Для цитирования: *Каднова А.М. Методический подход к оценке вероятностного показателя своевременности выполнения типовых операций администратором системы защиты информации автоматизированной системы. Вестник Дагестанского государственного технического университета. Технические науки. 2019; 46 (3): 87-96. DOI:10.21822/2073-6185-2019-46-3-87-96*

For citation: *A.M. Kadnova. Methodical approach to evaluating the probabilistic time performance indicator of automated administrator operations in information protection systems. Herald of Daghestan State Technical University. Technical Sciences. 2019; 46(3): 87-96. (In Russ.) DOI:10.21822/2073-6185-2019-46-3-87-96*

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 621.3
DOI:10.21822/2073-6185-2019-46-3-87-96

МЕТОДИЧЕСКИЙ ПОДХОД К ОЦЕНКЕ ВЕРОЯТНОСТНОГО ПОКАЗАТЕЛЯ СВОЕВРЕМЕННОСТИ ВЫПОЛНЕНИЯ ТИПОВЫХ ОПЕРАЦИЙ АДМИНИСТРАТОРОМ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

Каднова А.М.
Воронежский институт Министерства внутренних дел России,
394065, г. Воронеж, пр. Патриотов, 53, Россия

Резюме. Цель. *В настоящее время в соответствии с требованиями руководящих документов ФСТЭК России, а также международными стандартами при разработке и эксплуатации защищенных автоматизированных систем необходимо проводить оценку эффективности (общей полезности) систем защиты информации. Статья посвящена разработке способа оценки эргатотехнических характеристик программных систем защиты информации для использования оценки общей полезности систем защиты информации. Целью работы является разработка методики оценки вероятностного показателя своевременности выполнения типовых операций по администрированию систем защиты информации.* ***Метод.*** *Для реализации данной цели были созданы группы пользователей, выполняющие типовые операции администратора системы защиты информации. Время выполнения операции каждой группой фиксировалось инструментальным средством IOGraphV1.0.1 и использовалось при расчете вероятностей своевременного выполнения типовых операций администратором по формуле усеченного нормального распределения.* ***Результат.*** *Проведена оценка вероятностного показателя, позволяющего оценить своевременность выполнения операций администратором системы защиты информации.* ***Вывод.*** *Полученные результаты могут быть использованы при комплексной оценке эффективности (надежности) функционирования программных систем защиты информации в автоматизированных системах с целью моделирования и анализа защищенности объектов информатизации специального назначения.*

Ключевые слова: *система защиты информации, несанкционированный доступ, защита информации, автоматизированная система, программная система, эргатотехнические характеристики*

COMPUTER SCIENCE, COMPUTER ENGINEERING AND MANAGEMENT

METHODICAL APPROACH TO EVALUATING THE PROBABILISTIC TIME PERFORMANCE INDICATOR OF AUTOMATED ADMINISTRATOR OPERATIONS IN INFORMATION PROTECTION SYSTEMS

A.M. Kadnova
Voronezh Institute of the Ministry of the Interior of the Russian Federation,
53 Patriotov Str., Voronezh 394065, Russia

Abstract Objectives *At present, in accordance with the requirements of the guiding documents of the Federal Service for Technical and Export Control (FSTEC) of Russia, as well as international standards in the development and operation of protected automated systems, it is necessary to evaluate the effectiveness (general utility) of information protection systems. The article is devoted to the development of a method for assessing the ergotechnical characteristics of software information security systems for use the assessment of the general utility of such systems. The aim of the work is to develop a methodology for assessing the probabilistic indicator of the timeliness of typical operations for the administration of information security systems.* ***Method*** *To achieve this goal, user groups were created in order to perform typical administrative operations within the information protection system. The operation time for each group, recorded using the IOGraphV1.0.1 tool, was utilised to calculate the probabilities of timely execution of typical operations by the administrator according to a truncated normal distribution formula.* ***Results*** *An assessment of a probabilistic indicator was carried out in order to evaluate the timeliness of operations performed by the administrator of the information protection system.* ***Conclusion*** *The results can be used in a comprehensive assessment of the effectiveness (reliability) of the automated functioning of information security software systems when modelling and analysing the security of special-purpose informatisation facilities.*

Keywords: *information protection system, unauthorised access, information protection, automated system, software system, ergotechnical characteristics*

Введение. Анализ нормативных документов, посвященных защите информации, обрабатываемой автоматизированными системами (АС) [1–6] и качеству программных систем [7–12], показал, что на сегодняшний день отсутствуют показатели оценки эргатотехнических характеристик систем защиты информации (СЗИ) в АС и методики их оценки.

