Для цитирования: *Качаева Г.И., Попов А.Д., Рогозин Е.А. Показатели эффективности функционирования при разработке систем защиты информации от несанкционированного доступа в автоматизированных информационных системах. Вестник Дагестанского государственного технического университета. Технические науки. 2018; 45 (1): 147-159. DOI:10.21822/2073-6185-2018-45-1-147-159*
For citation: *Kachaeva G.I., Popov A.D., Rogozin E.A. Functional performance indicators during systems development to protect information from unauthorised access. Herald of Daghestan State Technical University. Technical Sciences. 2018; 45 (1):147-159. (In Russ.) DOI:10.21822/2073-6185-2018-45-1-147-159*

ТЕХНИЧЕСКИЕ НАУКИ
ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК: 004.056
DOI: 10.21822/2073-6185-2018-45-1-147-159

ПОКАЗАТЕЛИ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ПРИ РАЗРАБОТКЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Качаева Г.И.[1], Попов А.Д.[2], Рогозин Е.А.[3]
[1]Дагестанский государственный технический университет,
[1]367026, г. Махачкала, пр.И.Шамиля 70, Россия,
[2-3]Воронежский институт МВД России,
[3-4]394065, г. Воронеж, пр. Патриотов,53, Россия,
[1]e-mail:Providetc@mail.ru,[2]e-mail:anton.holmes@mail.ru,[3]e-mail: evgenirogozin@yandex.ru

Резюме: Цель. *Целью и задачами исследования являются: анализ нормативных международных и российских документов, а также научных материалов по проблемам оценки качества программного обеспечения; исследование свойств эффективности функционирования систем защиты информации от несанкционированного доступа в автоматизированных информационных системах; аналитическое обобщение существующих недостатков систем защиты информации от несанкционированного доступа в автоматизированных информационных системах, на основе которых разработать показатели эффективности функционирования. На основе проведенного анализа обосновать и разработать критерии оценок эффективности функционирования систем защиты информации от несанкционированного доступа в автоматизированных информационных системах. На основе созданных критериев и показателей разработать алгоритм интегральной оценки эффективности функционирования систем защиты информации от несанкционированного доступа в автоматизированных информационных системах.* ***Метод.*** *Методической основой решения поставленных цели и задач являются основные положения теории эффективности и теории систем.* ***Результат.*** *Разработаны критерии и показатели эффективности функционирования при создании в автоматизированных информационных системах на основе проведенного анализа открытых литературных источников и существующих недостатков реального использования систем защиты информации от несанкционированного доступа. Разработан алгоритм интегральной оценки эффективности функционирования систем защиты информации от несанкционированного доступа.* ***Вывод.*** *Создана система показателей эффективности функционирования систем защиты информации от несанкционированного доступа, включающая частные показатели (статические), практически независимые от времени, достоверность которых основывается на экспертных оценках) и интегральные (динамические), зависимые от времени, оценка которых основывается на математическом моделировании.*

Ключевые слова: *автоматизированная информационная система, несанкционированный доступ к информации, качество, показатель, критерий, система защиты информации, оценка эффективности*

TECHNICAL SCIENCE
COMPUTER SCIENCE, COMPUTER ENGINEERING AND MANAGEMENT

FUNCTIONAL PERFORMANCE INDICATORS DURING SYSTEMS DEVELOPMENT TO PROTECT INFORMATION FROM UNAUTHORISED ACCESS

Gyulkhanum I. Kachaeva[1], Anton D. Popov[2], Evgeny A. Rogozin [3]
[1]Daghestan State Technical University,
[1]70 I. Shamilya Ave.,Makhachkala, 367026, Russia,
[2-3]Voronezh Institute of the Ministry of Internal Affairs of Russia,
[2-3]53 Patriotov Ave., Voronezh 394065, Russia,
[1]e-mail:Providetc@mail.ru,[2]e-mail:anton.holmes@mail.ru,[3]e-mail: evgenirogozin@yandex.ru

Abstract Objectives. *In order to investigate the property of the operational effectiveness of automated systems for protecting information from unauthorised access, it is necessary to analyse the normative documents (both international and Russian) and scientific materials devoted to the evaluation of software quality. The aim of the study consists in the analysis of the existing deficiencies in systems for protecting information from unauthorised access, on the basis of which analysis it is possible to develop performance indicators, substantiate and develop the criteria for assessing the operational effectiveness of the information protection systems from unauthorised access in automated information systems and develop an algorithm for the integrated evaluation of the operational effectiveness of information protection systems on the basis of the established criteria and indicators.* ***Methods.*** *One of the methods for solving the set goals consists in the main provisions of efficiency and systems theories, which in turn became the theoretical basis for solving problems involved in the creation of criteria and assessment of performance indicators of information protection systems.* ***Results.*** *The criteria and performance indicators for the creation of automated information systems are developed on the basis of the analysis of open literature sources and existing shortcomings in the real use of systems for protecting information from unauthorised access. An algorithm for the integrated evaluation of the operational effectiveness of the information protection systems is developed.* ***Conclusion.*** *In the article, based on the analysis of normative documents (both international and Russian), as well as on the scientific materials devoted to the quality (function efficiency) of complex software systems, to which the information protection systems can be related, a system of performance indicators was developed. These can be indicators can be classified as partial (static, practically independent of time, the evaluation of which is based on expert estimates) and integral (dynamic, time-dependent, the evaluation of which is based on mathematical modeling).*

Keywords: *automated information system, unauthorised access to information, quality indicator criterion, information protection system, efficiency assessment*

Введение. Использование автоматизированных информационных системы (АИС), в повседневной деятельности человека уже считается обыденным. Обрабатываемая в них информация зачастую несет в себе критический характер, например, в отраслях атомной энергетики, военной, органов внутренних дел, а также в других государственных структурах, где присутствует обработка, хранение и передача конфиденциальной информации (согласно нормативных документов Федеральной службы по техническому и экспортному контролю (ФСТЭК) России под конфиденциальной понимается информации требующая защиты[1]).

