Для цитирования: *А.В. Бацких, В.В.Конобеевских, С.В. Ефимов. Способы оценки эффективности функционирования подсистем управления доступом на объектах информатизации органов внутренних дел и аспекты их совершенствования. Вестник Дагестанского государственного технического университета. Технические науки. 2021; 48(2): 29-39. DOI:10.21822/2073-6185-2021-48-2-29-39*
For citation: *A.V. Batskikh, V.V. Konobeevskikh, S.V. Efimov. Methods for assessing the efficiency of access control subsystems at informatization facilities of internal affairs bodies and aspects of their improvement. Herald of Daghestan State Technical University. Technical Sciences. 2021; 48 (2): 29-39. (In Russ.) DOI:10.21822/2073-6185-2021-48-2-29-39*

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

УДК 621.3
DOI: 10.21822/2073-6185-2021-48-2-29-39

СПОСОБЫ ОЦЕНКИ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ПОДСИСТЕМ УПРАВЛЕНИЯ ДОСТУПОМ НА ОБЪЕКТАХ ИНФОРМАТИЗАЦИИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ И АСПЕКТЫ ИХ СОВЕРШЕНСТВОВАНИЯ

А.В. Бацких, В.В Конобеевских, С.В. Ефимов
Воронежский институт МВД России,
394065, г. Воронеж, пр. Патриотов, 53, Россия

Резюме. Цель. *Целью исследования является анализ существующего методического обеспечения, используемого при оценивании эффективности функционирования систем защиты информации от несанкционированного доступа в автоматизированные системы, на основе исследования открытых литературных источников, международных и отраслевых стандартов РФ по информационной безопасности АС, руководящих документов и приказов Федеральной службы по техническому и экспортному контролю России, а также ведомственных приказов, инструкций и нормативных актов. Результатом анализа является выявление достоинств и недостатков указанного методического обеспечения, а также возможностей его использования при проведении количественной оценки эффективности функционирования подсистем управления доступом систем защиты информации от несанкционированного доступа на объектах информатизации органов внутренних дел.* ***Метод.*** *Применен метод системного анализа подходов, используемых при оценивании эффективности средств и систем обеспечения информационной безопасности.* ***Результат.*** *Представлены результаты анализа основных подходов, используемых при оценивании эффективности средств и систем обеспечения информационной безопасности автоматизированных систем. Определена связь показателя эффективности функционирования подсистем управления доступом систем защиты информации от несанкционированного доступа с основным недостатком их применения в защищенных автоматизированных системах органов внутренних дел. Обоснованы основные направления совершенствования существующего методического обеспечения, предложены способы и показатели для проведения количественной оценки эффективности функционирования подсистем управления доступом (в том числе модифицированных на основе использования новых информационно-коммуникационных технологий).* ***Вывод.*** *Полученные результаты могут быть использованы для проведения количественной оценки защищенности существующих и разрабатываемых автоматизированных систем на объектах информатизации органов внутренних дел.*

Ключевые слова: *автоматизированная система, система защиты информации, подсистема управления доступом, несанкционированный доступ, показатель эффективности, количественная оценка эффективности*

METHODS FOR ASSESSING THE EFFICIENCY OF ACCESS CONTROL SUBSYSTEMS AT INFORMATIZATION FACILITIES OF INTERNAL AFFAIRS BODIES AND ASPECTS OF THEIR IMPROVEMENT

A.V. Batskikh, V.V. Konobeevskikh, S.V. Efimov
Voronezh Institute of the Ministry of Internal Affairs of Russian Federation,
53 Patriotov Ave., Voronezh 394065, Russia

Abstract. Objective. *The purpose of the article is to analyse the existing methodology used to assess the efficiency of automated information security systems by studying open literature sources, international and industry standards of the Russian Federation on information security of automated systems, guidelines and orders of the Federal Service for Technical and Expert Control of Russia, as well as departmental orders, instructions and regulations on information security at informatization facilities of internal affairs bodies. The analysis results in identifying the advantages and disadvantages of the specified methodology, as well as the possibilities of its use when conducting a quantitative assessment of the efficiency of access control subsystems of information security systems at the informatization facilities of internal affairs bodies.* ***Methods.*** *To achieve this goal, the method for system analysis of approaches used to assess the efficiency of information security tools and systems has been applied.* ***Results.*** *The paper presents results of analysing the main approaches used to assess the efficiency of tools and systems for information security of automated systems. The paper determines the relationship between the efficiency indicator of access control subsystems of information security systems and the main disadvantage of their use in protected automated systems of internal affairs bodies. The paper substantiates main directions of improving the existing methodology, proposes methods and indicators for quantifying the efficiency of access control subsystems (including those modified on the basis of using new information and communication technologies) of information security systems in protected automated systems of internal affairs bodies.* ***Conclusion.*** *The results obtained can be used to quantify the security level of existing automated systems and those being developed at informatization facilities of internal affairs bodies.*

Keywords: *automated system, information security system, access control subsystem, unauthorized access, efficiency indicator, efficiency quantification*

