1 представлены результаты анализа, классификации и систематизации уязвимостей компонентов и ПО АС на объектах информатизации ОВД с точки зрения реализации сетевых атак, полученные по итогам опроса экспертов в области обеспечения ИБ.

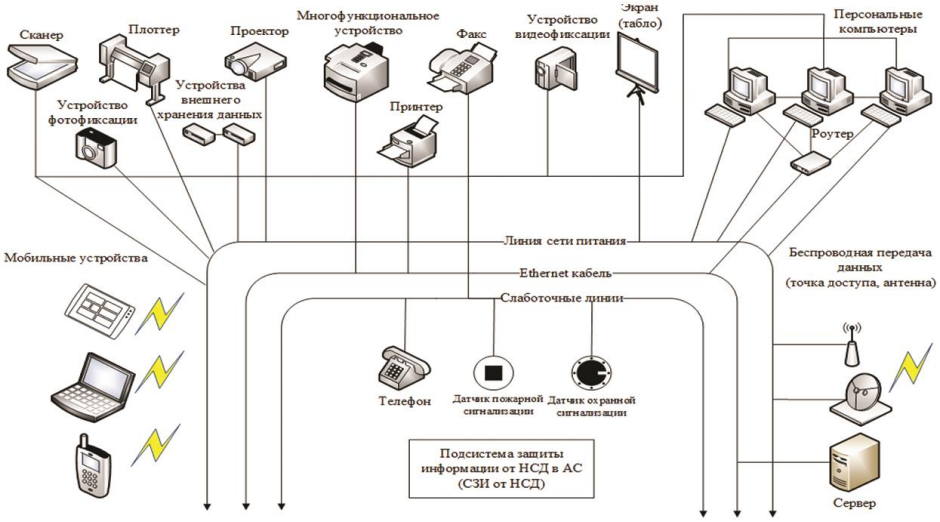

Рис.3.Типовая аппаратура и потенциальные каналы реализации сетевых атак в АС ОВД
Fig. 3. Typical equipment and potential channels for implementing network attacks in the ATS AS

Таблица 1. Звенья АС на объекте информатизации ОВД и соответствующие им уязвимости
Table 1. NPP links at the ATS informatization facility and the corresponding vulnerabilities

№ п/п	Звенья АС ОВД ATS links	Вид уязвимост Vulnerability type	Способ реализации уязвимости Method of vulnerability implementation
1	Мобильные Устройства Mobile devices	1. Получение удаленного управления над устройством. 2. Перехват передаваемой информации. 3. Блокирование работы. 4. Получение обрабатываемой информации. 5. Сокрытие обрабатываемой и передаваемой информации от легитимного пользователя 1. Getting remote control over the device. 2. Interception of transmitted information. 3. Blocking work. 4. Getting processed information. 5. Concealment of processed and transmitted information from a legitimate user	1. Заражение мобильного устройства вредоносным ПО. 2. Получение физического доступа к устройству. 3. Перехват передаваемой информации по беспроводным линиям связи 1. Infection of a mobile device with malware. 2. Obtaining physical access to the device. 3. Interception of transmitted information over wireless communication lines
2	Сканер Scanner	1. Незаконное копирование информации пользователем. 2. Перехват передаваемой информации от устройства сканирования до устройства хранения 1. Illegal copying of information by the user. 2. Interception of transmitted information from scanning device to storage device	1. Создание нелегитимных копий пользователем или злоумышленником. 2. Незаконное подключение к линиям передачи информации от устройства сканирования до устройства хранения 1 Creation of illegitimate copies by a user or an attacker. 2. Illegal connection to information transmission lines from the scanning device to the storage device
3	Устройство фотофиксации Device photofixation	1. Незаконное изготовление изображений пользователем. 2. Перехват передаваемой информации от устройства фотофиксации до устройства хранения. 3. Незаконное получение информации из памяти устройства фотофиксации 1. Illegal production of images by the user. 2. Interception of transmitted information from a photofixation device to a storage device. 3. Illegal obtaining of information from the memory of a photographic device	1. Создание нелегитимных изображений пользователем или злоумышленником. 2. Незаконное подключение к линиям передачи информации от устройства фотофиксации до устройства хранения. 3. Получение физического доступа к устройству фотофиксации 1. Creation of illegitimate images by a user or an attacker. 2. Illegal connection to information transmission lines from a photofixation device to a storage device. 3. Obtaining physical access to the photofixation device