В результате невозможности их оценки на этапе разработки СЗИ возникают следующие проблемы:

1) не полностью обеспечивается реализация целей и требований заказчиков к функционалу и потребительскому качеству СЗИ;

2) вследствие низкой достоверности первичной оценки бюджета, требования заказчика могут быть выполнены не в полной мере;

3) вследствие недостаточного контроля выполнения проекта, повышается риск отсутствия у конечного программного продукта требуемого качества;

4) отсутствие эргатотехнических показателей затрудняет сравнение и оценку сертифицированных СЗИ при их выборе.

Постановка задачи. В связи с необходимостью решения вышеперечисленных проблем целью настоящей работы является разработка методики оценки вероятностного показателя своевременности выполнения типовых операций по администрированию системы защиты информации.

Методы исследования. В интересах исследования вероятностных показателей «удобства использования» СЗИ введем ряд упрощающих ограничений, существенно не оказывающих влияние на общность решения задачи:

1. Реализация угрозы безопасности информации (БИ) и проявление ошибки

администратора являются независимыми и редкими событиями; проявление двух и более одноименных событий в период времени работы системы защиты информации практически не возможно.

2. Способность парирования угрозы несанкционированного доступа и безошибочность работы являются независимыми свойствами администратора.

Вероятность нахождения АС в состоянии БИ определяется вероятностью реализации угрозы в течение времени работы системы и возникающими ущербами. Реализация угрозы БИ может привести к следующим четырем случаям в АС:

1. Угроза БИ обнаружена СЗИ. Автоматизированная система продолжает функционировать. При этом СЗИ (администратор безопасности) работает в режиме частичных ущербов БИ и комплекса мероприятий по реагированию на угрозы БИ.
2. Угроза БИ полностью устраняется системоц защиты информации без каких-либо последствий. Работа АС продолжается.
3. Реализация угрозы БИ приводит к полному прекращению функционирования АС.
4. Работа АС продолжается в условиях не обнаруженной реализации угрозы БИ.

Проведем анализ протекающих процессов в системе «Угроза безопасности информации — система защиты информации — администратор безопасности».

В первом случае реализация угрозы БИ приводит к нарушению состояния БИ автоматизированной системы. Администратору безопасности удается локализовать проблему и продолжить работу системы в условиях частичных ущербов БИ, возникающих при реализации угрозы.

Работа АС продолжается в режиме частичного нарушения уровня информационной безопасности. При этом администратор безопасности работает в особом режиме с перегрузкой и может своевременно компенсировать ущербы с вероятностью P_k .

Таким образом, безопасное состояние АС в первом случае будет полностью характеризоваться не только вероятностью реализации угроз БИ, но и вероятностными характеристиками администратора по своевременной локализации угрозы БИ и организации дальнейшей работы АС в условиях возникающих ущербов БИ, не приводящих к полному прекращению работы.

Для оценки показателей информационной безопасности в первом случае необходима оценка своевременности выполнения работы администратором.

Во втором случае реализация угрозы БИ приводит к необходимости остановки АС на время, необходимое для реализации мероприятий по реагированию на угрозы БИ. Если время остановки АС меньше, чем $\tau_{оп}$, определяемое условиями функционирования АС, то можно считать, что состояние безопасности АС не нарушено.

Поэтому в качестве показателя «удобства использования» администратором необходимо выбрать вероятностный показатель восстановления безопасного состояния после реализации угрозы БИ. При этом случайное время восстановления должно удовлетворять условию:

$$\tau_в \le \tau_{оп}$$

где $\tau_в$ — случайное время восстановления безопасного состояния администратором безопасности.

В третьем случае, реализация угрозы БИ недопустима, т.к. ее реализация приводит к полному прекращению функционирования АС. В этом случае показатель «удобства использования» целесообразен только для настройки системы защиты информации и не является ни вероятностным, ни временным.

В четвертом случае отсутствует возможность парирования угрозы БИ и, соответственно, целесообразность оценки эргатотехнических показателей системы защиты информации для администратора.

