ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004. 0567
DOI: 10.21822/2073-6185-2023-50-3-167-171

Обзорная статья / Review article

Алгоритмизация расчета оценки защищенности операционных систем АИС органов внутренних дел, разработанного на основе анализа требований безопасности ГОСТ Р ИСО/МЭК 15408 и возможных угроз

А.И. Янгиров[1], Е.А. Рогозин[2], О.И. Бокова[3], С.Б. Ахлюстин[4]
[1]ФКУ «НИЦ «Охрана» Росгвардии,
[1]111539, г. Москва, Реутовская, 12Б, Россия,
[2,4] Воронежский институт МВД России,
[2,4] 394065, г. Воронеж, проспект Патриотов, 53, Россия,
[3]ООО «Каскад»,
[3]109444, г. Москва, ул. Ферганская, д. 2, к. 2, оф. 7, Россия

Резюме. Цель. В статье проводится обобщенная алгоритмизация процессов, необходимых для разработки программного обеспечения для оценки защищенности операционных систем автоматизированных информационных систем органов внутренних дел Российской Федерации. **Метод.** Исследование провдено на основе метода анализа возможных угроз безопасности операционных систем, а также требований стандарта ГОСТ Р ИСО/МЭК 15408. **Результат.** Результатом работы автоматизированной системы расчета показателя защищенности анализируемой ОС является один из заданных критериев показателей степени защищенности ОС. Путем сравнения полученного показателя выдается соответствующий результат **Вывод**. Авторами дана обобщенная алгоритмизация процессов, необходимых для разработки программного обеспечения для оценки защищенности ОС АИС ОВД РФ.

Ключевые слова: оценка защищенности, функциональные требования безопасности, банк данных угроз безопасности информации, политика безопасности, показателя защищенности, операционная система, автоматизированная система расчета, программное обеспечение.

Для цитирования: А.И. Янгиров, Е.А. Рогозин, О.И. Бокова, С.Б. Ахлюстин. Алгоритмизация расчета оценки защищенности операционных систем АИС ОВД, разработанного на основе анализа требований безопасности ГОСТ Р ИСО/МЭК 15408 и возможных угроз. Вестник Дагестанского государственного технического университета. Технические науки. 2023; 50(3): 167-171. DOI:10.21822/2073-6185-2023-50-3-167-171

Algorithmization for calculating the security assessment of AIS operating systems of internal affairs bodies, developed on the basis of an analysis of security requirements GOST R ISO/IEC 15408 and possible threats

A.I. Yangirov [1], E.A. Rogozin [2], O.I. Bokova [3], S.B. Akhlyustin [4]
[1]FKU “Research Center “Protection” of the Russian Guard,
[1]12B Reutovskaya Str., Moscow 111539, Russia,
[2,4] Voronezh Institute of the Ministry of Internal Affairs of Russia,
[2,4] 53 Patriotov Ave., Voronezh 394065, Russia,
[3]OOO “Cascade”,
[3]2 Ferghanskaya St., room 2, of. 7, Moscow 109444, Russia

Abstract. Objective. The article provides a generalized algorithmization of the processes necessary for developing software for assessing the security of operating systems of automated information systems of internal affairs bodies of the Russian Federation. **Method.** The research was carried out based on the method of analyzing possible threats to the security of operating systems, as well as the requirements of the GOST R ISO/IEC 15408 standard. **Result.** The result of the automated system for calculating the

security indicator of the analyzed OS is one of the specified criteria for indicators of the degree of security of the OS. By comparing the obtained indicator, the corresponding result is output. **Conclusion.** The authors provide a generalized algorithmization of the processes necessary for developing software for assessing the security of the AIS OS of the Russian Federation ATS.

Keywords: security assessment, functional security requirements, data bank of information security threats, security policy, security indicators, operating system, automated calculation system, software.

For citation: A.I. Yangirov, E.A. Rogozin, O.I. Bokova, S.B. Akhlyustin. Algorithmization for calculating the security assessment of AIS operating systems of internal affairs bodies, developed on the basis of an analysis of security requirements GOST R ISO/IEC 15408 and possible threats. Herald of Daghestan State Technical University. Technical Science. 2023; 50(3): 167-171. DOI:10.21822/2073-6185-2023-50-3-167-171

Введение. В настоящей работе проводится обобщенное описание алгоритма оценки защищенности операционных систем (далее - ОС) АИС ОВД РФ, реализованного в специальном программном обеспечении, ранее представленного в статье, посвященной разработке автоматизированной системы расчета оценки защищенности операционных систем информационных систем на основе анализа требований безопасности [1,4].

Постановка задачи. Процесс алгоритмизации необходим для построения алгоритма решения задачи, результатом которого является выделение этапов процесса обработки данных, формальная запись содержания этих этапов и определение порядка их выполнения [2,5-7].

