ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056
DOI: 10.21822/2073-6185-2023-50-1-81-88 Оригинальная статья /Original Paper

Анализ особенностей функционирования защищенных автоматизированных систем органов внутренних дел в условиях воздействия угроз несанкционированного доступа

А.О. Ефимов, В.С. Наседкина, А.Д. Попов, Е.А. Рогозин, В.Р. Романова
Воронежский институт МВД России,
394065, г. Воронеж, пр. Патриотов, 53, Россия

Резюме. Цель. Целью исследования является анализ особенностей функционирования защищенных автоматизированных систем и разработка структурной схемы типовой АС ОВД, включающей в свой состав различные структурные элементы. **Метод.** В качестве основополагающего метода проведения исследования является метод системного анализа. **Результат.** На основе разработанной типовой структурной схемы АС ОВД определены в соответствии с официальным сайтом ФСТЭК, угрозы к веб-серверам, а также, в соответствии с ними выявлены потенциальные уязвимости (слабые места с точки зрения информационной безопасности); разработана и приведена классификация всех потенциально опасных угроз к информационному ресурсу защищенных АС ОВД. **Вывод.** Материалы статьи могут быть использованы для проведения анализа и разработки методики количественной оценки рисков нарушения информационной безопасности web-серверов АС ОВД РФ; методики оценки уровня защищенности АС ОВД РФ; методики доступа штатных пользователей АС ОВД РФ к информационному ресурсу этих систем на основе семантического анализа.

Ключевые слова: угроза, атака, конфиденциальная информация, интернет, нарушитель, информационный ресурс, веб-сервер

Для цитирования: А.О. Ефимов, В.С. Наседкина, А.Д. Попов, Е.А. Рогозин, В.Р. Романова. Анализ особенностей функционирования защищенных автоматизированных систем органов внутренних дел в условиях воздействия угроз несанкционированного доступа. Вестник Дагестанского государственного технического университета. Технические науки. 2023; 50(1):81-88. DOI:10.21822/2073-6185-2023-50-1-81-88

Analysis and features of the functioning of protected automated systems of internal affairs bodies under the influence of threats of unauthorized access

A.O. Efimov, V.S. Nasedkina, A.D. Popov, E.A. Rogozin, V.R. Romanova
Voronezh Institute of the Ministry of Internal Affairs of Russia,
53 Patriotov Str., Voronezh 394065, Russia

Abstract. Objective. The purpose of the study is to analyze the features of the functioning of protected automated systems and develop a structural diagram of a typical ATS AS, which includes various structural elements. **Method.** As a fundamental method of conducting research is the method of system analysis. **Result.** Based on the developed typical structural diagram of the ATS AS, threats to web servers were identified in accordance with the official website of the FSTEC, and, in accordance with them, potential vulnerabilities (weak points in terms of information security) were identified; a classification of all potentially dangerous threats to the information resource of protected ATS automated systems was developed and presented. **Conclusion.** The materials of the article can be used to analyze and develop a methodology for quantitatively assessing the risks of information security violations of the web servers of the ATS of the Russian Federation; methods for assessing the level of security of the ATS of the Russian Federation; methods of access of regular users of the RF ATS AS to the information resource of these

systems based on semantic analysis.

Keywords: Threat, attack, confidential information, internet, intruder, information resource, web server

For citation: A.O. Efimov, V.S. Nasedkina, A.D. Popov, E.A. Rogozin, V.R. Romanova. Analysis features of the functioning of protected automated systems of internal affairs bodies under the influence of threats of unauthorized access. Herald of the Daghestan State Technical University. Technical Science. 2023; 50(1): 81-88. DOI:10.21822/2073-6185-2023-50-1-81-88

Введение. Процесс автоматизации нашел широкое применение в органах внутренних дел РФ, компьютерные системы широко используются на всех уровнях он нижнего звена до наивысшего, включая управленческий аппарат. Как показывает опыт эксплуатации этих систем, основной особенностью которых является обработка, хранение и передача конфиденциальной информации, что требует своевременного принятия организационных и технических мер, связанных с защитой информации в этих системах (далее по тексту – АС ОВД), а также организацию обеспечения требуемого уровня безопасности информации (БИ) в целом.