Особенностью рассматриваемых систем является их повышенная привлекательность со стороны криминальных структур [2].

Для противодействия различным угрозам специалисты по информационной безопасности внедряют программно-технические средства защиты информации, к которым относятся системы защиты информации от несанкционированного доступа (СЗИ от НСД). Они представляют собой сложную организационно-программную систему, направленную на обеспечение защиты информации от несанкционированного доступа к информационному ресурсу, уничтоже-

ния, модификации, блокирования, копирования информации и иных действий, ведущих к нарушению функционирования АИС в целом [3].

Постановка задачи. Разработка СЗИ от НСД, как существующей подсистемы современной АИС, представляет собой сложный, комплексный, многоэтапный процесс [3], его ключевой особенностью является выполнение поставленных целей при проектировании, которые бы не влияли на работоспособность АИС и их компонентов в целом.

Одной из задач разработки АИС в защищенном исполнении является поиск и выбор оптимальных (с точки зрения их структуры) вариантов функционирования СЗИ от НСД в АИС, что необходимо учитывать на всех этапах разработки этих сложных систем.

Поэтому при разработке СЗИ от НСД в АИС и при ее функционировании в режиме реального времени, согласно нормативной документации ФСТЭК необходимо проводить оценку качества (эффективности функционирования) программного обеспечения (ПО), к которому, несомненно, можно отнести СЗИ от НСД [4].

Методы исследования. В настоящее время выделяют три подхода к оцениванию эффективности функционирования СЗИ от НСД в АИС: экспертный, вероятностный, оценочный [4-6]. Существует множество мнений, которые определяют один из подходов приоритетнее другого, но единственным правильным выходом из сложившихся противоречий будет комплексное использование всех трех подходов к оценке эффективности функционирования СЗИ от НСД на этапах ее разработки. Поэтому предлагается использовать вероятностно-экспертный подход, основанный на математическом моделировании и экспертных оценках, который позволяет учитывать, как динамические, так и статические характеристики эффективности функционирования СЗИ от НСД.

Вероятностный подход используется при описании неизвестных (случайных событий), в частности, их вероятностно-временных характеристик; экспертный подход, основан на мнении экспертов в данной области и определяется достаточностью статических (практически не связанных со временем) параметров, определяющих эффективность функционирования СЗИ от НСД, к которым, например, можно отнести вычислительные ресурсы АИС и т.д., а оценочный – при определении предметной области, на первоначальном этапе разработки СЗИ от НСД [3].

Существующий ГОСТ-28806-89 трактует понятие качество СЗИ, как совокупность свойств, которые обуславливают его пригодность удовлетворять заданные или подразумеваемые потребности в соответствии с его предназначением [7]. В различных российских и международных стандартах [7-11], связанных с качеством (эффективностью функционирования СЗИ от НСД) определение качества функционирования СЗИ от НСД в АИС трактуется как степень (полноту выполнения) предъявляемых к ним требований. Качество СЗИ от НСД определяется в зависимости от того с какой целью разрабатывается данный программный продукт [12-13].

Квалиметрические измерения рассматривают качество, как ранжированную совокупность свойств, которые могут включать в себя свойства, представляющие более низкий уровень. Между всеми свойствами (показателей) качества функционирования СЗИ от НСД существует взаимосвязь, которая позволяет комплексно оцениватьэти системы [14].

Проведенный анализ [7] позволил определить следующие основные свойства качества функционирования при разработке СЗИ от НСД на объектах информатизации: функциональность СЗИ от НСД; надежность СЗИ от НСД; удобство использования СЗИ от НСД; эффективность СЗИ от НСД; сопровождаемость СЗИ от НСД; мобильность СЗИ от НСД.

Данный перечень свойств качества СЗИ от НСД в АИС в различных открытых литературных источниках трактуется шире [15-17], что в настоящее время при разработке СЗИ от НСД в АИС представляет собой значительную неопределенность и трудностьс точки зрения сложной (иерархической) программной системы.

Поэтому в статье рассмотрим не оценку качества функционирования СЗИ от НСД, а оценку одного из свойств качества – эффективность функционирования и его атрибутов в соответствиинормативной документации ФСТЭК [4] при разработке СЗИ от НСД на объектах информатизации. Поэтому, при оптимальном выборе параметров и характеристик СЗИ от НСД предпочтение отдается измерению эффективности функционирования СЗИ от НСД в сравне-

нии с ееразличными вариантами реализации.

Описание рассматриваемого свойства можно найти в теории эффективности сложных систем и процессов, так как СЗИ от НСД в АИС является сложной динамической системой, и каждая операция имеет четкую поставленную цель.

Под эффективностью функционирования СЗИ от НСД следует понимать степень соответствия результатов защиты информации в АИС, относительно поставленной цели при разработке СЗИ от НСД [18]. В настоящее время существует множество понятий эффективности функционирования СЗИ от НСД и их интерпретаций, значительные расхождения имеют даже место быть в нормативных документах, поэтому стоит максимально осторожно оперировать данным определением и его смысловым значением [19-21].

При эксплуатации СЗИ от НСД эти системы, как правило, на свое функционирование в АИС требуют значительных вычислительных ресурсов, то при её разработке необходимо найти разумный компромисс (с точки зрения вычислительных ресурсов) между функционированием СЗИ и АИС по своему прямому предназначению, к которым относятся (обработка, хранение и передача конфиденциальной информации).

Возникает вопрос, каким способом необходимо провести оценку их эффективности функционирования? Чтобы на него ответить необходимо оценивать результаты выполняемых операций СЗИ от НСД и сопоставлять их с поставленными задачами и затратами, требуемыми для их реализации в АИС, поскольку проблема состоит в выборе лучшего из сравниваемых вариантов функционирования СЗИ от НСД.