Таким образом, анализ системы «Администратор и СЗИ» с учетом требований высоких значений уровня БИ при реализации угроз различного вида показал, что основной проблемой

взаимодействия администратора с СЗИ является своевременность выполнения работ при выполнении типовых операций, определяемая средним временем их выполнения.

Случайная величина времени выполнения формализуется функцией распределения вида:

$$q(b) = P\{B < b\} \quad (1)$$

где t – заданное время выполнения типовой операции.

Своевременность выполнения типовой операции для операторов с различным уровнем подготовки, состояния здоровья и в разных условиях работы целесообразно формализовать усеченным нормальным распределением вида [13]:

$$\overline{f(b)} = cf(b) = \frac{c}{\sigma_b\sqrt{2\pi}}\exp(-\frac{(b-m_b)}{2\sigma_b{}^2 b}) \quad (2)$$

где m_b – среднее значение времени выполнения типовой операции;

σ_b – среднеквадратичное отклонение времени выполнения типовой операции;

c – нормирующий множитель усеченного распределения;

b – параметр усеченного распределения, определяемый экспериментально, в соответствии с [13].

Нормирующий множитель, усеченного распределения (2) рассчитывается из условия:

$$c = \int_{b_1}^{b_2} f(b)db = 1$$

где b_1 и b_2 – нижнее и верхнее ограничения времени выполнения типовой операции.

Определение значений m_b и σ_b осуществлялось по результатам эксперимента, описанного далее.

Обсуждение результатов. Для проведения эксперимента привлекались студенты в количестве 80 человек, которые были поделены на группы в зависимости от уровня пользования системы защиты информации (опытные, среднего уровня и начального уровня).

На рис. 1 приведена структурная схема лабораторной установки, представленной в виде средств вычислительной техники, с установленным на них программным обеспечением Страж NT 3.0 с заводскими номерами, а также приложением IOGraph V1.0.1, реализующим метод *mouse-tracking*, и используемой при проведении эксперимента.

Mouse-tracking (отслеживание курсора) инструмент, позволяющий отслеживать движение мыши администратором безопасности и сделанные им клики. Использование этого инструмента позволяет построить последовательность передвижения курсора по интерфейсу и карту кликов, показывающую по каким элементам интерфейса системы защиты информации чаще «кликали».

Также программа IOGraph V1.0.1, реализующая технологию отслеживания мыши, позволяет экспериментально определить операционные характеристики программы, такие как время выполнения всей операции и время задержки курсора на элементе интерфейса программы.

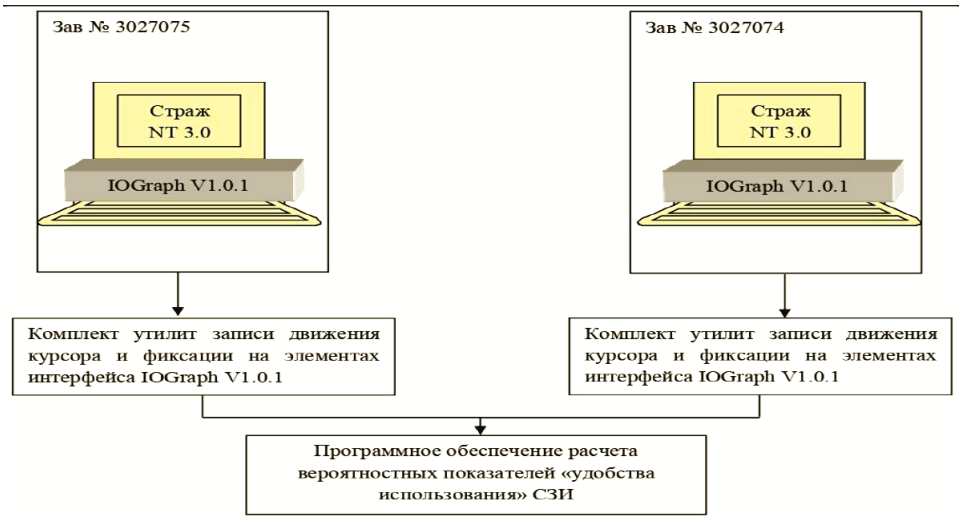

Рис. 1. Структурная схема программного обеспечения, используемого для проведения расчетов по оценке «удобства использования» СЗИ «Страж NT 3.0»
Fig. 1. The structural diagram of the software used for calculations to assess the "Usability" SZI "Sentinel NT 3.0"

Студенты выполняли типовые операции администратора СЗИ в соответствии с [14,15], представленные в табл. 1.