Как показывает анализ [1-9], одним из самых опасных видов атак АС ОВД РФ, являются атаки, связанные с несанкционированным доступом (НСД) злоумышленника на информационный ресурс, что в целом может привести к нарушению надежности функционирования этих систем. Важность этой проблемы, в частности, подчеркивается в [5, 8].

Постановка задачи. В данной статье, в качестве примера, разработана обобщенная структурная схема АС ОВД РФ, включая веб-серверы (рис.1). Определены, в соответствии с требованиями действующей методической документации Федеральной службы по техническому и экспертному контролю (ФСТЭК) [7] основные угрозы НСД, представляющие опасность веб-серверам, также, в соответствии с ними определены основные уязвимости («слабые места с точки зрения ИБ») (рис.2), а также приведена и разработана классификационная схема угроз НСД с учетом веб-серверов (рис.3).

Методы исследования. Анализ открытых литературных источников [1-9] позволил разработать структурную схему типовой АС ОВД РФ, представленной на рис.1, где одним из основных компонентов этой системы является веб-сервер.

Веб-сервер – это совокупность аппаратного и программного обеспечения, решающая ряд задач, основной задачей которой, является предоставление пользователю результатов запроса после его обработки. Веб-серверы не только выдают информацию по запросу, но и могут выполнять более сложные операции по её обработке. На выходе веб-сервера информация пользователю выдается в формате «*.html», поэтому защита веб-сервера от компьютерных атак, связанных с НСД, является весьма актуальной задачей.

Уязвимость веб-сервера – это свойство веб-сервера, предоставляющее возможность реализации угроз безопасности обрабатываемой в ней информации [1, с.147].

Защита информации направлена на предупреждение возможности возникновения, предотвращение реализации или снижение ущерба от последствий несанкционированных действий в результате реализации той или иной угрозы безопасности информации.

Введение термина «угроза безопасности информации» позволяет объединить одним понятием все возможные негативные условия и факторы, влияющие прямым образом на безопасность информации, то есть на ее целостность, доступность или конфиденциальность [1, с.147]. Под угрозой безопасности информации понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [1, с.147].

Под источником угрозы безопасности информации понимается субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации. [1, с.151].