Под показателем эффективности функционирования СЗИ от НСД понимается мера степени соответствия реального результата функционирования СЗИ от НСД требуемому [10]. Каждый показатель эффективности функционирования характеризует достаточность определенного свойства СЗИ от НСД. При разработке СЗИ от НСД возникают сложности в ее оценки эффективности функционирования, а именно не все характеристики подвергаются оценке. В следствие этого, проанализируем показатели эффективности функционирования СЗИ от НСД и сопоставим их с недостатками, возникающими при разработке СЗИ от НСД в АИС, чтобы учесть все свойства, влияющие на работоспособность в целом АИС.

Существует множество мнений относительно выбора атрибутов (показателей) оценки эффективности функционирования в СЗИ от НСД, приведенных в табл. 1.

Перечисленные атрибуты (показатели) эффективности функционирования могут классифицироваться как частные, подробнее этот вопрос освещен в [16]. Стоит заметить, что смысловые значения показателей эффективности функционирования СЗИ от НСД (табл. 1) принципиально схожи. К недостаткам применения СЗИ от НСД на объектах информатизации АИС критического применения можно отнести [3] (табл. 2):

1. Оптимальность программного кода. В связи с тем, что СЗИ от НСД представляет собой комплекс программных средств защиты информации (включая организационные меры), то и разрабатываемый программный код должен быть максимально оптимизированс точки зрения оптимальности использования ресурсов АИС.
2. Отсутствие возможности исследовать эти системы в динамическом (временном) диапазоне.
3. Зависимость ресурсоёмкости СЗИ от НСД от вычислительных ресурсов АИС, к которым можно отнести процессорное время, оперативную память и дисковое пространство. Ограниченность перечисленных ресурсов АИС оказывает непосредственное влияние на время выполнения защитных функций СЗИ от НСД, и как следствие несоответствие предъявляемым к ней требованиям.
4. Недостатком будет являться полная или частичная неприспособленность СЗИ от НСД выполнять возложенные на нее задачи, так как моральное старение СЗИ от НСД будет характеризоваться частичной или полной непригодностью адекватно реагировать на существующие деструктивные воздействия на информационный ресурс АИС.
5. Изменение структуры АИС с точки зрения программного и технического обеспечения этих систем, могут оказывать влияние на выполнение защитных функций СЗИ от НСД в

АИС. В качестве примера можно привести дублирование защитных функций СЗИ от НСД антивирусными программными средствами.

Таблица 1. Представление атрибутов (показателей) оценки эффективности функционирования системы защиты информации от несанкционированного доступа
Table 1. Representation of attributes (indicators) of an estimation of the effectiveness of the system of protecting information from unauthorized access

Источник Source	Атрибут свойства эффективности Attribute of the performance property
ISO/IEC 9126	*Временная эффективность* – свойство, характеризующее поведение АИС, включая и СЗИ от НСД, как при разработке, так и эксплуатации; *Ресурсоемкость* – свойство, характеризующее поведение используемых ресурсов АИС, включая и СЗИ от НСД, как при разработке, так и при их эксплуатации; *Согласованность* – свойство, характеризующее количество функций СЗИ от НСД не соответствующим стандартам. [8-11]
ГОСТ 28806	*Времяемкость* – совокупность свойств СЗИ от НСД, характеризующихся обеспечением при его функционировании временем реакции на запросы, на скорость обработки данных и на пропускную способность; *Ресурсоемкость*–совокупность свойств СЗИ от НСД, характеризующихся объемом используемых при его функционирования вычислительных ресурсов АИС и продолжительности их использования. *Функциональность* – совокупность свойств СЗИ от НСД, определяемая наличием и конкретными особенностями защитных функций, способных удовлетворять заданные или подразумеваемые потребности в защите информации на объектах информатизации [7]
ГОСТ 25010	*Результативность* – точность и полнота, с которой достигается цель функционирования СЗИ от НСД; *Производительность* – связь точности и полноты достижения пользователями целей с израсходованными вычислительными ресурсами АИС [22]
Липаев В.В.	*Временная эффективность*–свойство СЗИ от НСД, характеризующее требуемое время отклика и обработки заданий, а также производительность решения задач защиты информации с учетом количества используемых вычислительных ресурсов АИС в установленных условиях; *Используемость ресурсов*–степень загрузки доступных вычислительных ресурсов АИС в установленных условиях эксплуатации СЗИ от НСД. [14]
Боем Б.	*Рациональность*–рассматривается с точки зрения оптимальности разработки СЗИ от НСД; *Доступность*–рассматривается как селективность использования ее компонент, имеется в ввиду, что при изменении какой-либо характеристики, пользователь должен иметь доступ к необходимым данным.[15]
Петухов Г.Б.	*Результативность*–характеризуется результатом достижения цели функционирования СЗИ от НСД на объектах информатизации; *Ресурсоемкость*–характеризуется расходомвсех видов вычислительных ресурсов АИС, необходимых для проведения операции и достижения ею цели, функционирования по прямому назначению; *Оперативность*–характеризуется расходом операционного времени АИС, т.е. времени, потребного для достижения цели функционирования СЗИ от НСД. [4]
Черников Б.В.	*Уровень автоматизации* – характеризуется рациональностью функциональной структуры СЗИ от НСД, а именно с точки зрения взаимодействия с ней пользователя и использования вычислительных ресурсов АИС; *Временная эффективность* – способность СЗИ от НСД выполнять заданные действия за определенный интервал времени; *Ресурсоемкость* – минимально необходимые вычислительные ресурсы для эксплуатации СЗИ от НСД. [16]
Макколл Дж.А.	*Эффективность исполнения* – характеризуется минимальным временем функционирования СЗИ от НСД. *Эффективность хранения* – характеризуется эффективным доступом (минимальным временем) к информации, хранящейся в АИС. [23-24]
FEA Consolidated Reference Model Document	*Производительность* – свойство, характеризующее АИС или ее приложения с точки зрения времени отклика, интероперабельности, доступности пользователей и улучшения технических возможностей или характеристик; *Результативность* – степень удовлетворенности пользователей соответствующим приложением или системой, независимо от того, соответствует ли они требованиям пользователя, и их влияние на производительность операций.[25]

Для устранения приведенных недостатков, введем соответствующие показатели эффективности функционирования СЗИ от НСД, с помощью которых можно оценить реальную эффективность функционирования этих систем, приведенные в табл. 2.