№ п/п	Звенья АС ОВД ATS links	Вид уязвимост Vulnerability type	Способ реализации уязвимости Method of vulnerability implementation
4	ПлоттерPlotter	1. Незаконное использование плоттера для создания нелегитимных копий пользователем. 2. Незаконное копирование выводимой плоттером информации. 3. Перехват передаваемой информации от устройства обработки и хранения до плоттера 1. Illegal use of a plotter to create illegitimate copies by the user. 2. Illegal copying of information output by the plotter. 3. Interception of transmitted information from the processing and storage device to the plotter	1. Создание нелегитимных копий пользователем. 2. Получение физического доступа к устройству. 3. Незаконное подключение к линиям передачи информации от устройства обработки и хранения до плоттера. 1. Creation of illegitimate copies by the user. 2. Obtaining physical access to the device. 3. Illegal connection to information transmission lines from the processing and storage device to the plotter.
5	Устройства внешнего хранения данных External storage devices	1. Перехват передаваемой информации от устройств обработки и хранения до устройств внешнего хранения данных 2. Кража устройств внешнего хранения данных или используемых в них машинных носителей информации. 3. Незаконное копирование информации, хранимой на устройствах внешнего хранения данных 1. Interception of transmitted information from processing and storage devices to external data storage devices 2. Theft of external storage devices or the machine media used in them. 3. Illegal copying of information stored on external storage devices	1. Незаконное подключение к линиям передачи информации от устройств обработки и хранения до устройств внешнего хранения данных с целью перехвата передаваемой информации. 2. Получение физического доступа к устройству. 3. Незаконное непосредственное подключение к устройствам внешнего хранения данных. 4. Незаконное подключение к устройствам внешнего хранения данных через линии передачи информации 1. Illegal connection to information transmission lines from processing and storage devices to external data storage devices in order to intercept transmitted information. 2. Obtaining physical access to the device. 3. Illegal direct connection to external storage devices. 4. Illegal connection to external data storage devices through data transmission lines
6	Проектор Projector	1. Незаконное получение визуальной информации, проецируемой на экран. 2. Незаконный перехват информации за счет утечек по каналам побочных электромагнитных излучений и наводок (ПЭМИН) (кабель передачи данных от устройства генерации сигнала до проектора) 1. Illegal receipt of visual information projected on the screen. 2. Illegal interception of information due to leaks through the channels of incidental electromagnetic radiation and interference (PEMIN) (data transmission cable from the signal generating device to the projector)	1. Проникновение в помещение, где установлен проектор. 2. Установка аппаратной закладки для получения аудио- и визуальной информации в помещении, где установлен проектор. 3. Получение удалённого визуального доступа в помещение, где установлен проектор. 4. Размещение оборудования для получения ПЭМИН в зоне, обеспечивающей получение данной информации 1. Penetration into the room where the projector is installed. 2. Installation of a hardware bookmark for receiving audio and visual information in the room where the projector is installed. 3. Obtaining remote visual access to the room where the projector is installed. 4. Placement of equipment for receiving PEMIN in the area providing this information
7	Многофункциональное устройство Multifunction device	1. Незаконное копирование информации пользователем. 2. Перехват передаваемой информации от устройства сканирования до устройства хранения. 3. Незаконное использование многофункционального устройства для создания нелегитимных копий пользователем. 4. Незаконное копирование выводимой многофункциональным устройством информации. 5. Перехват передаваемой информации от устройства обработки и хранения до многофункционального устройства 1. Illegal copying of information by the user. 2. Interception of transmitted information from the scanning device to the storage device. 3. Illegal use of a multifunctional device to create illegitimate copies by the user. 4. Illegal copying of information displayed by a multifunctional device. 5. Interception of transmitted information from a processing and storage device to a multifunctional device	1. Создание нелегитимных копий пользователем или злоумышленником. 2. Незаконное подключение к линиям передачи информации от устройства сканирования до устройства хранения. 3. Создание нелегитимных копий пользователем. 4. Получение физического доступа к устройству. 5. Незаконное подключение к линиям передачи информации от устройства обработки и хранения до многофункционального устройства 1. Creation of illegitimate copies by a user or an attacker. 2. Illegal connection to data transmission lines from the scanning device to the storage device. 3. Creation of illegitimate copies by the user. 4. Obtaining physical access to the device. 5. Illegal connection to information transmission lines from a processing and storage device to a multifunctional device
8	Принтер Printer	1. Незаконное использование принтера для создания нелегитимных копий пользователем. 2. Незаконное копирование выводимой принтером информации. 3. Перехват передаваемой информации от устройства обработки и хранения до принтера 1. Illegal use of the printer to create illegitimate copies by the user. 2. Illegal copying of information output by the printer.	1. Создание нелегитимных копий пользователем. 2. Получение физического доступа к устройству. 3. Незаконное подключение к линиям передачи информации от устройства обработки и хранения до принтера. 1. Creation of illegitimate copies by the user. 2. Obtaining physical access to the device. 3. Illegal connection to information transmission lines from the processing and storage device to the printer