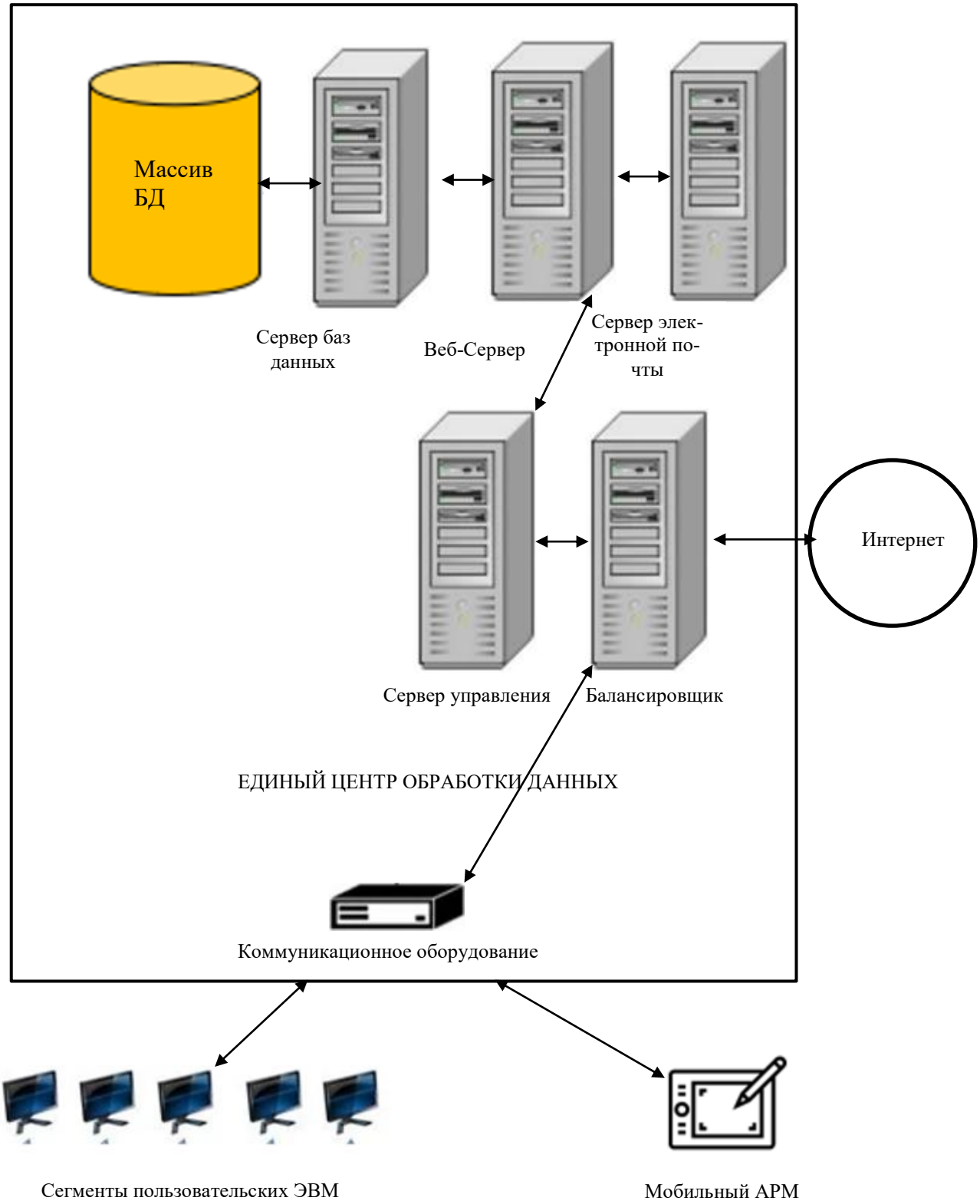

Рис.1. Типовая структура АС ОВД
Fig. 1. Typical structure of ATS AS

Внешний источник угрозы БИ – это субъект (физическое лицо, организация, служба иностранного государства и т.п.), который способен извне по отношению к АС ОВД РФ создать обстоятельства, при которых функционирование системы может оказаться под угрозой. Внутренний источник угрозы БИ – это субъект в пределах территории организации, деятельность которого, преднамеренно или непреднамеренно может привести к нарушению БИ, циркулирующей в АС ОВД РФ.

Указанными субъектами могут быть: нарушитель, программная или программно-аппаратная закладка, носитель с установленной на нем вредоносной или иной программой, используемой для реализации угрозы безопасности информации в ИС [1, с.151].

Из-за различных уязвимостей, которыми могут обладать веб-сервера, в соответствии с требованиями действующей методической документации Федеральной службы по техническому и экспертному контролю (ФСТЭК) были проанализированы угрозы, способствующие нанести ущерб веб-серверам (рис. 2).