Таблица 2. Показатели оценки эффективности функционирования системы защиты информации от несанкционированного доступа
Table 2. Indicators for assessing the effectiveness of the system of protecting information from unauthorized access

Показатель Index	Смысловое значение показателя The meaning of the indicator	Недостаток Drawback
$V_{ВЭСЗИ}$ Временная эффективность функционирования СЗИ от НСД	Способность СЗИ от НСД соответствовать заявленным к ним требованиям (с точки зрения временных параметров их функционирования), а также находить разумный компромисс между функционированием АИС по прямому предназначению и СЗИ от НСД.	1)-3)
$V_{РСЗИ}$ Ресурсоемкость СЗИ от НСД	Аналогично предыдущему	3)
$V_{ОСЗИ}$ Оптимальность программного кода СЗИ от НСД	Корректность программного кода СЗИ от НСД	1) и 5)
$V_{ФСЗИ}$ Функциональность СЗИ от НСД	Способность СЗИ от НСД при ее разработке, соответствовать предъявляемому уровню секретности, относительно ее функциональных компонентов. Данный показатель не соответствует недостаткам, так как процедура является традиционной.	-
$V_{УСЗИ}$ Моральное старение СЗИ от НСД	Способность СЗИ от НСД выполнять свои целевые функции по истечении определенного интервала времени, связанного с жизненным циклом функционирования СЗИ от НСД в АИС	1)-5)
$V_{ИЗСЗИ}$ Изменяемость СЗИ от НСД	Возможность изменения (с точки зрения уменьшения ее защитных функций) в связи с модификацией существующего ПО АИС.	5)

Представленные показатели можно структурировать в зависимости от эксплуатации СЗИ от НСД, в зависимости от имеющегося количества ресурсов АИС и от необходимого количества функций защиты СЗИ от НСД рис.1.

Показатели эффективности функционирования СЗИ от НСД представлены не единственной величиной, поэтому представим ее в векторной форме (1).

$$\vec{V} = V_{ВЭСЗИ}, V_{РСЗИ}, V_{ОСЗИ}, V_{ФСЗИ}, V_{УСЗИ}, V_{ИЗСЗИ}. \quad (1)$$

Из них частные показатели эффективности функционирования $V_{РСЗИ}, V_{ОСЗИ}, V_{ФСЗИ}, V_{УСЗИ}$, $V_{ИЗСЗИ}$ отражают адекватность типовой СЗИ от НСД требованиям по полноте имеющегося функционала СЗИ от НСД.

Расчет данных показателей осуществляют на основе эвристических методов путем определения адекватности СЗИ от НСД предъявляемым к ней требованиям на основе анализа её технической документации.

Расчет и измерение данных показателей эффективности функционирования типовой СЗИ от НСД в АИС необходимо произвести по соответствующей качественной шкале в виде булево-независимых переменных, где 1 – значение данного показателя соответствует заявленному свойству СЗИ от НСД и можно интерпретировать как соответствие предъявляемым требованиям, а 0 – значение данного показателя не соответствует заявленному свойству СЗИ от НСД, и можно интерпретировать как несоответствие предъявляемым требованиям, где s стратегия функционирования СЗИ от НСД.

Динамический (количественный) показатель эффективности функционирования при

разработке типовой СЗИ от НСД в АИС «временная эффективность функционирования СЗИ от НСД» $V_{ВЭСЗИ}$ является отражением вероятностно-временных характеристик динамики функционирования этих систем, которые оказывают прямое и непосредственное влияние на эффективность функционирования АИС по прямому назначению.

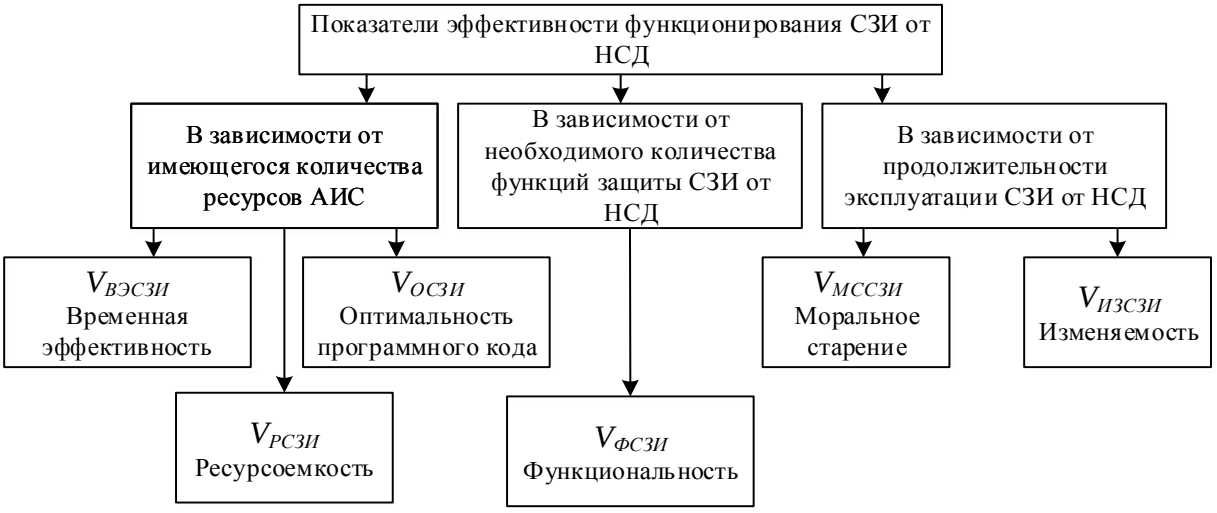

Рис. 1. Структурная схема показателей эффективности функционирования системы защиты информации от несанкционированного доступа в автоматизированной информационной системе
Fig. 1. Structural diagram of the performance indicators of the information protection system from unauthorized access in the automated information system

$$V_{РСЗИ}(s), V_{ОСЗИ}(s), V_{ФСЗИ}(s), V_{УСЗИ}(s), V_{ИЗСЗИ}(s) = \begin{cases} 1, \textit{ соответствует свойству}; \\ 0, \textit{ не соответствует свойству}. \end{cases} \quad (2)$$