№ п/п	Звенья АС ОВД ATS links	Вид уязвимост Vulnerability type	Способ реализации уязвимости Method of vulnerability implementation
		3. Interception of transmitted information from the processing and storage device to the printer	
9	Факс Fax	1. Незаконное копирование информации пользователем. 2. Перехват передаваемой факсимильной информации 1. Illegal copying of information by the user. 2. Interception of transmitted facsimile information	1. Копирование передаваемой информации (принятые или отправляемые факсимильные сообщения) пользователем. 2. Получение физического доступа к устройству. 3. Незаконное подключение к телефонным линиям передачи информации от факсимильного устройства 1. Copying of transmitted information (received or sent fax messages) by the user. 2. Obtaining physical access to the device. 3. Illegal connection to telephone lines of information transmission from a facsimile device
10	Устройство видеофиксации Device video recording	1. Незаконное изготовление видеизображений пользователем. 2. Перехват передаваемой информации от устройства видеофиксации до устройства хранения. 3. Незаконное получение информации из памяти устройства видеофиксации 1. Illegal production of video images by the user. 2. Interception of transmitted information from a video recording device to a storage device. 3. Illegal obtaining of information from the memory of the video recording device	1. Создание нелегитимных видеоизображений пользователем или злоумышленником. 2. Незаконное подключение к линиям передачи информации от устройства сканирования до устройства хранения. 3. Получение физического доступа к устройству 1. Creation of illegitimate video images by a user or an intruder. 2. Illegal connection to data transmission lines from the scanning device to the storage device. 3. Getting physical access to the device
11	Экран (табло) Screen scoreboard	1. Незаконное получение визуальной информации, проецируемой на экран. 2. Незаконный перехват информации за счёт утечек по каналам ПЭМИН (кабель передачи данных от устройства генерации сигнала до экрана). 1. Illegal receipt of visual information projected on the screen. 2. Illegal interception of information due to leaks through PEMIN channels (data transmission cable from the signal generating device to the screen)	1. Проникновение в помещение, где установлен проектор. 2. Установка аппаратной закладки для получения аудио и визуальной информации в помещении, где установлен проектор. 3. Получение удалённого визуального доступа в помещение, где установлен проектор. 4. Размещение оборудования для получения ПЭМИН в зоне, обеспечивающей получение данной информации 1. Penetration into the room where the projector is installed. 2. Installation of a hardware bookmark for receiving audio and visual information in the room where the projector is installed. 3. Obtaining remote visual access to the room where the projector is installed. 4. Placement of equipment for receiving PEMIN in the area providing this information
12	Персональные компьютеры Personal computers	1. Незаконное получение удаленного управления над персональным компьютером. 2. Перехват передаваемой информации. 3. Блокирование работы. 4. Незаконное получение обрабатываемой информации. 5. Незаконное получение хранимой информации. 6. Сокрытие обрабатываемой и передаваемой информации от легитимного пользователя. 7. Незаконная модификация информации. 8. Незаконный перехват информации за счет утечек по каналам ПЭМИН (кабель передачи данных от устройства генерации сигнала до проектора). 9. Работа от имени легитимного пользователя. 10. Уничтожение машинного носителя информации1. Illegal obtaining of remote control over a personal computer. 2. Interception of transmitted information. 3. Blocking work. 4. Illegal receipt of processed information. 5. Illegal receipt of stored information. 6. Concealment of processed and transmitted information from a legitimate user. 7. Illegal modification of information. 8. Illegal interception of information due to leaks through PEMIN channels (data transmission cable from the signal generating device to the projector). 9. Work on behalf of a legitimate user. 10. Destruction of machine information carrier	1. Заражение персонального компьютера вредоносным ПО. 2. Получение физического доступа к устройству. 3. Перехват передаваемой информации по каналам связи. 4. Нелегитимная установка и применение пользователем ПО, не являющегося вредоносным, но позволяющим осуществлять действия по модификации информации (шифрование, удаление), сбору и передаче информации или удалённому управлению. 5. Подключение внешних устройств с целью незаконного копирования информации пользователем или злоумышленником. 6. Размещение оборудования для получения ПЭМИН в зоне, обеспечивающей получение данной информации. 7. Физическое или механическое воздействие на машинный носитель информации. 8. Кража персонального компьютера или носителя информации. 1. Infection of a personal computer with malware. 2. Obtaining physical access to the device. 3. Interception of transmitted information through communication channels. 4. Illegal installation and use by the user of software that is not malicious, but allows actions to modify information (encryption, deletion), collect and transfer information or remote control. 5. Connection of external devices for the purpose of illegal copying of information by a user or an intruder. 6. Placement of equipment for receiving PEMIN in the area providing this information. 7. Physical or mechanical impact on the machine data carrier. 8. Theft of a personal computer or data carrier
13	Роутер Router	1. Подключение к роутеру. 2. Блокирование роутера. 3. Перехват информации, передаваемой через	1. Подбор учетных данных (логин, пароль) к роутеру. 2. Заражение роутера вредоносным ПО. 3. Использование программных или программно-