Таблица 1. Типовые операции администратора системы защиты информации
Table 1. Typical operations of information security system administrator

№ п.п.	**Наименование типовой операции выполняемой администратором Name of the typical operation performed by the administrator**
1	создание, удаление и переименование пользователей create, delete and rename users
2	смена пароля пользователя change user password
3	просмотр и редактирование свойств пользователя viewing and editing user properties
4	редактирование разрешений edit permissions
5	редактирование параметров системного аудита editing system audit settings
6	открытие и сохранение журнала событий opening and saving the event log
7	работа с фильтром событий work with an event filter
8	тестирование системы защиты security testing

В качестве примера рассмотрим действия студента, выполняющего типовую операцию администратора СЗИ «Создание, удаление и переименование пользователей».

Для создания пользователя администратор выбирает пункт меню «Компьютер», далее «Новый пользователь» или пункт меню «Домен», далее «Новый пользователь» либо вызывает контекстное меню нажатием правой кнопки мыши в пустой области списка пользователей и выбирает пункт «Новый пользователь…».

После этого на экране появляется диалог, в котором администратор вводит имя пользователя, полное имя, описание, а также его пароль и допуск. Для создания пользователя администратор нажимает кнопку «Создать». Если администратору необходимо создать пользователя в домене, то в таком случае существует возможность размещения его учетной записи в контейнере Active Directory, отличном от контейнера «по умолчанию». Для этого в

вышеуказанном диалоге администратор нажимает кнопку «Выбрать…» и в появившемся окне выбирает необходимый контейнер AD. При установке администратором флажка «Создать профиль пользователя на этом компьютере» после удачного создания пользователя на данном компьютере формируется его локальный профиль.

Для удаления пользователя администратор выбирает его в списке пользователей и выбирает пункт меню «Пользователь», далее «Удалить» либо выбирает пункт «Удалить» вызванного нажатием правой кнопки мыши контекстного меню. Для переименования пользователя администратор выбирает его в списке пользователей и выбирает пункт меню «Пользователь», далее «Переименовать» либо выбирает пункт «Переименовать» вызванного нажатием правой кнопки мыши контекстного меню. После этого администратор вводит новое имя пользователя и нажимает клавишу «Enter».

В процессе выполнения каждой операции, в частности, расписанной выше, инструментальное средство IOGraph V1.0.1, реализующее метод mouse-tracking, записывало траекторию движения курсора каждого администратора и время выполнения им операции. Затем для каждой группы администраторов подсчитывались значения среднего времени выполнения каждой из перечисленных операций. Данные значения использовались для расчета вероятностей своевременного выполнения типовых операций администраторами в соответствии с (2). Результаты представлены в табл.2.

Таблица 2. Результаты оценки вероятностного показателя типовой операции, выполняемой администратором системы защиты информации

Table 2. The results of the assessment of the probability indicator of a typical operation performed by the administrator of the Information Security System

№ п.п.	Наименование типовой операции выполняемой администратором СЗИ «Страж NT 3.0» The name of the typical operation performed by the administrator of the SZI “Guard NT 3.0”	Значение требуемого времени выполнения типовой операции администратором СЗИ «Страж NT 3.0», с. The value of the required execution time of a typical operation by the administrator of the security system “Sentinel NT 3.0”, c.	Вероятность выполнения типовой операции администратором СЗИ «Страж NT 3.0» The likelihood of a typical operation being performed by the administrator of the security system “Guard NT 3.0”		
			группа «пользователи начального уровня» user group "entry–level users"	группа «пользователи среднего уровня» user group "mid–level users"	группа «опытные пользователи» user group "advanced users"
1	Создание, удаление и переименование пользователей Create, delete and rename users	40	–	0,0227	0,0227
		50	–	0,1586	0,1586
		60	–	0,4999	0,4999
		70	0,0013	0,8412	0,8412
		80	0,0227	0,9771	0,9771
		90	0,1586	0,9986	0,9986
		100	0,4999	–	–
		110	0,8412	–	–
		120	0,9771	–	–
		130	0,9986	–	–
2	Смена пароля пользователя Change user password	40	–	0,0061	0,0227
		60	0,0227	0,3084	0,4999
		80	0,4999	0,9331	0,9771
		100	0,9998	0,9998	0,9995