Реализация функций СЗИ от НСД, как показывает опыт эксплуатации, ведет к значительному отвлечению вычислительных ресурсов АИС (процессорного времени и оперативной памяти), что приводит к увеличению времени отклика в этих системах и является неприемлемым для выполнения АИС своих функций по прямому назначению.

Поэтому при разработке СЗИ от НСД технические требования задаются на этапе 6 [3] в виде области допустимых значений, которые могут быть получены в результате натурного эксперимента, а также при имитационном моделировании.

$$V_{ВЭСЗИ}(s) = \begin{cases} 1, \textit{если } V_{ВЭСЗИ}(s) \le V^{тр}; \\ 0, \textit{если } V_{ВЭСЗИ}(s) > V^{тр}. \end{cases} \quad (3)$$

Таким образом, динамический показатель эффективности функционирования $V_{ВЭСЗИ}$ СЗИ от НСД в АИС определяется как вероятность своевременной реализации функционала СЗИ от НСД, основанного на выбранной стратегии и описывается математическим выражением (4):

$$V_{ВЭСЗИ}(s) = P(s(\tau) \le s(\tau^{тр})). \quad (4)$$

где τ – время выполнения СЗИ от НСД своего функционала в АИС, $\tau_{тр}$ – максимально допустимое время выполнения своего функционала в АИС, указанного в технической документации по эксплуатации в разделе «защита информации от НСД».

Оценка данного показателя эффективности функционирования типовой СЗИ от НСД в АИС необходимо осуществить на основе анализа разработанной сети Петри как марковской цепи с конечным числом состояний, причем последнее является поглощающим [24].

Для описания соответствия реального результата функционирования СЗИ от НСД, введем функцию соответствия s, которая показывает степень достижения цели функционирования СЗИ от НСД по некоторой шкале.

$$z = z(s(\tau), s(\tau^{mp})). \quad (5)$$

Соответственно показатель временной эффективности СЗИ от НСД есть математическое ожидание от функции соответствия (6).

$$V_{ВЭСЗИ}(s) = [z(s(\tau), s(\tau^{mp}))]. \quad (6)$$

Динамический показатель эффективности функционирования при разработке типовой СЗИ от НСД в АИС «временная эффективность функционирования СЗИ от НСД»$V_{ВЭСЗИ}$ является главным, а остальные будут определяться по правилу (4).

Тогда в общем виде функционирование СЗИ от НСД в АИС должно соответствовать выражению (7).

$$\begin{cases} V_{ВЭСЗИ}(s) \le V^{mp}; \\ V_{РСЗИ}(s), V_{ОСЗИ}(s), V_{ФСЗИ}(s), V_{УСЗИ}(s), V_{ИЗСЗИ}(s) = V_{bool}{}^{mp}. \end{cases} \quad (7)$$

Интегральную оценку эффективности функционирования типовой СЗИ от НСД в АИС необходимо провести с использованием интегрального показателя эффективности функционирования СЗИ от НСД в АИС, агрегирующего приведенные выше частные показатели в один интегральный показатель эффективности функционирования этих систем.

Выше изложенное позволяет провести оценку интегрального показателя эффективности функционирования СЗИ от НСД в АИС с помощью выражения (2, 3) получим (8) [26]:

$$\vec{V}_{ИСЗИ}(s) = \begin{cases} \vec{V}_{ВЭСЗИ}(s), & \textit{если} \quad V_{РСЗИ}(s) \wedge V_{ОСЗИ}(s) \wedge V_{ФСЗИ}(s) \wedge V_{УСЗИ}(s) \wedge V_{ИЗСЗИ}(s) = 1, \\ 0, & \textit{иначе} \end{cases} \quad (8)$$

Критерий эффективности представляет собой руководящее правило, позволяющее оценивать степень достижения цели СЗИ от НСД, относительно затрачиваемых при этом ресурсов.

Как было сказано выше показатели $V_{РСЗИ}, V_{ОСЗИ}, V_{ФСЗИ}, V_{УСЗИ}, V_{ИЗСЗИ}$ являются булевыми, поэтому задачу определения критерия эффективности можно свести к определению критерия по показателю $V_{ВЭСЗИ}$.

Как и в оценке качества, так и в оценке эффективности, реализуется совокупность критериев, каждый из которых относится к определенной концепции, согласно теории эффективности, выделяют следующие [8-10]:

- концепция пригодности – предполагает приемлемость любой стратегии функционирования, удовлетворяющей необходимым требованиям, из которых минимально выделяется одна;
- концепция оптимальности – предполагает стратегию рационального выбора из заданного ограниченного множества пригодных, которые обеспечивают наилучшую результативность (максимальный эффект);
- концепция адаптивности – предполагает прогнозирование возможных стратегий и способов их проведения на основе не только статической, но и изменяющейся информации. Концепция направлена, не только на выбор лучшей стратегии, но и к стремлению создания наиболее гибкой стратегии, которая учитывала все динамические свойства системы.