Введение. Проблема оценивания эффективности функционирования подсистем управления доступом систем защиты информации (СЗИ) от несанкционированного доступа (НСД) в защищенные автоматизированные системы (АС) органов внутренних дел (ОВД) является одним из ключевых вопросов формирования требований по идентификации и аутентификации штатных пользователей как составной части общих требований по защите информации (ЗИ) в АС, эксплуатируемых на объектах информатизации ОВД [1-3]. Оценивание эффективности функционирования подсистемы управления доступом СЗИ от НСД в АС ОВД необходимо проводить: при разработке СЗИ от НСД; при ее входном и периодическом контроле; при приемке; при сертификации, а также при аттестации объекта информатизации, эксплуатирующего защищенную АС ОВД в целом [4-5].

В приказе МВД России от 14.03.2012 № 169 «Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года» определены цели, задачи, принципы и основные направления обеспечения информационной безопасности (ИБ) ОВД. Одним из механизмов реализации Концепции является разработка критериев и методов оценки эффективности систем обеспечения ИБ ОВД, однако конкретная методика оценки эффективности функционирования СЗИ от НСД в АС, а тем более их подсистем, в приказе не рассматривается [3]. В то же время, данный документ во многом подтверждает актуальность проблемы оценивания эффективности как СЗИ от НСД в целом, так и их отдельных подсистем и определяет перспективные аспекты научных исследований в данной области применительно к объектам информатизации, эксплуатирующим защищенные АС ОВД.

В связи с недостаточностью научных исследований, посвященных разработке методов и процедур оценки эффективности функционирования отдельных подсистем СЗИ от НСД в АС ОВД, проанализируем способы и показатели, используемые в настоящее время при оценивании эффективности функционирования СЗИ от НСД в АС с целью выявления их достоинств и недостатков, а также возможностей применения при проведении количественной оценки эффективности функционирования подсистем управления доступом СЗИ от НСД на объектах информатизации ОВД.

Постановка задачи. Для реализации поставленной цели необходимо решить следующие задачи:

1. Проанализировать открытые литературные источники, международные и отраслевые стандарты Российской Федерации по ИБ АС, руководящие документы и приказы ФСТЭК России, а также ведомственные приказы, инструкции и нормативные акты по вопросам ЗИ от НСД на объектах информатизации ОВД.

2. Определить основные аспекты совершенствования существующего методического обеспечения, используемого при оценивании эффективности функционирования СЗИ от НСД в АС, с целью проведения количественной оценки эффективности функционирования подсистем управления доступом (в том числе модифицированных на основе использования новых информационно-коммуникационных технологий) СЗИ от НСД в защищенных АС на объектах информатизации ОВД.

Методы исследования. Методологической основой исследования является системный анализ подходов, используемых при оценивании эффективности средств и систем обеспечения ИБ. Согласно [6] эффективность программных средств (ПСр) трактуется как совокупность свойств ПСр, характеризующая аспекты его уровня пригодности, связанные с характером и временем использования ресурсов (других ПСр, технических средств, материалов, услуг различных категорий персонала), необходимых при заданных условиях функционирования. Приведенные в [6] термины и определения справедливы не только для ПСр, но и для программных систем, их объединяющих, к которым в полной мере можно отнести и СЗИ от НСД в АС ОВД.

В стандартах [6-8] представлены иерархические модели качества ПСр, приведены термины и определения характеристик и рассмотрены примеры подхарактеристик их качества, позволяющие оценивать качество и эффективность ПСр (включая и ПСр ЗИ), задавая иерархию характеристик и подхарактеристик качества. В данном случае эффективность ПСр рассматривается как одна из характеристик их качества.

С учетом выше изложенного и в соответствии с [9-11] эффективность функционирования СЗИ от НСД при эксплуатации АС ОВД в защищенном исполнении можно определить, как степень соответствия результатов защиты конфиденциальной информации поставленной цели защиты или степень решения поставленной совокупности задач ЗИ.

Таким образом, эффективность функционирования СЗИ от НСД может оцениваться как относительно заранее определенных и декларированных для конкретной АС ОВД задач защиты, которые должны выполняться ее СЗИ, так и относительно всех задач защиты, сформулированных для данной АС ОВД. Для частичного парирования такой условности на практике используются три основных подхода при оценивании эффективности, основанные на унификации целей и задач ЗИ (табл. 1), однако ни один из них не позволяет парировать указанную условность в полной мере, что обусловлено относительностью, присущей самому понятию «эффективность» [9, 8, 12-14].