Методы исследования. Обобщенная алгоритмизация процессов, проводимых в данном расчете, представляется в формате блок-схем соответствующих этапов методики. Данный формат был предопределен возможностью графического представления алгоритма расчета для обеспечения наглядности последовательности действий.

На основе автоматизированной системы расчета оценки защищенности ОС АИС ОВД, а также соответствующей методики оценки защищенности ОС, основанную на анализе требований ГОСТ Р ИСО/МЭК 15408 и возможных угроз ОС, описание основных этапов работы программного обеспечения [3].

Под ОС АИС ОВД понимаются операционные системы, предназначенные для применения на автоматизированных рабочих местах информационных систем, используемых в ОВД. В соответствии с разработанной методикой оценки защищенности ОС АИС ОВД определяющими критериями защищенности ОС являются перечень угроз, выбранных из банка данных угроз безопасности информации, разработанного ФАУ «ГНИИИ ПТЗИ ФСТЭК России», а также разработанные в соответствии с ГОСТ Р ИСО/МЭК 15408 требования, предъявляемые к ОС [3].

Обсуждение результатов. В процесс оценки защищенности ОС АИС ОВД включены три этапа, в которые входят: ранжирование и выборка угроз, проверка соответствия требований безопасности в соответствии с ГОСТ Р ИСО/МЭК 15408, политик и целей безопасности в соответствии с выбранным эталонным профилем защиты, а также расчет показателя защищенности анализируемой ОС. В обобщенном представлении процесс оценки защищенности ОС АИС ОВД, реализованный в специальном программном обеспечении может быть изображен в следующем виде (рис.1). В блоке входных данных для оценки защищенности ОС АИС ОВД после произведенной выборки необходимых элементов экспертом по безопасности программой формируется специальный класс «Data», в который входят необходимые требования безопасности, а также перечень возможных угроз, способных воздействовать на ОС. После ввода входных данных программой автоматически производится расчет коэффициента угроз ОС на основе перечня возможных угроз. Алгоритм расчета коэффициента угроз ОС «K» представлен на рис. 2.

Далее производится расчет соответствия совпадения требований, реализованных в оцениваемой ОС, с эталонной ОС.

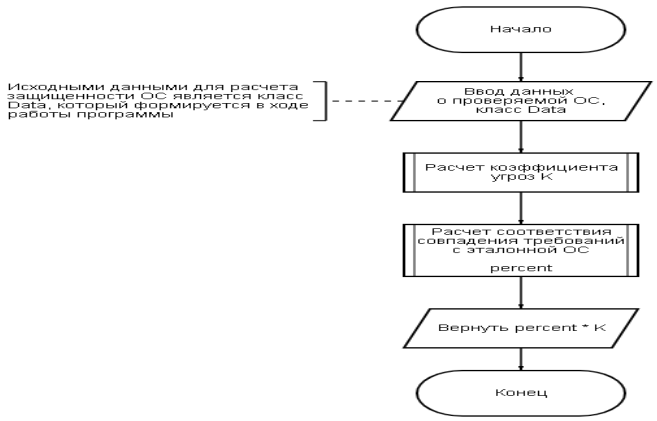

Рис. 1. Обобщенный процесс оценки защищенности ОС АИС ОВД
Fig. 1. Generalized process for assessing the security of the AIS ATS OS

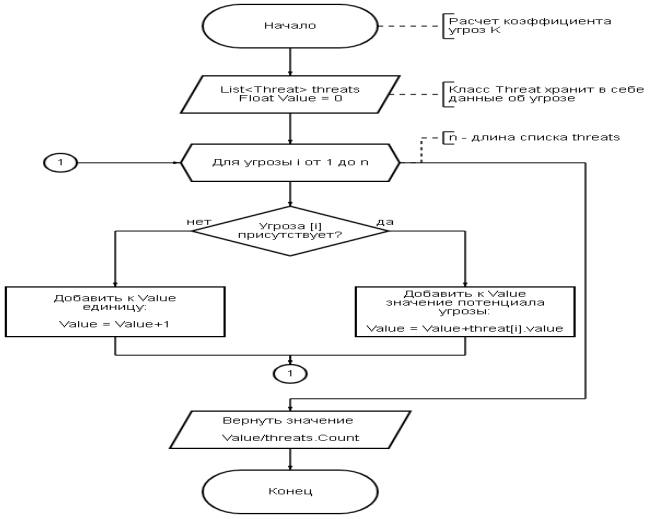

Рис. 2. Алгоритм расчета коэффициента угроз ОС
Fig. 2. Algorithm for calculating the OS threat coefficient

На рис. 3 представлен алгоритм расчета процента соответствия оцениваемой ОС к эталонной ОС.