№ п/п	Звенья АС ОВД ATS links	Вид уязвимост Vulnerability type	Способ реализации уязвимости Method of vulnerability implementation
		роутер 1. Connecting to a router. 2. Blocking the router. 3. Interception of information transmitted through the router	аппаратных устройств для перехвата и анализа трафика (снифферов), подключённых к линям передачи информации роутера. 4. Физический доступ к устройству 1. Selection of credentials (login, password) for the router. 2. Infection of the router with malware. 3. The use of software or hardware-software devices for intercepting and analyzing traffic (sniffers) connected to the router's information transmission lines. 4. Physical access to the device
14	Беспроводная передача данных (точка доступа, антенна) Wireless data transmission (access point, antenna)	1. Беспроводная передача данных на фиксированных частотах по стандартным алгоритмам. 2. Отсутствие или слабое шифрование передаваемых пакетов 1. Wireless transmission of data at fixed frequencies using standard algorithms. 2. Absence or weak encryption of transmitted packets	1. Перехват передаваемых пакетов. 2. Дешифрация передаваемых пакетов 1. Interception of transmitted packets. 2. Decryption of transmitted packets
15	Сервер Server	1. Незаконное получение удаленного управления над сервером. 2. Перехват передаваемой информации. 3. Блокирование работы. 4. Незаконное получение обрабатываемой информации. 5. Незаконное получение хранимой информации. 6. Сокрытие обрабатываемой и передаваемой информации от легитимного пользователя. 7. Незаконная модификация информации. 8. Незаконный перехват информации за счёт утечек по каналам ПЭМИН (кабель передачи данных от устройства генерации сигнала до проектора). 9. Работа от имени легитимного пользователя. 10. Уничтожение машинного носителя информации 1. Illegal obtaining of remote control over the server. 2. Interception of transmitted information. 3. Blocking work. 4. Illegal receipt of processed information. 5. Illegal receipt of stored information. 6. Concealment of processed and transmitted information from a legitimate user. 7. Illegal modification of information. 8. Illegal interception of information due to leaks through PEMIN channels (data transmission cable from the signal generating device to the projector). 9. Work on behalf of a legitimate user. 10. Destruction of machine information carrier	1. Заражение сервера вредоносным программным обеспечением. 2. Получение физического доступа к устройству. 3. Перехват передаваемой информации по каналам связи. 4. Нелегитимная установка и применение пользователем ПО, не являющегося вредоносным, но позволяющим осуществлять действия по модификации информации (шифрование, удаление), сбору и передаче информации или удалённому управлению. 5. Подключение внешних устройств с целью незаконного копирования информации пользователем или злоумышленником. 6. Размещение оборудования для получения ПЭМИН в зоне, обеспечивающей получение данной информации. 7. Физическое или механическое воздействие на машинный носитель информации. 8. Кража сервера или носителей информации 1. Server infection with malicious software. 2. Obtaining physical access to the device. 3. Interception of transmitted information through communication channels. 4. Illegal installation and use by the user of software that is not malicious, but allows actions to modify information (encryption, deletion), collect and transfer information or remote control. 5. Connection of external devices for the purpose of illegal copying of information by a user or an intruder. 6. Placement of equipment for receiving PEMIN in the area providing this information. 7. Physical or mechanical impact on the machine data carrier. 8. Theft of the server or media
16	Телефон Telephone	1. Незаконное получение речевой информации 1. Illegal receipt of speech information	1. Незаконное подключение к каналам связи. 2. Установка аппаратной закладки для получения речевой информации 1. Illegal connection to communication channels. 2. Installation of a hardware bookmark for receiving speech information
17	Датчик пожарной сигнализации Fire alarm sensor	1. Линяя передачи информации за счёт утечек по каналам ПЭМИН. 2. Может использоваться в качестве маскирующего устройства при установке в нём камеры или микрофона либо усилителя радиосигналов. 1. Linear information transmission due to leaks through PEMIN channels. 2. Can be used as a masking device when installing a camera or microphone or amplifier of radio signals in it	1. Размещение оборудования для получения ПЭМИН в зоне, обеспечивающей получение данной информации, или непосредственное подключение к линям обслуживания датчика. 2. Физический доступ. 3. Установка в датчик камеры или микрофона при производстве устройства или после его установки. 4. Установка в датчик усилителя радиосигналов при производстве устройства. 1. Placement of equipment for receiving PEMIN in the area providing this information, or direct connection to the sensor service lines. 2. Physical access. 3. Installation of a camera or microphone in the sensor during the manufacture of the device or after its installation.