Таблица 1. Основные подходы, используемые при оценивании эффективности средств и систем обеспечения информационной безопасности автоматизированных систем
Table 1. The main approaches used in assessing the effectiveness of tools and systems for ensuring information security of automated systems

№	Характеристика подхода Characteristics of the approach	Способ реализации подхода How to implement the approach
1	Основан на определении соответствия средств и систем обеспечения информационной безопасности сформированным требованиям. Based on determining the compliance of information security tools and systems with the formed requirements	Требования по ЗИ задаются в виде перечня механизмов ЗИ, которые необходимо иметь в АС для ее соответствия определенному уровню (классу) защищенности [15, 16] Requirements for RFI are set in the form of a list of RFI mechanisms that must be in the AS for its compliance with a certain level (class) of security [15, 16]
		Требования по ЗИ задаются в виде перечня функций, которые необходимо выполнить для достижения определенного уровня (класса) защищенности информации в АС [1, 17] Requirements for IS are set in the form of a list of functions that must be performed to achieve a certain level (class) of information security in the AU [1, 17]
2	Основан на экспертных суждениях о достижении средствами и системами обеспечения ИБ цели ЗИ. Based on expert judgments about the achievement of IS goals by means and systems of information security.	Результаты экспертного опроса специалистов обрабатываются и представляются в виде балльной оценки, которая интерпретируется в виде суждений об эффективности принятых мер защиты [9, 10, 18] The results of the expert survey of specialists are processed and presented in the form of a score, which is interpreted in the form of judgments about the effectiveness of the protection measures taken [9, 10, 18]
3	Основан на математическом моделировании процессов функционирования средств и систем обеспечения ИБ. Based on mathematical modeling of the functioning of information security tools and systems.	Для оценивания эффективности средств и систем обеспечения ИБ в АС используются соответствующие критерии и показатели, определяемые с помощью применяемых для этих целей математических методов и моделей [4, 11, 19, 20] To assess the effectiveness of the means and systems for ensuring IS in the nuclear power plant, the corresponding criteria and indicators are used, which are determined using the mathematical methods and models used for these purposes [4, 11, 19, 20]

Первый подход (оценочный), используемый при оценивании эффективности средств и систем обеспечения ИБ, получивший широкое распространение для оценивания эффективности функционирования СЗИ от НСД в АС (в том числе и в АС ОВД), заключается в формировании требований по защите, выполнение которых будет свидетельствовать о достаточности принятых мер [1, 15-17]. При этом целью защиты станет достижение условий, обеспечивающих выполнение указанных требований. В данном случае эффективность защиты является мерой приближения к заданным условиям.

Указанный подход реализуется в двух вариантах, но наибольшую популярность получил так называемый «функциональный» вариант, при котором требования по ЗИ в АС задаются в виде перечня функций, выполнение которых необходимо для достижения определенного уровня защищенности информации [1, 17]. Уровень защищенности (в качестве таких уровней могут рассматриваться классы защищенности АС) чаще всего устанавливается декларативно экспертным путем. ЗИ считается эффективной, если выполняются все функции, соответствующие заданному уровню защищенности информации (так называемые «функции безопасности» (ФБ)) [9, 10].

Основным недостатком «функционального» варианта является проведение, по сути, «бинарной оценки», при которой не оценивается эффективность конкретных ФБ, а констатируется лишь факт ее наличия или отсутствия при реализации данных функций сертифицированными ПСр [20]. При этом происходит подмена понятия эффективности понятием достаточно-

сти принятых мер защиты, что не является мерой приближения к поставленной цели защиты [9].

Сущность второго подхода (экспертного), используемого при оценивании эффективности средств и систем обеспечения ИБ, заключается в том, что факту достижения цели защиты ставится в соответствие ряд экспертных суждений с использованием некоторой качественной шкалы, которая затем переводится в балльную шкалу [9, 10, 18]. Набранные баллы суммируются (или перемножаются).

Решение о достаточности принятых мер защиты принимается при превышении полученной суммой (произведением) баллов определенного порога. Каждому значению суммы (произведения) ставится в соответствие определенное суждение об эффективности защиты. В этом случае сумма (или произведение) баллов рассматривается как мера эффективности [9, 10].

Данный подход реализуется применением балльного метода оценки эффективности ЗИ, основанного на опросе экспертов-специалистов, обработке полученных результатов и выдаче в виде баллов с последующей интерпретацией полученной балльной оценки в виде суждений об эффективности принятых мер защиты.

Указанный метод реализован в целом ряде международных стандартов и программных продуктов, таких как ISO/IEC 27002:2005-2013 [18] и его инструментарии — программном продукте COBRA, программном продукте Risk Watch, программном продукте, реализующем широко используемый в настоящее время метод CRAMM, и др. [9].

Очевидным недостатком изложенных подходов применительно к оцениванию эффективности функционирования подсистем управления доступом СЗИ от НСД в АС ОВД является их недостаточная точность, обусловленная экспертным участием в процессе оценивания.

Указанных выше недостатков лишен третий подход (вероятностный), используемый при оценивании эффективности, основанный на математическом моделировании (аналитическом, имитационном) процессов функционирования средств и систем обеспечения ИБ в АС. В рассматриваемых методах оценки применяются различные критерии и показатели эффективности, методики их расчета и критерии оптимальности [4, 5, 9-11, 19, 20].

Данный подход используется для описания случайных событий, в частности, на основе определения их вероятностно-временных характеристик (ВВХ), что дает возможность проводить количественную оценку эффективности средств и систем обеспечения ИБ в АС и исследовать их в динамическом (временном) режиме функционирования [11, 18, 20-23].