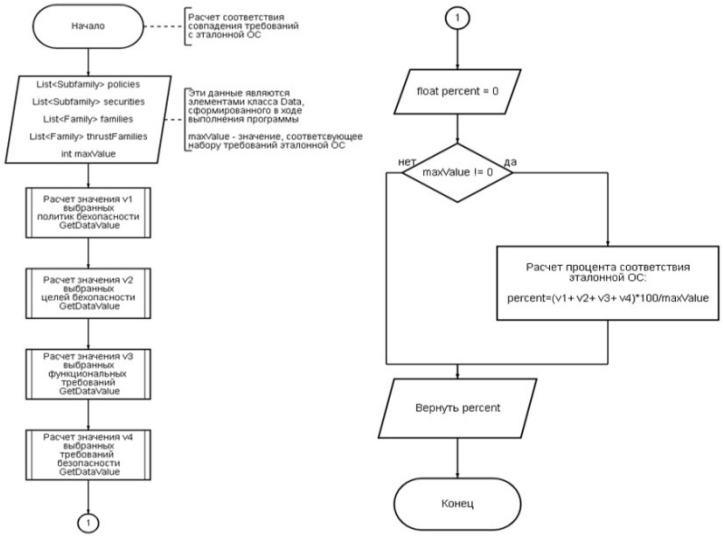

Рис. 3. Алгоритм расчета процента соответствия оцениваемой ОС к эталонной ОС
Fig. 3. Algorithm for calculating the percentage of compliance of the evaluated OS with the reference OS

Стоит отметить, что архитектура программного обеспечения построена на объектно-ориентированном подходе, что отражается в построении классов требований к ОС на основе

абстрактного класса информации «Dataset». Это позволяет универсализировать функцию расчета значений необходимых требований безопасности ОС, в соответствии с ГОСТ Р ИСО/МЭК 15408, а также необходимых политик и целей безопасности соответствующего профиля защиты в функцию «GetDataValue» (рис. 4).

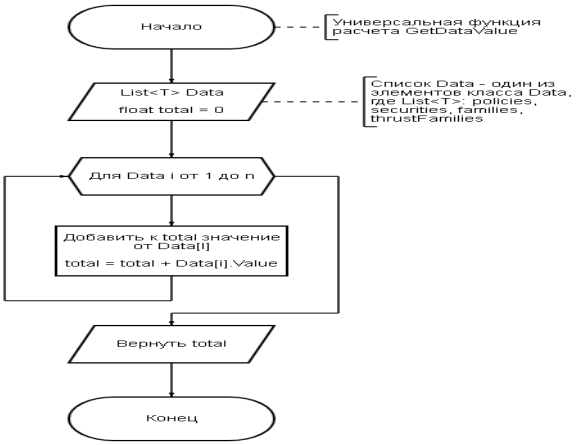

Рис. 4. Алгоритм универсальной функции «GetDataValue»
Fig. 4. Algorithm of the universal function "GetDataValue"

Выходным значением процесса работы алгоритмов, изображенных на рис.3-4, является показатель соответствия, представленный в процентном формате «Percent». В заключительном этапе полученный процент соответствия «Percent» корректируется с учетом коэффициента угроз «K» путем произведения данных показателей. Оценка полученного показателя защищенности ОС производится в соответствии с табл. 1.

Таблица 1. Определение степени защищенности ОС
Table 1. Determining the degree of OS security

Показатель защищенности ОС **OS security indicator**	**Степень защищенности ОС** **OS security level**
$Q_{защ} < 80\%$	Низкая/Low
$80\% \le Q_{защ} \le 90\%$	Средняя/ Average
$Q_{защ} > 90\%$	Высокая/High

Результатом работы автоматизированной системы расчета показателя защищенности анализируемой ОС является один из заданных критериев показателей степени защищенности ОС. Путем сравнения полученного показателя выдается соответствующий результат (рис. 5).

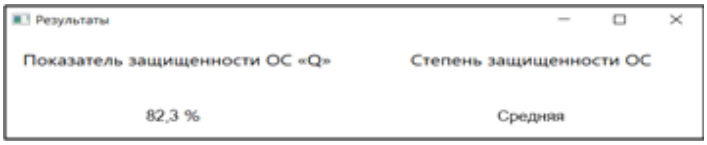

Рис. 5. Результат работы программного обеспечения, предназначенного для оценки защищенности ОС
Fig. 5. The result of the software,designed to assess OS security

Вывод. В статье приводится обобщенная алгоритмизация процессов, необходимых для разработки программного обеспечения для оценки защищенности ОС АИС ОВД РФ, разрабатываемого на основе метода анализа возможных угроз безопасности операционных систем, а также требований стандарта ГОСТ Р ИСО/МЭК 15408.