3	Просмотр и редактирование свойств пользователя View and edit user properties	40	0,0061	0,0227	0,1586
		60	0,3084	0,4999	0,8412
		80	0,9331	0,9771	0,9986
		100	0,9998	0,9995	–
4	Редактирование разрешений Editing Permissions	80	–		0,0013
		100	–	0,0227	0,1586
		120	–	0,4999	0,8412
		140	–	0,9771	0,9986
		160	–	0,9999	–
		180	0,0227	–	–
		200	0,4999	–	–
		220	0,9771	–	–
		240	0,9999	–	–
5	Редактирование параметров системного аудита Editing system audit settings	30	0,0013	0,1586	0,3083
		40	0,0013	0,4999	0,6913
		60	0,1586	0,9771	0,9936
		80	0,8412	0,9999	–
		100	0,9986	–	–
6	Открытие и сохранение журнала событий Opening and saving the event log	30	0,0677	0,3083	0,4999
		40	0,3084	0,6913	0,8399
		50	0,6914	0,9330	0,9758
		60	0,9331	0,9936	0,9973
7	Работа с фильтром событий Working with an event filter	270	–	0,0013	0,0013
		290	–	0,1586	0,1586
		310	0,0002	0,8412	0,8412
		330	0,0227	0,9986	0,9986
		350	0,4999	0,9999	0,9999
		370	0,0771	–	–
8	Тестирование системы защиты Security Testing	40	0,0001	0,1586	0,1586
		50	0,0061	0,4999	0,4999
		60	0,0667	0,8412	0,8412
		70	0,3084	0,9771	0,9771
		80	0,6914	–	–
		90	0,9331	–	–

Вывод. Использование СЗИ для обеспечения защиты информации, обрабатываемой АС, требует детального анализа их эргатотехнических характеристик. Основным показателем, характеризующим эргатотехнические характеристики СЗИ, является своевременность выполнения типовой операции администратором безопасности.

В статье на основе экспериментально измеренных средних значений времени выполнения типовых операций администраторами, составляющими репрезентативные группы, оценены вероятностные характеристики своевременности выполнения типовых операций.

Полученные значения вероятностей выполнения типовых операций могут в дальнейшем использоваться при сравнительном анализе «удобства использования» СЗИ различных классов, разработке планов работы служб по организации информационной безопасности и обоснованию требований к организации и составу служб обеспечения информационной безопасности.

Библиографический список:

1. Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006 № 149-ФЗ (в ред. от 19.12.2016) // СПС «Консультант Плюс».

2. 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.

3. ФСТЭК РФ. 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.

4. ФСТЭК РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. – Москва : Воениздат, 1992.

5. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: постановление Правительства РФ от 01.11.2012 N 1119 // СПС «КонсультантПлюс».

6. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : приказ ФСТЭК России от 18.02.2013 № 21 // СПС «КонсультантПлюс».

7. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 2 : Функциональные компоненты безопасности. – Введ. 2013-11-08. – [Электронный ресурс]. – URL: https://files.stroyinf.ru/Data2/1/4293774/4293774728.pdf.

8. ISO/IEC 17000:2004. Оценка соответствия. Словарь и общие принципы. – Введ. 2001-11-01. – [Электронный ресурс]. – URL: https://pqm-online.com/assets/files/lib/std/iso_17000-2004.pdf.

9. ГОСТ 28806-89. Качество программных средств. Термины и определения. – Введ. 1990-12-25. – [Электронный ресурс]. – URL: http://www.kimmeria.nw.ru/standart/glosys/gost_28806_90.pdf.

10. ГОСТ 28195-89. Оценка качества программных средств. Общие положения. – Введ. 1989-07-28. – Москва : Госстандарт СССР. 1990 г. – 15 с.

11. ГОСТ Р ИСО/МЭК 9126-93. Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению. – Введ. 1993-12-28. – [Электронный ресурс]. – URL: http:// http://docs.cntd.ru/document/gost-r-iso-mek-9126-93.