Поскольку функционирование СЗИ от НСД в АС представляет собой сложный динамический процесс для его описания в настоящее время широко применяются модели, построенные на сетях Петри-Маркова (основанные на теории сетей Петри и марковских (полумарковских) процессах), что позволяет определять ВВХ функционирования СЗИ от НСД [9-11, 24-27].

Вероятностный подход, как и предыдущие два подхода, используется при оценивании эффективности функционирования СЗИ от НСД в целом как сложной программной системы. В то же время некоторые из предложенных методик [11, 17] могут быть применены и при оценивании эффективности функционирования отдельных подсистем СЗИ от НСД (включая подсистему управления доступом) в защищенных АС, эксплуатируемых на объектах информатизации ОВД, при условии совершенствования существующего математического обеспечения оценки эффективности путем введения ВВХ отдельных состояний функционирования СЗИ от НСД с использованием обратного преобразования Лапласа.

Обсуждение результатов. Задачи анализа, обоснования и разработки показателей эффективности функционирования СЗИ от несанкционированного доступа применительно к проектированию и управлению процессами ЗИ в АС не являются новыми и решены в ряде науч-

ных работ [12, 14, 19-22]. Под показателем эффективности функционирования понимается мера степени соответствия реального и требуемого результатов функционирования СЗИ от НСД [11].

В [11] проведен достаточно подробный анализ вариантов выбора атрибутов (показателей) эффективности функционирования СЗИ от несанкционированного доступа в АС, смысловые значения которых принципиально схожи.

Исследуя процесс функционирования СЗИ от несанкционированного доступа в АС на трех уровнях (концептуальном, операционном, детальном), автором предложена система частных показателей эффективности функционирования данной сложной (иерархической) программной системы, учитывающих реально существующие недостатки эксплуатации защищенных АС на объектах информатизации ОВД, и обосновано введение агрегирующего их интегрального показателя эффективности.

Опыт эксплуатации современных АС на объектах информатизации ОВД показал, что из указанных в [11] недостатков их эксплуатации максимальное влияние на эффективность функционирования подсистем управления доступом СЗИ от несанкционированного доступа оказывает непосредственная зависимость ресурсоемкости СЗИ от несанкционированного доступа от вычислительного ресурса АС (процессорного времени, оперативной памяти, дискового пространства).

Использование новых информационно-телекоммуникационных технологий с целью повышения реальной защищенности современных АС в процессе их эксплуатации на объектах информатизации ОВД не должно усугублять указанный недостаток.

В качестве одной из таких технологий применительно к подсистеме управления доступом СЗИ от несанкционированного доступа в АС ОВД предлагается дополнительная биометрическая аутентификация, основанная на распознавании субъекта доступа по индивидуальной динамике клавиатурного набора (клавиатурному почерку).

Управление функциональностью доработанной (модифицированной) подсистемы управления доступом СЗИ от несанкционированного доступа в АС ОВД за счет усложнения процедуры аутентификации штатных пользователей (в первую очередь, при обращении к особо важному информационному ресурсу) и сокращения необходимого для ее реализации временного диапазона обеспечит достижение требуемого уровня защищенности конфиденциальной информации без нарушения эффективности функционирования АС ОВД по прямому назначению.

В соответствии с выше изложенным в качестве показателя эффективности функционирования подсистемы управления доступом СЗИ от несанкционированного доступа в защищенных АС, эксплуатируемых на объектах информатизации ОВД, целесообразно использовать напрямую зависимый от времени динамический показатель временной эффективности $V_{\text{ВЭ ПУД}}$, под которым согласно [7] понимается способность программы выполнять заданные действия в интервал времени, отвечающий заданным требованиям.

Взаимосвязь данного показателя и выявленного недостатка функционирования АС в защищенном исполнении на объектах информатизации ОВД представлена в табл. 2.

Таким образом, $V_{\text{ВЭ ПУД}}$ отражает спектр свойств подсистемы управления доступом (в том числе модифицированного варианта) с учетом динамики ее функционирования. Задачу оценивания $V_{\text{ВЭ ПУД}}$ в математическом виде можно представить как нахождение отображения F: $V_{\text{ВЭ ПУД}} \rightarrow \{0,1\}$, где F определяет правила, реализуемые соответствующими моделями и алгоритмами.