  В рамках концепции адаптивности, также можно использовать принцип самообучения, основанного на нейросетевых технологиях, что является перспективным направлением исследования, хотя слабо формализованным [9-10]

Критерий пригодности СЗИ от НСД, представляет собой выбор любой рациональной стратегии функционирования s, при которой показатель $V_{ВЭСЗИ}$ принимает значения не выше требуемого (9). На практике данное требование прописывается в техническом задании на разрабатываемую СЗИ от НСД.

$$V_{ВЭСЗИ}(s) \le V^{mp}, s \in S, \quad (9)$$

где исход всех положительных и отрицательных стратегий равноценен, а S есть множество допустимых значений.

Критерий оптимальности СЗИ от НСД, представляет собой выбор тех рациональных стратегий из множества пригодных, которые обеспечивают наибольшую результативность (максимальный эффект), то есть обеспечивает их предпочтительность (10).

$$V_{ВЭСЗИ}(s_{опт}) = \max V^{тр}(s), s \in S_{пр}, \quad (10)$$

где $s_{опт}$ есть множество оптимальных значений, а $S_{пр}$ область пригодных значений.

Критерий адаптивности СЗИ от НСД, представляет собой изменение стратегии s на основе не только статической, но и текущей и прогнозной информации с целью достижения или сохранения определенного состояния системы при изменяющемся комплексе условий проведения операции.

$$V_{ВЭСЗИ}(s_{опт}(\tau), l) \le V^{тр}_{ВЭСЗИ}(s(\tau), l),\ s(\tau) \in S(\tau, l), \quad (11)$$

где l – упреждение прогноза.

Как можно заметить, каждый последующий критерий является подмножеством множества стратегий предыдущего, что позволяет определить стратегию в зависимости от необходимой степени достижения цели разработки СЗИ от НСД.

На рис. 2 представлен алгоритм интегральной оценки эффективности функционирования СЗИ от НСД в АИС в соответствии с введенными критериями и показателями.

1 блок. Ввод исходных данных для работы алгоритма:

1) $V^{тр}_{ВЭСЗИ}$ – требуемое значение показателя временной эффективности функционирования СЗИ от НСД, определяемое в требованиях на этапе 6 [3] при разработке СЗИ от НСД;
2) $V_{РСЗИ}, V_{ОСЗИ}, V_{ФСЗИ}, V_{УСЗИ}, V_{ИЗСЗИ}.$ – значение показателей оценки эффективности СЗИ от НСД, определяемого на основе анализа документации.

2 блок. Двоичное умножение значений показателей эффективности функционирования СЗИ от НСД.$V_{РСЗИ}, V_{ОСЗИ}, V_{ФСЗИ}, V_{УСЗИ}, V_{ИЗСЗИ}$

3 блок. Проверка условия (2), если оно не выполняется, выполняется переход к блоку 10.

4 блок. Ввод критериев эффективности СЗИ от НСД.

5 блок. Вычисление значения показателя временной эффективности СЗИ от НСД $V_{ВЭСЗИ}$ в соответствии с алгоритмом представленном в [26].

6 блок. Проверка результата вычисления $V_{ВЭСЗИ}$ по критерию пригодности (9), при его выполнении осуществляется переход к блоку 7, при его достаточности переходим к блоку 11, а при невыполнении к блоку 10.