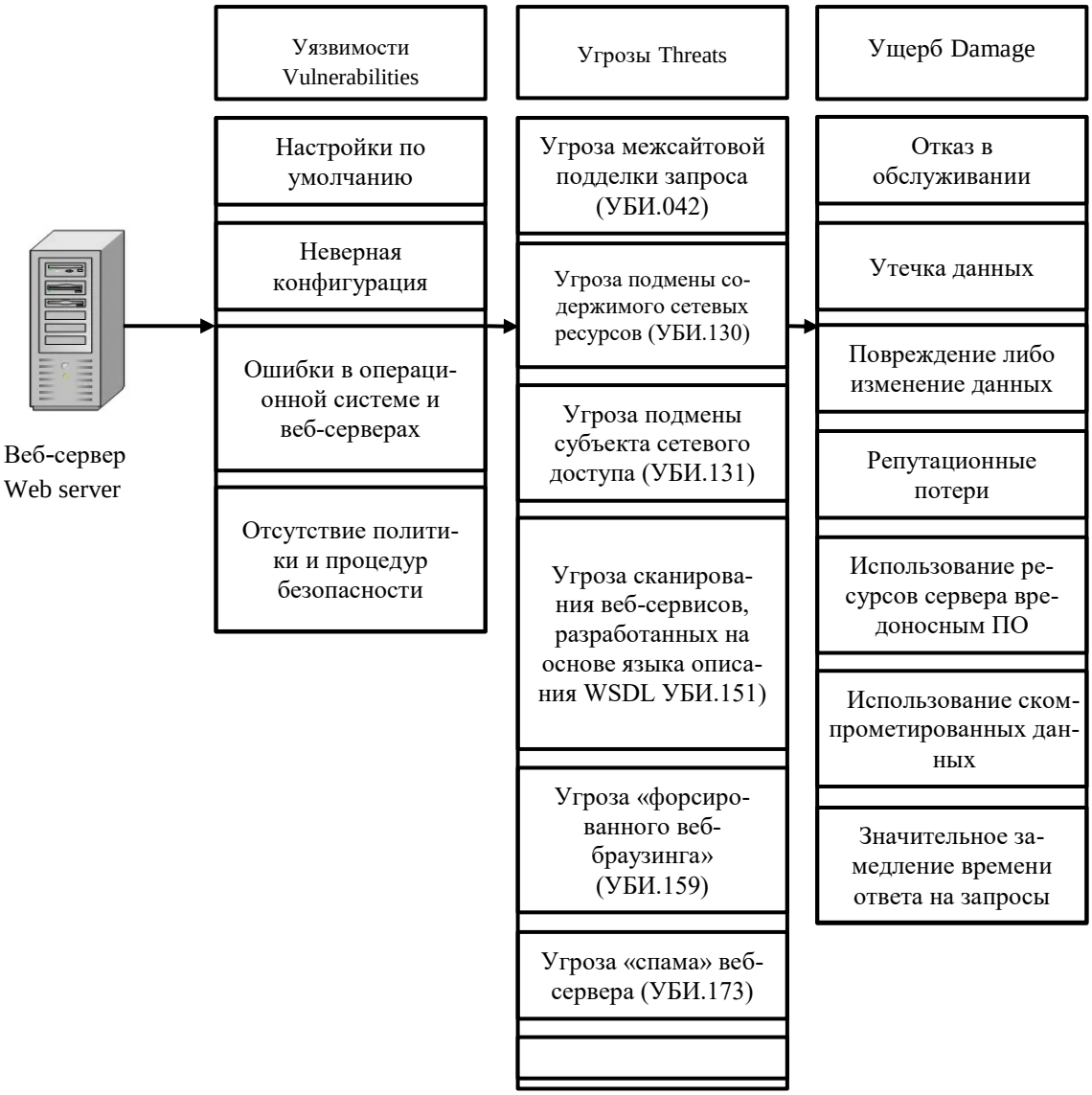

Рис. 2.Угрозы, способствующие нанести ущерб веб-серверам
Fig. 2.Threats that help damage web servers

Угрозы, представляющие опасность веб-серверам АС ОВД РФ, с точки зрения их ИБ приведены в таб. 1. Источником угроз могут являться внешние нарушители с низким или средним потенциалом. К последствиям реализации угрозы можно отнести нарушение конфиденциальности, целостности, доступности [3], что в целом ведет к нарушению работоспособности АС ОВД РФ.