Таблица 2. Связь показателя эффективности функционирования подсистем управления доступом СЗИ от НСД с основным недостатком его применения в защищенных АС ОВД

Table 2. Relationship between the efficiency indicator of the functioning of the access control subsystems of the information security system from the unauthorized access system with the main disadvantage of their use in protected ATS AS

Показатель Indicator	$V_{ВЭ\ ПУД}$ — временная эффективность функционирования подсистемы управления доступом СЗИ от НСД $V_{ВЭ\ ПУД}$ — temporal efficiency of the functioning of the access control subsystem of the information security system from the unauthorized access system.
Смысловое значение показателя Semantic value of the indicator	Способность подсистемы управления доступом соответствовать заявленным требованиям (с точки зрения временных параметров ее функционирования), а также находить разумный компромисс (эффективное решение), связанный с совместным функционированием СЗИ от несанкционированного доступа и АС ОВД по ее прямому функциональному назначению (обработка, хранение и передача конфиденциальной информации). The ability of the access control subsystem to meet the stated requirements (in terms of the time parameters of its functioning), as well as find a reasonable compromise (effective solution) associated with the joint operation of the information security system from the NSD and the ATS AS according to its direct functional purpose (processing, storage and transmission of confidential information).
Недостаток Flaw	Непосредственная зависимость ресурсоемкости СЗИ от НСД от вычислительного ресурса АС. Direct dependence of the resource intensity of the information security system on the NSD on the computing resource of the AS
Смысловое значение недостатка The semantic meaning of lack	Выполнение СЗИ от НСД защитных функций осуществляется в процессе функционирования АС ОВД в защищенном исполнении, что приводит к снижению производительности системы за счет использования процедурой защиты части вычислительного ресурса АС в ущерб реализации ее целевых функций. Ограниченность вычислительного ресурса АС ОВД влечет за собой увеличение времени реализации СЗИ от НСД защитных функций и, как следствие, наблюдается несоответствие используемой СЗИ предъявляемым к ней требованиям по ЗИ. The implementation of the security information system from the unauthorized system of protective functions is carried out in the process of functioning of the ATS AS in a protected version, which leads to a decrease in the performance of the system due to the use of the procedure for protecting a part of the computing resource of the AS to the detriment of the implementation of its target functions. The limited computing resource of the ATC AS entails an increase in the time for the implementation of the ISS from the NSD of protective functions and, as a consequence, there is a discrepancy between the ISS used and the IS requirements for it.

Вывод. Таким образом, анализ научно-технической литературы по проблеме оценивания эффективности функционирования средств и систем обеспечения ИБ [4, 5, 9-11, 19, 20], международных и отраслевых стандартов РФ по ИБ АС [1, 6-8, 17, 18], руководящих документов и приказов Федеральной службы по техническому и экспортному контролю (ФСТЭК) России [2, 15, 16], а также ведомственных нормативных актов по вопросам ЗИ на объектах информатизации ОВД [3] выявил ряд вопросов, требующих безотлагательного решения применительно к подсистеме управления доступом СЗИ от НСД с целью повышения реальной защищенности АС на объектах информатизации ОВД:

– практически отсутствуют показатели эффективности и методики количественной оценки эффективности функционирования подсистем управления доступом СЗИ от НСД в защищенных АС ОВД;

– существующие показатели эффективности и методики количественной оценки эффективности ПСр и систем обеспечения ИБ, как правило, не отражают реальные недостатки эксплуатации защищенных АС на объектах информатизации ОВД, а, следовательно, не применимы при оценивании эффективности их функционирования;

– показатели эффективности и методики, разработанные для оценки эффективности функционирования СЗИ от НСД с учетом реально существующих недостатков эксплуатации защищенных АС ОВД, позволяют количественно оценивать эффективность функционирования СЗИ от НСД в целом как сложной программной системы, но не могут быть применены при оценивании эффективности функционирования отдельных ее подсистем (включая подсистему управления доступом);

– для повышения реальной защищенности современных АС в процессе их эксплуатации на объектах информатизации ОВД целесообразно доработать существующие подсистемы управления доступом СЗИ от НСД на основе использования новых информационно-телекоммуникационных технологий;

– для проведения количественной оценки эффективности функционирования подсистем управления доступом СЗИ от НСД в защищенных АС, эксплуатируемых на объектах информатизации ОВД, требуются: разработка динамического показателя временной эффективности, отражающего реальные динамические свойства подсистемы управления доступом (в том числе ее модифицированного варианта); совершенствование существующего математического обеспечения оценки эффективности путем введения вероятностно-временных характеристик отдельных состояний функционирования СЗИ от НСД с использованием обратного преобразования Лапласа.

Библиографический список:

1. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2: Функциональные компоненты безопасности [Электронный ресурс]. URL:https://files.stroyinf.ru/Data2/1/4293774/4293774728.pdf (дата обращения: 28.02.2020).
2. ФСТЭК России. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации [Электронный сурс]. URL:http://fstec.ru/component/attachments/ download/299 (дата обращения: 28.02.2020).
3. 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: 02.03.2020).
4. Методики оценки надежности систем защиты информации от несанкционированного доступа автоматизированных систем / Бокова О.И. [и др.] // Труды СПИИ РАН. Т. 18 № 6 (2019). С.-Пб.: СПИИРАН, 2019. 2019. Т. 18. № 6. С. 1300-1331. SSN 2078-918. DOI 10.15622/sp.2019.18.6.
5. Дровникова И.Г. Численные методы расчета показателя эффективности вспомогательной подсистемы в системе электронного документооборота / И.Г. Дровникова, П.В. Зиновьев, Е.А. Рогозин // Вестник Воронеж. ин-та МВД России. 2016. № 4. С. 114-121.
6. ГОСТ 28806-89. Качество программных средств. Термины и определения [Электронный ресурс]. URL:http://www.kimmeria.nw.ru/standart/glosys/gost_28806_90.pdf (дата обращения: 03.03.2020).
7. ГОСТ 28195-89. Оценка качества программных средств. Общие положения [Электронный ресурс]. URL:http://docs.cntd.ru/document/1200009135 (дата обращения: 05.03.2020).
8. ГОСТ Р ИСО/МЭК 9126-93. Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению [Электронный ресурс]. URL:http://docs.cntd.ru/document/gost-r-iso-mek-9126-93 (дата обращения 05.03.2020).
9. Радько Н.М. Проникновения в операционную среду компьютера: модели злоумышленного удаленного доступа: учеб. пособие / Н.М. Радько, Ю.К. Язов, Н.Н. Корнеева. Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет», 2013. 265 с.
10. Радько Н.М. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа / Н.М. Радько, И.О. Скобелев. М: РадиоСофт, 2010. 232 с.
11. 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.
12. 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. pp. 869-873.

13. 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: 06.03.2020).

14. 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.

15. ФСТЭК России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации [Электронный ресурс]. URL:http://fstec.ru/ tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g (дата обращения: 06.03.2020).

16. ФСТЭК России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации [Электронный ресурс]. URL:https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g (дата обращения: 10.03.2020).

17. ISO/IEC 17000:2004. Conformity assessment. Dictionary and General principles [Электронный ресурс]. — URL:https://pqm-online.com/assets/files/ lib/std/iso_17000-2004.pdf (дата обращения: 10.03.2020).

18. ISO/IEC 27002:2005-2013. Information technology. Security method. Practical rules of information security management [Электронный ресурс]. URL:http://docs.cntd.ru/ document/gost-r-iso-mek-17799-2005 (дата обращения 10.03.2020).

19. Разработка моделей и алгоритмов оценки эффективности подсистемы защиты конфиденциальных сведений при ее проектировании в системах электронного документооборота ОВД: монография [Электронный ресурс] / Дровникова И.Г. [и др.]. Воронеж: Воронеж. ин-т МВД России, 2019. 116 с.

20. Застрожнов И.И. Моделирование и исследование динамики функционирования программных систем защиты информации для оценки и анализа качества их функционирования при проектировании и управлении: дис. ... канд. техн. наук: 05.13.18 / Застрожнов Игорь Иванович. Воронеж, 2005. 181 с.

21. Korniyenko B.Y. Design and research of mathematical model for information security system in computer network / B.Y. Korniyenko, L.P. Galata // Science-Based Technologies. 2017. Vol. 34. Issue 2. pp. 114–118.

22. Nazareth D. System dynamics model for information security management / D. Nazareth, J. Choi // Information & Management. 2015. Vol. 52. Issue 1. pp. 123–134.

23. Kresimir S. The information systems' security level assessment model based on an ontology and evidential reasoning approach / S. Kresimir, O Effectiveness Evaluation on Cyberspace Security Defense System. Hrvoje, G. Marin // Computers & Security. 2015. pp. 100-112.

24. White S.C. Comparison of Security Models: Attack Graphs Versus Petri Nets / S.C. White, S.S. Sarvestani // Advances in Computers. 2014. Vol. 94. pp. 1–24.

25. Nikishin K. Implementation of time-triggered ethernet using colored Petri NET / K. Nikishin, N. Konnov, D. Pashchenko // International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM). 2017. pp. 1–5.

26. Charaf H. A colored Petri-net model for control execution of distributed systems / H. Charaf, S. Azzouzi // 4th International Conference on Control, Decision and Information Technologies (CoDIT). 2017. pp. 277-282.

27. Network security analyzing and modeling based on Petri net and Attack tree for SDN / Y. Linyuan [and others] // 2016 International Conference on Computing, Networking and Communications (ICNC). 2016. pp. 133-187.

References:

1. GOST R ISO/MEK 15408-2-2013. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti informatsionnykh tekhnologiy. Chast' 2: Funktsional'nyye komponenty bezopasnosti [GOST R ISO / IEC 15408-2-2013. Information technology. Methods and means of ensuring safety. Criteria for assessing the security of information technology. Part 2: Functional components of security [Electronic resource]. URL: https: //files.stroyinf.ru/Data2/1/4293774/4293774728.pdf (date accessed: 02/28/2020). (In Russ)]
2. FSTEK Rossii. Rukovodyashchiy dokument. Kontseptsiya zashchity sredstv vychislitel'noy tekhniki i avtomatizirovannykh sistem ot nesanktsionirovannogo dostupa k informatsii [Elektronnyy resurs]. [FSTEC of Russia. Guidance document. The concept of protection of computer technology and automated systems from unauthorized access to information [Electronic resource]. URL: http: //fstec.ru/component/attachments/ download / 299 (date accessed: February 28, 2020). (In Russ)]
3. Ob utverzhdenii Kontseptsii obespecheniya informatsionnoy bezopasnosti organov vnutrennikh del Rossiyskoy Federatsii do 2020 goda: prikaz MVD Rossii ot 14.03.2012 № 169 [Elektronnyy resurs]. [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: 03/02/2020). (In Russ)]
4. Metodiki otsenki nadezhnosti sistem zashchity informatsii ot nesanktsionirovannogo dostupa avtomatizirovannykh sistem / Bokova O.I. [i dr.] [Methods for assessing the reliability of information protection systems against unauthorized access of automated systems / Bokova OI. [and others] // Proceedings of the SPII RAS. Vol.