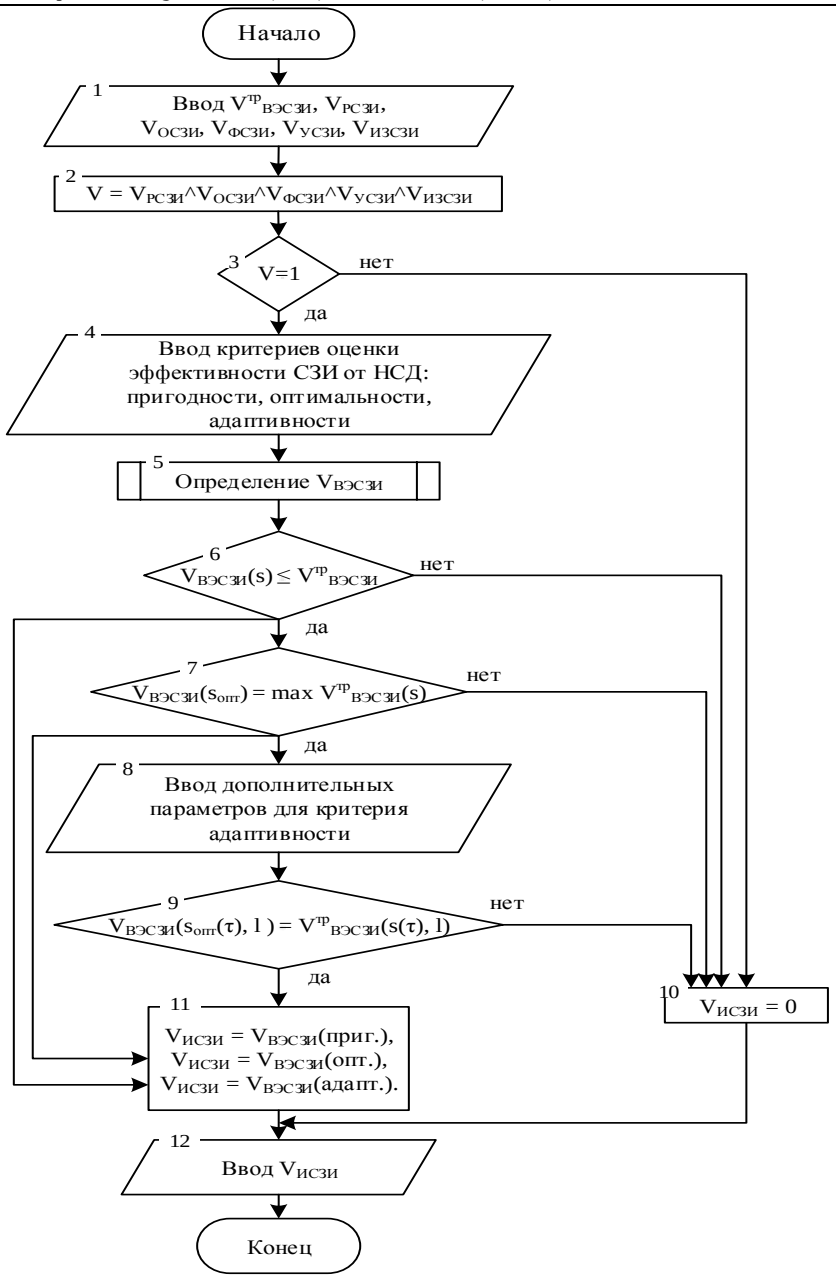

Рис. 2. Алгоритм оценки интегрального показателя эффективности функционирования при разработке системы защиты информации от несанкционированного доступа в автоматизированной информационной системе

Fig.2. Algorithm for estimating the integral indicator of the effectiveness of functioning in the development of a system for protecting information from unauthorized access in an automated information system

7 блок. Проверка результата вычисления $V_{ВЭСЗИ}$ по критерию оптимальности(10) с использованием множества пригодных стратегий, при его выполнении осуществляется переход к блоку 8, при его достаточности переходим к блоку 11, а при невыполнении к блоку 10.

8 блок. Ввод дополнительных параметров, используемых для самообучения, требующие учета в критерии адаптивности, в зависимости от поставленных задач при разработке СЗИ от НСД.

9 блок. Проверка результата вычисления $V_{ВЭСЗИ}$ по критерию адаптивности(11) с использованием множества оптимальных стратегий, при его выполнении осуществляется переход к блоку 11, при невыполнении к блоку 10.

10 блок. При невыполнении условий (2), (9), (10), (11) значение интегрального показателя эффективности функционирования СЗИ от НСД равно нулю.

11 блок. При выполнении условий (2), (9), (10), (11) интегрального показателя эффективности функционирования СЗИ от НСДоценивается по формуле $V_{ИСЗИ} = V_{ВЭСЗИ}$ следующей из равенства (8).

12 блок. Вывод найденного значения интегрального показателя эффективности функционирования СЗИ от НСД($V_{ИСЗИ}$) – результата работы алгоритма.

Обсуждение результатов. Проведенный анализ одного из качественных свойств эффективности функционирования, позволил учесть все характеристики, прописанные в нормативных документах и научной литературе, что позволило учесть нюансы, связанные с выбором показателей эффективности функционирования СЗИ от НСД.

Выявленные недостатки функционирования СЗИ от НСД позволили их сопоставить с выделяемыми характеристиками эффективности функционирования СЗИ от НСД, что в итоге дало возможность представить показатели эффективности функционирования СЗИ от НСД для исследуемой предметной области.

Предлагается оценить эффективности функционирования СЗИ от НСД, основываясь, как на динамических показателях, так и на статических, что согласно теории эффективности, является наиболее перспективным.

Представленные критерии позволяют учитывать множественные варианты функционирования СЗИ от НСД, что позволяет осуществить выбор стратегии согласно цели разработки.

Перспективным направление в этой области является усовершенствование критерия эффективности с учетов принципов самообучения. Алгоритм интегральной оценки эффективности функционирования СЗИ от НСД поэтапно описывает порядок действий (методику) оценки и аккумулирует в себе как представленные показатели, так и критерии.

Вывод. Разработанная концепция позволит на основе как экспериментальных, так и имитационных данных оценивать эффективность функционирования СЗИ от НСД в АИС.

Представленные метрики и критерии направлены на повышение уровня надёжности СЗИ от НСД в АИС с точки зрения выбора оптимальной стратегии функционирования при разработке подобных систем.

Библиографический список:

1. ФСТЭК Руководящий документ Защита от несанкционированного доступа к информации. Термины и определения. URL: https://fstec.ru/component/attachments/download/298 (дата обращения: 26.02.2018).
2. Герасименко В.Г. Проблемы обеспечения информационной безопасности при использовании открытых информационных технологий в системах критических приложений // Информация и безопасность: Регион.науч.-техн. вестник. – Воронеж: ВГТУ, 1999. – Вып. 4. – С. 66–67.
3. Е. А. Рогозин, А. Д. Попов, Т. В. Шагиров. Проектирование систем защита информации от несанкционированного доступа в автоматизированных системах органов внутренних дел // Вестник Воронежского института МВД России. – 2016. – № 2. – С. 174 – 183.
4. Петухов Г. Б., Якунин В. И. Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем. М: АСТ, 2006. 504 с.
5. Авдуевский В. С. [и др.] Надежность и эффективность в технике: Т. 1 Методология. Организация. Терминология / под ред. А. И. Рембезы. М: Машиностроение, 1986. 224 с.
6. Дробин В. У. [и др.] Надежность и эффективность в технике: Т. 3 Эффективность технических систем / под общ.ред. В. Ф. Уткина, Ю. В. Крючкова. М: Машиностроение, 1988. 328 с.
7. ФСТЭК РФ. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. URL: https://fstec.ru/component/attachments/download/299 (дата обращения: 26.02.2018).
8. ГОСТ 28806-90 Качество программных средств. Термины и определения. URL: http://www.kimmeria.nw.ru/standart/glosys/gost_28806_90.pdf (дата обращения: 23.02.2018).
9. ISO/IEC TR 9126-2:2003 Software engineering – Product quality – Part 2: External metrics.URL: https://www.iso.org/standard/22750.html (датаобращения: 26.02.2018).
10. ISO/IEC TR 9126-3:2003 Software engineering – Product quality – Part 3: Internal metrics. URL: https://www.iso.org/standard/22891.html (датаобращения: 26.02.2018).
11. ISO/IEC TR 9126-4:2004 Software engineering – Product quality – Part 4: Quality in use metrics. URL: https://www.iso.org/standard/39752.html (датаобращения: 26.02.2018).
12. СЗИ «Страж NT». Руководство администратора. URL: http://www.guardnt.ru/download/doc/admin_guide_nt_3_0.pdf (дата обращения: 23.02.2018).
13. Система защиты информации от несанкционированного доступа «Страж NT». Описание применения. URL: http://www.rubinteh.ru/public/opis30.pdf (дата обращения: 23.02.2018).
14. Липаев В. В. Качество программных средств. Методические рекомендации. / под. общ. ред. А. А. Полякова. М.: Янус-К, 2002. 400 с.
15. БоэмБ., Браун Дж., Каспар Х.[и др.] Характеристики качества программного обеспечения / пер. с англ. Е. К.