12. Каднова А.М. Система показателей качества функционирования при создании системы информационной безопасности на объекте информатизации ОВД / А.М. Каднова, О.И. Бокова, Е.А. Рогозин, А.С. Серпилин // Приборы и системы. Управление, контроль, диагностика. – 2019. – №1. – С. 32–39.

13. Дружинин Г.В. Надежность автоматизированных систем // Г.В. Дружинин. – Москва : Энергия, 1977. – 536 с.

14. Система защиты информации «Страж NT 3.0». Руководство администратора [Электронный ресурс]. – URL: https://www.guardnt.ru/doc/gnt_30_admin_guide.pdf

15. Каднова А.М. Имитационная модель функционирования системы защиты информации от несанкционированного доступа «Страж NT» в программной среде «CPN Tools» с целью исследования ее временных характеристик / А.М. Каднова, Е.А. Рогозин, Ю.С. Лунёв, А.Д. Попов // Охрана, безопасность, связь – 2018 : материалы международной научно-практической конференции. – Т 3. – № 4(4). – Воронеж : ВИ МВД России, –2019. – С. 78–81

References:

1. Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii: federal'nyy zakon ot 27.07.2006 № 149-FZ (v red. ot 19.12.2016) // SPS «Konsul'tant Plyus». [On information, information technology and information protection: Federal Law of July 27, 2006 No. 149-FZ (as amended on December 19, 2016) // ATP "Consultant Plus". (In Russ)]
2. 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. [On approval of the Concept of ensuring information security of the internal affairs bodies of the Russian Federation until 2020: Order of the Ministry of Internal Affairs of Russia dated 14.03.2012 No. 169 [Electronic resource]. - URL: http://policemagazine.ru/forum/showthread.php?t=3663. (In Russ)]
3. [FSTEC of the Russian Federation. 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-ot-25-iyuly . (In Russ)]
4. FSTEK RF. Rukovodyashchiy dokument. Sredstva vychislitel'noy tekhniki. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Pokazateli zashchishchennosti ot nesanktsionirovannogo dostupa k informatsii [Elektronnyy resurs]. – URL: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g. [FSTEC of the Russian Federation. Guidance document. Automated systems. Protection against unauthorized access to information. Classification of automated systems and information protection requirements. - Moscow: Military Publishing House, 1992. (In Russ)]
5. Ob utverzhdenii trebovaniy k zashchite personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh : postanovleniye Pravitel'stva RF ot 01.11.2012 N 1119 // SPS «Konsul'tantPlyus». [On approval of requirements for the protection of personal data during their processing in personal data information systems: Decree of the Government of the Russian Federation of 01.11.2012 N 1119 // ATP "Consultant Plus". (In Russ)]
6. Ob utverzhdenii sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh : prikaz FSTEK Rossii ot 18.02.2013 № 21 // SPS «Konsul'tantPlyus». [On approval of the composition and content of organizational and technical measures to ensure the security of personal data when they are processed in personal data information systems: Order of the FSTEC of Russia dated February 18, 2013 No. 21 // ATP "Consultant Plus".(In Russ)]
7. GOST R ISO/MEK 15408-2-2013. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti informatsionnykh tekhnologiy. CH. 2 : Funktsional'nyye komponenty bezopasnosti. – Vved. 2013-11-08. – [Elektronnyy resurs]. – URL: https://files.stroyinf.ru/Data2/1/4293774/4293774728.pdf. [GOST R ISO / IEC 15408-2-2013. Information technology. Security methods and tools. Criteria for assessing the security of information technology. Part 2: Functional safety components. - Enter. 2013-11-08. - [Electronic resource]. - URL: https://files.stroyinf.ru/Data2/1/4293774/4293774728.pdf. (In Russ)]
8. ISO/IEC 17000:2004. Otsenka sootvetstviya. Slovar' i obshchiye printsipy. – Vved. 2001-11-01. – [Elektronnyy resurs]. – URL: https://pqm-online.com/assets/files/lib/std/iso_17000-2004.pdf. [ISO / IEC 17000: 2004. Conformity assessment. Vocabulary and general principles. - Enter. 2001-11-01. - [Electronic resource]. - URL: https://pqm-online.com/assets/files/lib/std/iso_17000-2004.pdf. (In Russ)]
9. GOST 28806-89. Kachestvo programmnykh sredstv. Terminy i opredeleniya. – Vved. 1990-12-25. – [Elektronnyy resurs]. – URL: http://www.kimmeria.nw.ru/standart/glosys/gost_28806_90.pdf. [GOST 28806-89. The quality of software. Terms and Definitions. - Enter. 1990-12-25. - [Electronic resource]. - URL: http://www.kimmeria.nw.ru/standart/glosys/gost_28806_90.pdf. (In Russ)]
10. GOST 28195-89. Otsenka kachestva programmnykh sredstv. Obshchiye polozheniya. – Vved. 1989-07-28. – Moskva : Gosstandart SSSR. 1990 g. – 15 s. [GOST 28195-89. Software quality assessment. General Provisions - Enter. 1989-07-28. - Moscow: Gosstandart of the USSR. 1990. 15 p. (In Russ)]
11. GOST R ISO/MEK 9126-93. Informatsionnaya tekhnologiya. Otsenka programmnoy produktsii. Kharakteristiki kachestva i rukovodstva po ikh primeneniyu. – Vved. 1993-12-28. – [Elektronnyy resurs]. – URL: http:// http://docs.cntd.ru/document/gost-r-iso-mek-9126-93. [GOST R ISO / IEC 9126-93. Information technology. Evaluation of software products. Quality characteristics and guidelines for their use. - Enter. 1993-12-28. [Electronic resource]. URL: http: // http://docs.cntd.ru/document/gost-r-iso-mek-9126-93. (In Russ)]
12. Kadnova A.M. Sistema pokazateley kachestva funktsionirovaniya pri sozdanii sistemy informatsionnoy bezopasnosti na ob"yekte informatizatsii OVD / A.M. Kadnova, O.I. Bokova, Ye.A. Rogozin, A.S. Serpilin // Pribory i sistemy. Upravleniye, kontrol', diagnostika. – 2019. – №1. – S. 32–39. [Kadnova A.M. The system of indicators of the quality of functioning when creating an information security system at the ATS informatization