18 No. 6 (2019). S.-Pb .: SPIIRAS, 2019.2019.T. 18.No. 6.pp. 1300-1331. SSN 2078-918. DOI 10.15622 / sp.2019.18.6. (In Russ)]

5. Drovnikova I.G. Chislennyye metody rascheta pokazatelya effektivnosti vspomogatel'noy podsistemy v sisteme elektronnogo dokumentooborota [Drovnikova I.G. Numerical methods for calculating the efficiency indicator of the auxiliary subsystem in the electronic document management system / I.G. Drovnikova, P.V. Zinoviev, E.A. Rogozin // Bulletin Voronezh. Institute of the Ministry of Internal Affairs of Russia. 2016. No. 4. S. 114-121. (In Russ)]
6. GOST 28806-89. Kachestvo programmnykh sredstv. Terminy i opredeleniya [Elektronnyy resurs]. [GOST 28806-89. The quality of the software. Terms and definitions [Electronic resource]. URL: http://www.kimmeria.nw.ru/standart/glosys/gost_28806_90.pdf (date accessed: 03.03.2020). (In Russ)]
7. GOST 28195-89. Assessment of the quality of software. General provisions [Electronic resource]. URL: [GOST 28195-89. Otsenka kachestva programmnykh sredstv. Obshchiye polozheniya [Elektronnyy resurs]. URL:http://docs.cntd.ru/document/1200009135 (data obrashcheniya: 05.03.2020). http: //docs.cntd.ru/document/1200009135 (date accessed: 03/05/2020). (In Russ)]
8. GOST R ISO/MEK 9126-93. Informatsionnaya tekhnologiya. Otsenka programmnoy produktsii. Kharakteristiki kachestva i rukovodstva po ikh primeneniyu [GOST R ISO / IEC 9126-93. Information technology. Evaluation of software products. Quality characteristics and guidelines for their application [Electronic resource]. URL: http: //docs.cntd.ru/document/gost-r-iso-mek-9126-93 (date of treatment 03/05/2020). (In Russ)]
9. Rad'ko N.M. Proniknoveniya v operatsionnuyu sredu komp'yutera: modeli zloumyshlennogo udalennogo dostupa: ucheb. posobiye / N.M. Rad'ko, YU.K. YAzov, N.N. Korneyeva. Voronezh: FGBOU VPO «Voronezhskiy gosudarstvennyy tekhnicheskiy universitet», 2013. 265 s. [Radko N.M. Penetration into the operating environment of a computer: models of malicious remote access: textbook. allowance / N.M. Radko, Yu.K. Yazov, N.N. Korneeva. Voronezh: Voronezh State Technical University, 2013.265 p. (In Russ)]
10. Rad'ko N.M. Risk-modeli informatsionno-telekommunikatsionnykh sistem pri realizatsii ugroz udalennogo i neposredstvennogo dostupa / N.M. Rad'ko, I.O. Skobelev. M: RadioSoft, 2010. 232 s. [Radko N.M. Risk-models of information and telecommunication systems in the implementation of threats of remote and direct access / N.M. Radko, I.O. Skobelev. M: RadioSoft, 2010.232 p. (In Russ)]
11. Popov A.D. Modeli i algoritmy otsenki effektivnosti sistem zashchity informatsii ot nesanktsionirovannogo dostupa s uchetom ikh vremennykh kharakteristik v avtomatizirovannykh sistemakh organov vnutrennikh del: dis. ... kand. tekhn. nauk: 05.13.19 / Popov Anton Dmitriyevich. Voronezh, 2018. 163 s. [Popov A.D. Models and algorithms for evaluating the effectiveness of information protection systems against 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)]
12. 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. 869-873.
13. 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: 03/06/2020).
14. 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.
15. FSTEK Rossii. Rukovodyashchiy dokument. Sredstva vychislitel'noy tekhniki. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Pokazateli zashchishchennosti ot nesanktsionirovannogo dostupa k informatsii [Elektronnyy resurs]. [FSTEC of Russia. Guidance document. Computer facilities. Protection against unauthorized access to information. Indicators of security against unauthorized access to information [Electronic resource]. URL: http: //fstec.ru/ tekhnicheskaya-zashchita-informatsii / dokumenty / 114-spetsialnye-normativnye-dokumenty / 383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-otlya-25-iyu date of access: 03/06/2020). (In Russ)]
16. FSTEK Rossii. Rukovodyashchiy dokument. Avtomatizirovannyye sistemy. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Klassifikatsiya avtomatizirovannykh sistem i trebovaniya po zashchite informatsii [Elektronnyy resurs]. [FSTEC of Russia. Guidance document. Automated systems. Protection against unauthorized access to information. Classification of automated systems and requirements for information protection [Electronic resource]. URL: https: //fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predseda-gostekhkomissii-rossii-199-302-gart (date of access: 03/10/2020). (In Russ)]
17. ISO / IEC 17000: 2004. Conformity assessment. Dictionary and General principles [Electronic resource]. - URL: https: //pqm-online.com/assets/files/ lib / std / iso_17000-2004.pdf (date accessed: 03/10/2020).
18. ISO / IEC 27002: 2005-2013. Information technology. Security method. Practical rules of information security management [Electronic resource]. URL: http: //docs.cntd.ru/ document / gost-r-iso-mek-17799-2005 (date of access 03/10/2020).
19. Razrabotka modeley i algoritmov otsenki effektivnosti podsistemy zashchity konfidentsial'nykh svedeniy pri yeye proyektirovanii v sistemakh elektronnogo dokumentooborota OVD: monografiya [Elektronnyy resurs] / Drovni-