Изложенный материал не претендует на полноту охвата всех процессов, реализованных в программном обеспечении, однако его вполне достаточно для того, чтобы разобраться и выполнить ту часть названных работ, которая необходима для составления алгоритмов и их описания.

Библиографический список:

1. Банк данных угроз безопасности информации – [Электронный ресурс] – Режим доступа. – URL: https://bdu.fstec.ru/ (Дата обращения: 27.07.2022).

2. Metody i sredstva analiza i otsenki zashchishchennosti avtomatizirovannykh sistem spetsial'nogo naznacheniya na osnove trebovanii k bezopasnosti po GOST R ISO/MEK 15408-2-2013: monografiya/ I.G. Drovnikova, E.A. Rogozin [i dr.]. – Voronezh: VUNTs VVS «VVA», 2020. – 96 s.
3. ГОСТ Р ИСО/МЭК 15408-3-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности [Электронный ресурс] – Режим доступа. – URL: https://docs.cntd.ru/document/1200101777 (Дата обращения: 27.07.2022).
4. А.И. Мифтахова, Э.И. Янгиров, Е.И. Карасева, А.И. Янгиров, Е.Ю. Никулина, И.Г.Дровникова Разработка программно-технического решения для выявления трендов спроса на товары. Вестник Дагестанского государственного технического университета. Технические науки. 2023; 50(1):114-122.
5. Методика оценки угроз безопасности информации: Методический документ ФСТЭК России от 05.02.2021 // Информационно-правовой портал системы КонсультантПлюс. – Режим доступа: http://base.consultant.ru (дата обращения: 27.10.2022).
6. Банк данных угроз безопасности информации: [Электронный ресурс]. ФСТЭК России. URL: https://bdu.fstec.ru/. (Дата обращения: 27.10.2022).
7. ФСТЭК РФ. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения.

References

1. Bank dannykh ugroz bezopasnosti informatsii – [Elektronnyi resurs] – Rezhim dostupa. – URL: https://bdu.fstec.ru/ (Data obrashcheniya: 27.07.2022).
2. Методы и средства анализа и оценки защищенности автоматизированных систем специального назначения на основе требований к безопасности по ГОСТ Р ИСО/МЭК 15408-2-2013: монография / И.Г. Дровникова, Е.А. Рогозин [и др.]. – Воронеж: ВУНЦ ВВС «ВВА», 2020. – 96 с.
3. GOST R ISO/MEK 15408-3-2002. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti informatsionnykh tekhnologii. Chast' 3. Trebovaniya doveriya k bezopasnosti [Elektronnyi resurs] – Rezhim dostupa. – URL: https://docs.cntd.ru/document/ 1200101777 (Data obrashcheniya: 27.07.2022).
4. A.I. Miftakhova, E.I. Yangirov, E.I. Karaseva, A.I. Yangirov, E.Yu. Nikulina, I.G. Drovnikova. Development of a software and hardware solution to identify trends in demand for goods. Herald of the Daghestan State Technical University. Technical Science. 2023; 50(1):114-122.
5. Methodology for assessing threats to information security: Methodological document of the FSTEC of Russia dated 02/05/2021 // Information and legal portal of the ConsultantPlus system. – Access mode: http://base.consultant.ru (date of access: 10/27/2022).FSTEC of the Russian Federation. Guidance document. Protection against unauthorized access to information. Terms and definitions. (In Russ)
6. Data bank of information security threats: [Electronic resource]. FSTEC of Russia. URL: https://bdu.fstec.ru/. (Date of access: 27.10.2022). (In Russ)
7. FSTEC RF. Management document. Protection against unauthorized access to information. Terms and Definitions.

Сведения об авторах:

Янгиров Адиль Илдарович, начальник отделения лабораторных исследований и испытаний; adil-yan@yandex.ru

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

Бокова Оксана Игоревна, доктор технических наук, профессор; научно-технический консультант; o.i.bokova@gmail.com

Ахлюстин Сергей Борисович, кандидат технических наук, начальник кафедры тактико-специальной подготовки; cerg7676@yandex.ru

Information about authors:

Adil I. Yangirov, Head of the Laboratory Research and Testing Department; adil-yan@yandex.ru

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

Oksana I. Bokova, Dr. Sci. (Eng), Prof.; Scientific and Technical consultant; o.i.bokova@gmail.com

Sergey B. Akhlyustin, Cand. Sci. (Eng), Head of the Department of Tactical and Special Training; cerg7676@yandex.ru

Конфликт интересов/Conflict of interest.

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

Поступила в редакцию/Received 01.09.2023.

Одобрена после рецензирования/ Reviced 10.09.2023.

Принята в печать/Accepted for publication 10.09.2023.