№ п/п	Звенья АС ОВД ATS links	Вид уязвимост Vulnerability type	Способ реализации уязвимости Method of vulnerability implementation
			4. Installation of an amplifier of radio signals in the sensor during the manufacture of the device
18	Датчик охранной сигнализа-ции Security sensor alarms	1. Линяя передачи информации за счёт утечек по каналам ПЭМИН. 2. Может использоваться в качестве маскирующе-го устройства при установке в нём камеры или микрофона 1. Linear information transmission due to leaks through PEMIN channels. 2. Can be used as a masking device when installing a camera or microphone in it	1. Размещение оборудования для получения ПЭМИН в зоне, обеспечивающей получение данной информации, или непосредственное подключение к линям обслужива-ния датчика. 2. Физический доступ. 3. Установка в датчик камеры или микрофона при произ-водстве устройства или после его установки. 4. Установка в датчик усилителя радиосигналов при про-изводстве устройства. 1. Placement of equipment for receiving PEMIN in the area providing this information, or direct connection to the sensor service lines. 2. Physical access. 3. Installation of a camera or microphone in the sensor during the manufacture of the device or after its installation. 4. Installation of an amplifier of radio signals in the sensor during the manufacture of the device
19	Линия сети питания Power line	1. Линяя передачи информации за счёт утечек по каналам ПЭМИН. 2. Подключение устройств для незаконного пере-хвата информации 1. Linear information transmission due to leaks through PEMIN channels. 2. Connecting devices for illegal interception of in-formation	1. Размещение оборудования для получения ПЭМИН в зоне, обеспечивающей получение данной информации, или непосредственное подключение к линиям сети пита-ния. 2. Физический доступ. 1. Placement of equipment for receiving PEMIN in the area providing this information, or direct connection to power lines. 2. Physical access
20	Ethernet кабель Ethernet cable	1. Линяя передачи информации за счет утечек по каналам ПЭМИН. 2. Подключение устройств для незаконного пере-хвата информации 1. Shedding information transmission due to leaks through PEMIN channels. 2. Connecting devices for illegal interception of in-formation	1. Размещение оборудования для получения ПЭМИН в зоне, обеспечивающей получение данной информации, или непосредственное подключение к Ethernet кабелю. 2. Физический доступ. 1. Placement of equipment for receiving PEMIN in the area providing this information, or direct connection to an Ethernet cable. 2. Physical access
21	Слаботоч-ные линии Low current lines	1. Линяя передачи информации за счёт утечек по каналам ПЭМИН. 2. Подключение устройств для незаконного пере-хвата информации 1. Linear information transmission due to leaks through PEMIN channels. 2. Connecting devices for illegal interception of in-formation	1. Размещение оборудования для получения ПЭМИН в зоне, обеспечивающей получение данной информации или непосредственное подключение к слаботочным линиям. 2. Физический доступ. 1. Placement of equipment for receiving PEMIN in the area providing the receipt of this information or direct connection to low-current lines. 2. Physical access
22	Подсистема ЗИ от НСД в АС (СЗИ от НСД) Sub-system of IS from NSD in AS (IS from NSD)	1. ПО СЗИ от НСД. 2. Недостаточное качество функционирования СЗИ от НСД. 3. Использование неактуальной версии СЗИ от НСД. 4. Ошибки при проектировании. 5. Отсутствие актуального документа, связанного с обязательной сертификацией СЗИ от НСД. 1. ON SZI from NSD. 2. Insufficient quality (efficiency and reliability) of the functioning of the information security system from the NSD. 3. Use of an outdated version of the information secu-rity system from the NSD (from the point of view of the relevance of network attacks). 4. Errors in design. 5. Lack of an up-to-date document related to the man-datory certification of the information security system from the NSD	1. Сетевая атака на программный код СЗИ от НСД. 2. Ошибки персонала и операторов. 3. Несанкционированное изменение конфигурации СЗИ от НСД. 4. Несанкционированное изменение алгоритмов функцио-нирования СЗИ от НСД. 1. Network attack on the ISS program code from the NSD. 2. Errors of personnel and operators. 3. Unauthorized change in the configuration of the information security system from the NSD. 4. Unauthorized change of the algorithms for the functioning of the information security system from the NSD

Вывод. На основе анализа методической документации и отраслевых стандартов ФСТЭК России, посвященных ЗИ в АС, ведомственной документации МВД России, регламентирующей требования по ЗИ на объектах информатизации ОВД, открытой научно-технической литературы в области обеспечения ИБ в статье разработана типовая структура защищенной АС ОВД и определены ключевые особенности ее функционирования с точки зрения обеспечения ИБ.

Выявлены потенциальные каналы реализации сетевых атак к конфиденциальному информационному ресурсу, определены уязвимости звеньев АС и возможные способы их реализации на объектах информатизации ОВД.

Результаты проведенного исследования могут быть использованы в процессе проектирования и эксплуатации средств и систем ИБ на объектах информатизации ОВД в целях повышения их защищенности.

Библиографический список:

1. ГОСТ 34.003-90. Автоматизированные системы. Термины и определения [Электронный ресурс]. — URL:http://docs.cntd.ru/document/ 1200006979 (дата обращения: 24.10.2019).

2. Maximizing Uptime of Critical Systems in Commercial and Industrial Applications VAVR-8K4TVA_R1_EN.pdf [Электронный ресурс]. — URL:https://download.schneider-eletric.com/files?p_Doc_Ref=SPD_VAVR-8K4TVA_EN (дата обращения: 24.10.2019).

3. Butusov I.V. Methodology of Security Assessment Automated Systems as Objects Critical Information Infrastructure / I.V. Butusov, A.A. Romanov [Электронный ресурс]. — URL:fcyberrus.com/wp-content/uploads/ 2018/05/02-10-125-18_1.-Butusov.pd (дата обращения: 28.10.2019).

4. Xin Z. Research on effectiveness evaluation of the mission-critical system / Z. Xin, M. Shaojie, Z. Fang // Proceedings of 2013 2nd International Conference on Measurement, Information and Control. 2013. P. 869-873.

5. Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года: приказ МВД России от 14.03.2012 № 169 [Электронный ресурс]. — URL:http://policemagazine.ru/forum/showthread.php?t=3663 (дата обращения: 21.10.2019).

6. Security Trends & Vulnerabilities Review Corporate Information Systems // Positive Technologies 2017 [Электронный ресурс]. — URL: https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Corp-Vulnerabilities-2017-eng.pdf (дата обращения: 09.11.2019).

7. Bagayoko D. Understanding the Relativistic Generalization of Density Functional Theory (DFT) and Completing It in Practice / D. Bagayoko // Journal of Information Security. Vol. 7 № 9, May 2016 [Электронный ресурс]. — URL:https://www.scirp.org/journal/paperinformation.aspx?paperid=66781 (дата обращения: 02.11.2019).

8. Методы и средства оценки защищённости автоматизированных систем органов внутренних дел: монография [Электронный ресурс] / И.Г. Дровникова [и др.]. Воронеж: Воронеж. ин-т МВД России, 2017. 88 с.

9. Язов Ю.К. Защита информации в информационных системах от несанкционированного доступа: пособие / Ю.К. Язов, С.В. Соловьёв. Воронеж: Кварта, 2015. 440 с.

10. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения // СПС «КонсультантПлюс»

11. Kresimir S. The information systems' security level assessment model based on an ontology and evidential reasoning approach / S. Kresimir, O. Hrvoje, G. Marin // Computers & Security. — 2015. — P. 100-112.

12. Method to Evaluate Software Protection Based on Attack Modeling / H. Wang [et ol.] // 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing Year. 2013. PP. 837-844.

13. Effectiveness Evaluation on Cyberspace Security Defense System / L. Yun [et ol.] // International Conference on Network and Information Systems for Computers (IEEE Conference Publications). 2015. PP. 576-579.

14. ФСТЭК России. Методический документ. Методика определения угроз безопасности информации в информационных системах [Электронный ресурс]. — URL:http://https://fstec.ru/component/attachments/ download/812 (дата обращения: 21.10.2019).

15. Язов Ю.К. Организация защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. — Воронеж: Кварта, 2018. — 588 с.

16. Рогозин Е.А. Проектирование систем защиты информации от несанкционированного доступа в автоматизированных системах ОВД / Е.А. Рогозин, А.Д. Попов, Т.В. Шагиров // Вестник Воронеж. ин-та МВД России. 2016. № 2. С. 174-183.

17. 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: дис. ... канд. техн. наук: 05.13.19 / Попов Антон Дмитриевич. — Воронеж, 2018. — 163 с.

18. Радько Н.М. Проникновения в операционную среду компьютера: модели злоумышленного удаленного доступа: учеб. пособие / Н.М. Радько, Ю.К. Язов, Н.Н. Корнеева. — Воронеж: Воронеж. госуд. технич. ун-т, 2013. — 265 с.

19. ГОСТ Р ИСО/МЭК 7498-1-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель [Электронный ресурс]. — URL:https://files.stroyinf.ru/ Data2/1/4294818/4294818276.pdf (дата обращения: 04.11.2019).

20. ГОСТ Р 51583-2014. Порядок создания автоматизированных систем в защищенном исполнении [Электронный ресурс]. — URL: http://docs.cntd.ru/document/ 1200108858 (дата обращения: 04.11.2019).

21. Рогозин Е.А. Классификация угроз информационной безопасности в автоматизированных информационных системах / Е.А. Рогозин, А.Д. Попов, Д.И. Коробкин // Приборы и системы. Управление, контроль, диагностика. 2017. № 7. С. 22-26.

22. Руководящий документ Государственной технической комиссии от 30 июня 1992 года. Защита от несанкционированного доступа к информации. Термины и определения. [Электронный ресурс]. — URL: https://fstec.ru/component/attachments/download/298 (дата обращения: 05.11.2019).

23. Рогозин Е.А. Основные этапы и задачи разработки систем защиты информации ОВД в автоматизированных системах / Е.А. Рогозин, Е.Ю. Никулина, А.Д. Попов // Вестник Воронеж. ин-та ФСИН России. 2016. № 4. С. 94-98.

24. Система показателей качества функционирования при создании системы информационной безопасности на объ-

екте информатизации ОВД / А.М. Каднова [и др.] // Приборы и системы, управление, контроль, диагностика. 2019. № 1. С. 26-33.

References:

1. GOST 34.003-90. Avtomatizirovannyye sistemy. Terminy i opredeleniya [Elektronnyy resurs]. — URL:http://docs.cntd.ru/document/ 1200006979 (data obrashcheniya: 24.10.2019). [GOST 34.003-90. Automated systems. Terms and definitions [Electronic resource]. - URL: http: //docs.cntd.ru/document/ 1200006979 (date of access: 24.10.2019). (In Russ)]

2. Maximizing Uptime of Critical Systems in Commercial and Industrial Applications VAVR-8K4TVA_R1_EN.pdf [Electronic resource]. - URL: https: //download.schneider-eletric.com/files? P_Doc_Ref = SPD_VAVR-8K4TVA_EN (date accessed: 24.10.2019).

3. Butusov I.V. Methodology of Security Assessment Automated Systems as Objects Critical Information Infrastructure / I.V. Butusov, A.A. Romanov [Electronic resource]. - URL: fcyberrus.com/wp-content/uploads/ 2018/05 / 02-10-125-18_1.-Butusov.pd (date accessed: 28.10.2019).

4. Xin Z. Research on effectiveness evaluation of the mission-critical system / Z. Xin, M. Shaojie, Z. Fang // Proceedings of 2013 2nd International Conference on Measurement, Information and Control. 2013. P. 869-873.

5. Ob utverzhdenii Kontseptsii obespecheniya informatsionnoy bezopasnosti organov vnutrennikh del Rossiyskoy Federatsii do 2020 goda: prikaz MVD Rossii ot 14.03.2012 № 169 [Elektronnyy resurs]. — URL:http://policemagazine.ru/forum/showthread.php?t=3663 (data obrashcheniya: 21.10.2019). [On the approval of the Concept for ensuring information security of the internal affairs bodies of the Russian Federation until 2020: order of the Ministry of Internal Affairs of Russia dated March 14, 2012 No. 169 [Electronic resource]. - URL: http: //policemagazine.ru/forum/showthread.php?t = 3663 (date accessed: 21.10.2019). (In Russ)]

6. Security Trends & Vulnerabilities Review Corporate Information Systems // Positive Technologies 2017 [Electronic resource]. - URL: https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Corp-Vulnerabilities-2017-eng.pdf (date accessed: 09.11.2019).