kova I.G. [i dr.]. Voronezh: Voronezh. in-t MVD Rossii, 2019. [Development of models and algorithms for assessing the effectiveness of the subsystem for the protection of confidential information during its design in the systems of electronic document management of the Department of Internal Affairs: monograph [Electronic resource] / Drovnikova I.G. [and etc.]. Voronezh: Voronezh. Institute of the Ministry of Internal Affairs of Russia, 2019. (In Russ)]

20. Zastrozhnov I.I. Modelirovaniye i issledovaniye dinamiki funktsionirovaniya programmnykh sistem zashchity informatsii dlya otsenki i analiza kachestva ikh funktsionirovaniya pri proyektirovanii i upravlenii: dis. ... kand. tekhn. nauk: 05.13.18 / Zastrozhnov Igor' Ivanovich. Voronezh, 2005. 181 s. [Zastrozhnov I.I. Modeling and research of the dynamics of the functioning of information security software systems for assessing and analyzing the quality of their functioning in design and management: dis. ... Cand. tech. Sciences: 05.13.18 / Zastrozhnov Igor Ivanovich. Voronezh, 2005.181 p. (In Russ)]
21. Korniyenko B.Y. Design and research of mathematical model for information security system in computer network / B.Y. Korniyenko, L.P. Galata // Science-Based Technologies. 2017. Vol. 34. Issue 2. pp. 114-118.
22. Nazareth D. System dynamics model for information security management / D. Nazareth, J. Choi // Information & Management. 2015. Vol. 52. Issue 1. pp. 123-134.
23. Kresimir S. The information systems' security level assessment model based on an ontology and evidential reasoning approach / S. Kresimir, O Effectiveness Evaluation on Cyberspace Security Defense System. Hrvoje, G. Marin // Computers & Security. 2015. pp.100-112.
24. White S.C. Comparison of Security Models: Attack Graphs Versus Petri Nets / S.C. White, S.S. Sarvestani // Advances in Computers. 2014. Vol. 94. pp.1-24.
25. Nikishin K. Implementation of time-triggered ethernet using colored Petri NET / K. Nikishin, N. Konnov, D. Pashchenko // International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM). 2017. pp.1-5.
26. Charaf N. A colored Petri-net model for control execution of distributed systems / H. Charaf, S. Azzouzi // 4th International Conference on Control, Decision and Information Technologies (CoDIT). 2017. 277-282.
27. Network security analyzing and modeling based on Petri net and Attack tree for SDN / Y. Linyuan [and others] // 2016 International Conference on Computing, Networking and Communications (ICNC). 2016. pp.133-187.

Сведения об авторах:

Бацких Анна Вадимовна, адъюнкт, *svatikova96@mail.ru*

Конобеевских Владимир Валерьевич, кандидат технических наук, доцент кафедры автоматизированных информационных систем органов внутренних дел, *vkonobeevskikh@mail.ru*

Ефимов Сергей Венегдитович, кандидат технических наук, доцент, старший преподаватель кафедры огневой подготовки, *sclione@yandex.ru*

Information about the authors:

Anna V. Batskikh, adjunct, *svatikova96@mail.ru*

Vladimir V. Konobeevskikh, Cand. Sci. (Technical), Assoc. Prof. of the Department of Automated Information Systems of Internal Affairs Bodies, *vkonobeevskikh@mail.ru*

Sergey V. Efimov, Cand. Sci. (Technical), Assoc. Prof., Senior Lecturer of the Department of Fire Training, *sclione@yandex.ru*

Конфликт интересов.
Авторы заявляют об отсутствии конфликта интересов.
Поступила в редакцию 24.03.2021.
Принята в печать 01.04.2021.

Conflict of interest.
The authors declare no conflict of interest.
Received 24.03. 2021.
Accepted for publication 01.04.2021.