Таблица 1. Актуальные угрозы внешнего нарушителя БИ к информационному ресурсу веб-серверов локализованных в АС ОВД РФ
Table 1. Actual threats from an external BI violator to the information resource of web servers localized in the ATS of the Russian Federation

№	Наименование угрозы Name of the threat	Описание угрозы Description of the threat	Объект воздействия Object of influence
УБИ.042	Угроза межсайтовой подделки запроса Threat of cross-site request forgery	Угроза заключается в возможности отправки нарушителем дискредитируемому пользователю ссылки на содержащий вредоносный код веб-ресурс, при переходе на который автоматически будут выполнены неправомерные вредоносные действия от имени дискредитированного пользователя.	Сетевой узел, сетевое программное обеспечение
УБИ.130	Угроза подмены содержимого сетевых ресурсов The threat of spoofing the contents of network resources	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемым данным пользователей сети или проведения различных мошеннических действий путём скрытной подмены содержимого хранящихся или передаваемых по сети данных.	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик
УБИ.131	Угроза подмены субъекта сетевого доступа Threat of substitution of the subject of network access	Заключается в возможности осуществления нарушителем несанкционированного доступа к защищаемым данным пользователей сети или проведения различных мошеннических действий путём скрытной подмены в отправляемых дискредитируемым пользователем сетевых запросах сведений об отправителе сообщения.	Прикладное программное обеспечение, сетевое программное обеспечение, сетевой трафик
УБИ.151	Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL The threat of scanning web services developed based on the WSDL description language	Угроза заключается в возможности получения нарушителем сведений о текущей конфигурации веб-служб и наличии в ней уязвимостей путём исследования WSDL-интерфейса веб-сервера.	Сетевое программное обеспечение, сетевой узел
УБИ.159	Угроза «форсированного веб-браузинга» The Threat of "Forced Web Browsing"	Заключается в возможности получения нарушителем доступа к защищаемой информации, выполнения привилегированных операций или осуществления иных деструктивных воздействий на некорректно защищённые компоненты веб-приложений.	Сетевой узел, сетевое программное обеспечение
УБИ.173	Угроза «спама» веб-сервера Web Server Spam Threat	Угроза заключается в возможности неправомерного осуществления нарушителем массовой рассылки коммерческих, политических, мошеннических и иных сообщений на веб-сервер без запроса со стороны дискредитируемых веб-серверов.	Сетевое программное обеспечение

Основные уязвимости веб-серверов АС ОВД с точки зрения ИБ:

1. Настройки по умолчанию подразумевают под собой, что никаких изменений в работу программ не вносится, и они функционируют в соответствии с начальными алгоритмами.
2. Неверная конфигурация с точки зрения ИБ означает, что данный вид уязвимости относится к неверной реализации политики безопасности, предназначенной для качественной защиты данных, имеющиеся в приложениях.
3. Ошибки в операционной системе и веб-серверах демонстрируют, что в ОС имеется уязвимость типа «дыра», через которую можно получить доступ к информационному ресурсу АС ОВД РФ, что ведет к нарушению конфиденциальности, целостности, защищенности и доступности этих систем.

4. Отсутствие политики и процедур безопасности означает, что данная уязвимость ведет к нарушению защищенности АС ОВД в целом [2,4,6].

Рис. 3.Классификация угроз безопасности информации АС ОВД РФ с учетом веб-серверов
Fig. 3. Classification of threats to the security of information of the ATS of the Russian Federation, taking into account web servers

Ущербы, полученные в результате атак на информационный ресурс АС ОВД РФ:

1. Отказ в обслуживании подразумевает под собой недоступность запрашиваемых ресурсов, путем временного нарушения работоспособности АС ОВД РФ.
2. Утечка данных означает передачу конфиденциальной информации третьим лицам.