7. Bagayoko D. Understanding the Relativistic Generalization of Density Functional Theory (DFT) and Completing It in Practice / D. Bagayoko // Journal of Information Security. Vol. 7 № 9, May 2016 [Electronic resource]. - URL: https: //www.scirp.org/journal/paperinformation.aspx? Paperid = 66781 (date accessed: 02.11.2019).

8. Metody i sredstva otsenki zashchishchonnosti avtomatizirovannykh sistem organov vnutrennikh del: monografiya [Elektronnyy resurs] / I.G. Drovnikova [i dr.]. Voronezh: Voronezh. in-t MVD Rossii, 2017. 88 s. [Methods and tools for assessing the security of automated systems of internal affairs bodies: monograph [Electronic resource] / I.G. Drovnikov [and others]. Voronezh: Voronezh. Institute of the Ministry of Internal Affairs of Russia, 2017.88 p. (In Russ)]

9. YAzov YU.K. Zashchita informatsii v informatsionnykh sistemakh ot nesanktsionirovannogo dostu-pa: posobiye / YU.K. YAzov, S.V. Solov'yov. Voronezh: Kvarta, 2015. 440 s. [Yazov Yu.K. Protection of information in information systems from unauthorized access: manual / Yu.K. Yazov, S.V. Solovyov. Voronezh: Kvarta, 2015.440 p. (In Russ)]

10. GOST R 50922-2006. Zashchita informatsii. Osnovnyye terminy i opredeleniya // SPS «Konsul'-tantPlyus» [GOST R 50922-2006. Data protection. Basic terms and definitions // SPS "ConsultantPlus"(In Russ)]

11. Kresimir S. The information systems' security level assessment model based on an ontology and evidential reasoning approach / S. Kresimir, O. Hrvoje, G. Marin // Computers & Security. 2015. PP. 100-112.

12. Method to Evaluate Software Protection Based on Attack Modeling / H. Wang [et ol.] // 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing Year. 2013. PP. 837-844.

13. Effectiveness Evaluation on Cyberspace Security Defense System / L. Yun [et ol.] // International Conference on Network and Information Systems for Computers (IEEE Conference Publications). 2015. PP. 576-579.

14. FSTEK Rossii. Metodicheskiy dokument. Metodika opredeleniya ugroz bezopasnosti informa-tsii v informatsionnykh sistemakh [Elektronnyy resurs]. — URL:http://https://fstec.ru/component/attachments/ download/812 (data obrashcheniya: 21.10.2019). [FSTEC of Russia. Methodical document. Methods for determining threats to information security in information systems [Electronic resource]. - URL: http: // https: //fstec.ru/component/attachments/ download / 812 (date of access: 21.10.2019). (In Russ)]

15. YAzov YU.K. Organizatsiya zashchity informatsii v informatsionnykh sistemakh ot nesanktsioniro-vannogo dostupa: monografiya / YU.K. YAzov, S.V. Solov'yev. — Voronezh: Kvarta, 2018. — 588 s. [Yazov Yu.K. Organization of information protection in information systems from unauthorized access: monograph / Yu.K. Yazov, S.V. Soloviev. - Voronezh: Quarta, 2018. 588 p. (In Russ)]

16. Rogozin Ye.A. Proyektirovaniye sistem zashchity informatsii ot nesanktsionirovannogo dostupa v avtomatizirovannykh sistemakh OVD / Ye.A. Rogozin, A.D. Popov, T.V. Shagirov // Vestnik Voronezh. in-ta MVD Rossii. 2016. № 2. S. 174-183. [Rogozin E.A. Design of information protection systems against unauthorized access in automated ATC systems / E.A. Rogozin, A.D. Popov, T.V. Shagirov // Bulletin Voronezh. Institute of the Ministry of Internal Affairs of Russia. 2016. No. 2. pp. 174-183. (In Russ)]

17. Popov A.D. Modeli i algoritmy otsenki effektivnosti sistem zashchity informatsii ot ne-sanktsionirovannogo dostupa s uchetom ikh vremennykh kharakteristik v avtomatizirovannykh sistemakh orga-nov vnutrennikh del: dis. ... kand. tekhn. nauk: 05.13.19 / Popov Anton Dmitriyevich. — Voronezh, 2018. — 163 s. [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: dis. ... Cand. tech. Sciences: 05.13.19 / Popov Anton Dmitrievich. Voronezh, 2018 . 163 p. (In Russ)]

18. Rad'ko N.M. Proniknoveniya v operatsionnuyu sredu komp'yutera: modeli zloumyshlennogo uda-lennogo dostupa: ucheb. posobiye / N.M. Rad'ko, YU.K. YAzov, N.N. Korneyeva. — Voronezh: Voronezh. gosud. tekh-nich. un-t, 2013. — 265 s. [Radko N.M. Penetration into the operating environment of a computer: models of malicious remote access: textbook. manual / N.M. Radko, Yu.K. Yazov, N.N. Korneeva. - Voronezh: Voronezh. state tech-nich. un-t, 2013 . 265 p. (In Russ)]