facility / A. Kadnova, O.I. Bokova, E.A. Rogozin, A.S. Serpilin // Devices and Systems. Management, control, diagnostics. 2019. No. 1. pp. 32–39. (In Russ)]

13. Druzhinin G.V. Nadezhnost' avtomatizirovannykh sistem // G.V. Druzhinin. – Moskva : Energiya, 1977. – 536 s. [Druzhinin G.V. Reliability of automated systems // G.V. Druzhinin. Moscow: Energy, 1977. 536 p.

14. Sistema zashchity informatsii «Strazh NT 3.0». Rukovodstvo administratora [Elektronnyy resurs]. – URL: https://www.guardnt.ru/doc/gnt_30_admin_guide.pdf [The information security system "Guard NT 3.0". Administrator Guide [Electronic resource]. URL: https://www.guardnt.ru/doc/gnt_30_admin_guide.pdf(In Russ)]

15.Kadnova A.M. Imitatsionnaya model' funktsionirovaniya sistemy zashchity informatsii ot nesanktsionirovannogo dostupa «Strazh NT» v programmnoy srede «CPN Tools» s tsel'yu issledovaniya yeye vremennykh kharakteristik / A.M. Kadnova, Ye.A. Rogozin, YU.S. Lunov, A.D. Popov // Okhrana, bezopasnost', svyaz' – 2018 : materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii. T 3. № 4(4). Voronezh : VI MVD Rossii, 2019. S. 78–81. [Kadnova A.M. A simulation model of the operation of the information protection system against unauthorized access "Guard NT" in the Software environment "CPN Tools" in order to study its temporal characteristics / A.M. Kadnova, E.A. Rogozin, Yu.S. Lunev, A.D. Popov // Protection, Security, Communication. 2018: materials of the international scientific and practical conference. Vol 3. No. 4 (4). Voronezh: VI Ministry of Internal Affairs of Russia, 2019. pp. 78–81 (In Russ)]

Сведения об авторе:

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

Information about the author:

Ayzhana M. Kadnova, Adjunct, Department of automated information systems of law enforcement bodies; e-mail: **aizhana_kadnova@mail.ru**

Конфликт интересов.
Автор заявляет об отсутствии конфликта интересов.

Conflict of interest.
The author declare no conflict of interest.

Поступила в редакцию 15.06.2019.
Принята в печать 19.08.2019.

Received 15. 06. 2019.
Accepted for publication 19.08.2019.