3. Повреждение либо изменение данных обозначает нарушение целостности информации, часто приводящее к невозможности её использования.
4. Репутационными потерями являются потери финансового типа.
5. После использования ресурсов сервера вредоносными ПО может произойти, например, снижение производительности, отзывчивости ОС.
6. Использование скомпрометированных данных подразумевает под собой использование конфиденциальных данных третьими лицами.
7. Значительное замедление времени ответа на запросы означает уменьшение работоспособности системы в целом.

Обсуждение результатов. Для обобщения всего многообразия угроз была разработана классификационная схема угроз безопасности информации АС ОВД РФ с учетом веб-серверов (рис. 3). Проведенный в статье анализ позволил выявить и определить отличительные свойства защищенных АС ОВД РФ, к которым можно отнести [2, 7, 9]:

- значительное местоположение защищенных АС ОВД РФ;
- потребность в создании и администрировании защищенной сетевой инфраструктуры, регламентированную нормативными документами;
- организация управления доступом АС ОВД РФ;
- обеспечение поддержания надлежащего уровня ИБ за счет проведения регулярных комплексных проверок АС ОВД;
- объединение АС ОВД в единый массив банков данных различного уровня конфиденциальности информации (применительно к ОВД информация объединяется в единый банк данных, что по своей сути ведет к увеличению уязвимостей и сложностям в администрировании с точки зрения ИБ);
- нахождение в составе АС ОВД несертифицированного прикладного ПО (требования по ИБ не учитывают влияния прикладного ПО);
- сложность в хранении больших массивов данных.

Вывод. Материалы статьи могут быть использованы для разработки методик:

1. Методики количественной оценки рисков нарушения информационной безопасности web-серверов АС ОВД РФ;

2. Методики оценки уровня защищенности АС ОВД РФ;

3. Методики доступа штатных пользователей АС ОВД РФ к информационному ресурсу этих систем на основе семантического анализа.

Библиографический список:

1. Язов Ю.К., Соловьев С.В. Защита информации в информационных системах от несанкционированного доступа. Пособие – Воронеж: Кварта, 2015. – 440 с.
2. Анализ рисков ущерба от угроз информационной безопасности в информационно-технических системах органов внутренних дел: монография / Т. В. Мещерякова, Е. А Рогозин, И. В. Алехин [и др.]. — Воронеж: Воронежский институт МВД России, 2021. — 63 с.
3. Мишин С.А., Вольф В.А., Нестеровский О.И., Рогозин Е.А., Калач А.В. Анализ нормативной документации ФСТЭК РОССИИ с целью оценки защищенности операционных систем автоматизированных систем органов внутренних дел // Вестник Воронежского института ФСИН России, №2, (2022). – С. 111-120.
4. Мочалов Д.А., Вольф В.А., Романова В.Р., Рогозин Е.А., Калач А.В. Анализ существующих угроз внешнего нарушителя к информационному ресурсу веб-серверов в автоматизированных системах вооруженных сил российской федерации // Вестник Воронежского института ФСИН России №1– 2022. С. 68-75.
5. Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года: приказ МВД России от 14.03.2012 № 169 [Эл. ресурс].Режим доступа: http://policemagazine. ru/forum/showthread.php?t=3663(Дата обращения: 06.11.2022).
6. ФСТЭК России. Методический документ. Методика оценки угроз безопасности информации (утв. ФСТЭК России 5 февраля 2021 г.) [Эл.ресурс]. – Режим доступа: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021– (Дата обращения: 10.11.2022).
7. ФСТЭК России. Банк данных угроз безопасности информации. Угрозы безопасности информации [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru/threat.– (Дата обращения: 10.11.2022).

8. Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента РФ от 05.12.2016 № 646 // СПС «КонсультантПлюс» (дата обращения: 07.03.2018).
9. Попов А.Д. Модели и алгоритмы оценки эффективности типовых систем защиты информации от несанкционированного доступа в автоматизированных системах органов внутренних дел: дис. канд. технич. наук 05.13.19 / Попов А.Д. – Воронеж., 2020. – 108 с.
10. Системы обнаружения компьютерных атак : учебное пособие / В. Т. Еременко, А. П. Фисун, С. М. Макеев, Б. И. Соловьев, Д. О. Маркин. - Орёл : ОГУ имени И. С. Тургенева, 2018. - 135 с.