19. GOST R ISO/MEK 7498-1-99. Informatsionnaya tekhnologiya. Vzaimosvyaz' otkrytykh sistem. Ba-zovaya etalonnaya model'. Chast' 1. Bazovaya model' [Elektronnyy resurs]. — URL:https://files.stroyinf.ru/ Data2/1/4294818/4294818276.pdf (data obrashcheniya: 04.11.2019). [GOST R ISO / IEC 7498-1-99. Information technology. Interconnection of open systems. Basic reference model. Part 1. Basic model [Electronic resource]. - URL: https: //files.stroyinf.ru/ Data2 / 1/4294818 / 4294818276.pdf (date of access: 04.11.2019). (In Russ)]

20. GOST R 51583-2014. Poryadok sozdaniya avtomatizirovannykh sistem v zashchishchennom ispolnenii [Elektronnyy resurs]. — URL: http://docs.cntd.ru/document/ 1200108858 (data obrashcheniya: 04.11.2019). [GOST R 51583-2014. The order of creation of automated systems in a protected version [Electronic resource]. - URL: http://docs.cntd.ru/document/1200108858 (date of access: 04.11.2019). (In Russ)]

21. Rogozin Ye.A. Klassifikatsiya ugroz informatsionnoy bezopasnosti v avtomatizirovannykh in-formatsionnykh sistemakh / Ye.A. Rogozin, A.D. Popov, D.I. Korobkin // Pribory i sistemy. Upravleniye, kontrol', diagnostika. 2017. № 7. S. 22-26. [Rogozin E.A. Classification of threats to information security in automated information systems / E.A. Rogozin, A.D. Popov, D.I. Korobkin // Devices and Systems. Management, control, diagnostics. 2017. No. 7.P. 22-26. (In Russ)]

22. Rukovodyashchiy dokument Gosudarstvennoy tekhnicheskoy komissii ot 30 iyunya 1992 goda. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Terminy i opredeleniya. [Elektronnyy resurs]. — URL: https://fstec.ru/component/attachments/download/29 [Guidance document of the State Technical Commission dated June 30, 1992. Protection against unauthorized access to information. Terms and Definitions. [Electronic resource]. - URL: https://fstec.ru/component/attachments/download/298 (In Russ)]

23. Rogozin Ye.A. Osnovnyye etapy i zadachi razrabotki sistem zashchity informatsii OVD v avtomatizirovannykh si- stemakh / Ye.A. Rogozin, Ye.YU. Nikulina, A.D. Popov // Vestnik Voronezh. in-ta FSIN Rossii. 2016. № 4. S. 94-98 [Rogozin E.A. The main stages and tasks of developing ATS information protection systems in automated systems stemakh / E.A. Rogozin, E.Yu. Nikulina, A.D. Popov // Bulletin Voronezh. Institute of the Federal Penitentiary Service of Russia. 2016. No. 4. pp 94-98. (In Russ)]

24. Sistema pokazateley kachestva funktsionirovaniya pri sozdanii sistemy informatsionnoy bezopasnosti na ob"yekte informatizatsii OVD / A.M. Kadnova [i dr.] // Pribory i sistemy, upravleniye, kontrol', diagnostika. 2019. № 1. S. 26- 33 [The system of performance indicators for the creation of an information security system at the object of informatization of the internal affairs department Kadnova [et al.] // Devices and systems, control, monitoring, diagnostics. 2019. No. 1. pp 26-33 (In Russ)]

Сведения об авторах:

Баркалов Юрий Михайлович, заместитель начальника кафедры информационной безопасности; e-mail: ekcvor@mail.ru

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

Каднова Айжана Михайловна, адъюнкт кафедры автоматизированных информационных систем органов внутренних дел; e-mail: aizhana_kadnova@mail.ru

Овчинникова Елена Сергеевна, адъюнкт кафедры автоматизированных информационных систем органов внутренних дел; e-mail: yelena_ovchinnikova1@mail.ru.

Рогозин Евгений Алексеевич, доктор технических наук, профессор, профессор кафедры автоматизированных информационных систем органов внутренних дел; e-mail: evgenirogozin@yandex.ru

Information about the authors:

Yuri M. Barkalov, Deputy Head of the Information Security Department; e-mail: ekcvor@mail.ru

Irina G. Drovnikova, Dr. Sci. (Technical), Assoc. Prof., Prof., Department of Automated Information Systems of the Internal Affairs Bodies; e-mail: idrovnikova@mail.ru

Ayzhana M. Kadnova, Adjunct, Department of Automated Information Systems of Internal Affairs Bodies; e-mail: aizhana_kadnova@mail.ru

Elena S. Ovchinnikova, Adjunct of the Department of Automated Information Systems of Internal Affairs Bodies; e-mail: yelena_ovchinnikova1@mail.ru.

Evgeniy A. Rogozin, Dr. Sci. (Technical), Prof., Prof., Department of Automated Information Systems of Internal Affairs Bodies; e-mail: evgenirogozin@yandex.ru

Конфликт интересов.
Авторы заявляют об отсутствии конфликта интересов.
Поступила в редакцию 30.04.2020.
Принята в печать 28.05.2020.

Conflict of interest.
The authors declare no conflict of interest.
Received 30.04.2020.
Accepted for publication 28.05.2020.