References:

1. Yazov Yu.K., Soloviev S.V. Protection of information in information systems from unauthorized access. *Allowance.Voronezh: Quarta*, 2015; 440.[In Russ]
2. Risk analysis of damage from threats to information security in the information and technical systems of internal affairs bodies: monograph.T. V. Meshcheryakova, E. A. Rogozin, I. V. Alekhin [and others]. *Voronezh: Voronezh Institute of the Ministry of Internal Affairs of Russia*, 2021; 63.[In Russ]
3. Mishin S.A., Wolf V.A., Nesterovsky O.I., Rogozin E.A., Kalach A.V. Analysis of the regulatory documentation of the FSTEC of RUSSIA in order to assess the security of operating systems of automated systems of internal affairs bodies. *Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia*, 2022; 2:111-120.[In Russ]
4. Mochalov D.A., Wolf V.A., Romanova V.R., Rogozin E.A., Kalach A.V. Analysis of the existing threats of an external intruder to the information resource of web servers in the automated systems of the armed forces of the Russian Federation. *Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia*. 2022; 1: 68-75.[In Russ]
5. On the approval of the Concept for ensuring the 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 [El.res.] Access mode: http://policemagazine. ru/forum/showthread.php?t=3663. (Date of treatment: 06.11.2022) [In Russ]
6. FSTEC of Russia. Methodical document. Methodology for assessing threats to information security (approved by the FSTEC of Russia on February 5, 2021) [El.res.]. Access mode: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021. (Date of treatment: 11/10/2022) [In Russ]
7. FSTEC of Russia. Data bank of information security threats. Information Security Threats [Electronic resource]. Access mode: https://bdu.fstec.ru/threat.– (Date of access: 11/10/2022) [In Russ]
8. On approval of the Doctrine of Information Security of the Russian Federation: Decree of the President of the Russian Federation dated 05.12.2016 No. 646. *SPS "ConsultantPlus"*(date of access:03/07/2018)[In Russ]
9. Popov A.D. Models and algorithms for evaluating the effectiveness of typical systems for protecting information from unauthorized access in automated systems of internal affairs bodies: dis. cand. tech. Sciences 05.13.19 / Popov A.D. - Voronezh., 2020;108.[In Russ]
10. Computer attack detection systems: textbook. V. T. Eremenko, A. P. Fisun, S. M. Makeev, B. I. Soloviev, D. O. Markin. - Eagle: OSU named after I. S. Turgenev, 2018; 135. [In Russ]

Сведения об авторах:

Ефимов Алексей Олегович, адъюнкт очной формы обучения; ea.aleksei@yandex.ru

Наседкина Валерия Сергеевна, адъюнкт; valeriya.sn@mail.ru.

Попов Антон Дмитриевич, кандидат технических наук, старший реподаватель;anton.holmes@mail.ru

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

Романова Виктория Романовна, адъюнкт очной формы обучения; romanovna_vika@inbox.ru

Information about authors:

Aleksey O. Yefimov, full-time adjunct; ea.aleksei@yandex.ru

Valeria S. Nasedkina, adjunct; valeriya.sn@mail.ru.

Anton D. Popov, Cand. Sci. (Eng.), Senior lecturer; anton.holmes@mail.ru

Evgeny A. Rogozin, Dr. Sci. (Eng.), Prof., Prof., Department of Automated Information Systems of Internal Affairs Bodies; evgenirogozin@yandex.ru

Victoria R. Romanova, adjunct of full-time education; romanovna_vika@inbox.ru

Конфликт интересов/Conflict of interest.

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

Поступила в редакцию/Received 28.11.2022.

Одобрена после рецензирования/ Reviced 22.12.2022.

Принята в печать/Accepted for publication 22.12.2022.