Масловского. М.: Мир, 1981. 208 с.
16. Черников Б. В., Поклонов Б. Е. Оценка качества программного обеспечения: Практикум: учебное пособие. М.: ИД «ФОРУМ»: ИНФРА-М, 2012. 400 с.
17. Герасименко В. А., Малюк А. А. Основы защиты информации Москва: МИФИ, 1997. 537 с.
18. ГОСТ Р 50922–2006 Защита информации. Основные термины и определения. – М.: Стандартинформ, 2006. – 12 с.
19. Юсупов Р. М., Мусаев А. А. Особенности оценивания эффективности информационных систем и технологий. // Труды СПИИРАН. — 2017. — № 2 (51). — С. 5 — 34.
20. The Research and Discussion on Effectiveness Evaluation of Software Protection Huaijun Wang; Dingyi Fang; Junhuai Li; Yong Chang; Lei Yu 2016 12th International Conference on Computational Intelligence and Security (CIS) Year: 2016 Pages: 628 – 632 IEEE Conferences
21. Method to Evaluate Software Protection Based on Attack Modeling Huaijun Wang; Dingyi Fang; Ni Wang; Zhanyong Tang; Feng Chen; Yuanxiang Gu 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing Year: 2013 Pages: 837 – 844 Cited by: Papers (1) IEEE Conferences.
22. ГОСТ 25010–2015 Требования и оценка качества систем и программного обеспечения (SQuaRE). Модели качества систем и программных продуктов URL: http://ingraf.su/wp-content/uploads/GOST-R-ISO-MEK-25010-2015.pdf(дата обращения: 21.02.2018).
23. McCall J.A., Richards P.K., Walters G.F. Factors in Software Quality: Metric Data Collection and Validation. Final Technical Report. Vol. 2. National Technical Information Service, Springfield. 1977.
24. McCall J.A., Richards P.K., Walters G.F. Factors in Software Quality: Preliminary Handbook.
25. FEA Consolidated Reference Model Document.
26. Дровникова И. Г., Мещерякова Т. В., Попов А. Д, Рогозин Е. А., Ситник С.М. Математическая модель оценки эффективности систем защиты информации с использованием преобразования Лапласа и численного метода Гивенса // Труды СПИИРАН. – 2017. – № 3 (52). – С. 234–258.

References:

1. FSTEK Rukovodyashchii dokument Zashchita ot nesanktsionirovannogo dostupa k informatsii. Terminy i opredeleniya. URL: https://fstec.ru/component/attachments/ download/ 298 (data obrashcheniya: 26.02.2018). [FSTEK Guidance document Protection against unauthorized access to information. Terms and Definitions. URL: https://fstec.ru/component/attachments/download/298 (access date: 26.02.2018). (In Russ.)]
2. Gerasimenko V.G. Problemy obespecheniya informatsionnoi bezopasnosti pri ispol'zovanii otkrytykh informatsionnykh tekhnologii v sistemakh kriticheskikh prilozhenii. Informatsiya i bezopasnost': Region. nauch.-tekhn. vestnik. Voronezh: VGTU. 1999;4:66 - 67. [Gerasimenko V.G. Problems of ensuring information security when using open information technologies in critical application systems. Information and Security: Region. nauch.-tekhn. vestnik. Voronezh: VGTU. 1999;4:66 - 67. (In Russ.)]
3. Rogozin E.A., Popov A D., Shagirov T.V. Proektirovanie sistem zashchita informatsii ot nesanktsionirovannogo dostupa v avtomatizirovannykh sistemakh organov vnutrennikh del. Vestnik Voronezhskogo instituta MVD Rossii. 2016;2:174 - 183. [Rogozin E.A., Popov A D., Shagirov T.V. Designing systems to protect information from unauthorized access in automated systems of internal affairs bodies. The Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia. 2016;2:174 - 183. (In Russ.)]
4. Petukhov G.B., Yakunin V.I. Metodologicheskie osnovy vneshnego proektirovaniya tselenapravlennykh protsessov i tseleustremlennykh sistem. M: ACT; 2006. 504 s. [Petukhov G.B., Yakunin V.I. Methodological bases of external designing of purposeful processes and purposeful systems. M: ACT; 2006. 504 p. (In Russ.)]
5. Avduevskii V.S. i dr. Nadezhnost' i effektivnost' v tekhnike: T. 1 Metodologiya. Organizatsiya. Terminologiya. Pod red. A.I. Rembezy. M: Mashinostroenie; 1986. 224 s. [Avduevskii V.S. et al. Reliability and efficiency in technology: V. 1 Methodology. Organisation. Terminology. A.I. Rembeza (Ed.). M: Mashinostroenie; 1986. 224 p. (In Russ.)]
6. Drobin V.U. i dr. Nadezhnost' i effektivnost' v tekhnike: T. 3 Effektivnost' tekhnicheskikh sistem. Pod red. V.F. Utkina, Yu. V. Kryuchkova. M: Mashinostroenie; 1988. 328 s. [Drobin V.U. et al. Reliability and efficiency in technology: V. 3 Efficiency of technical systems. V.F. Utkin, Yu. V. Kryuchkov (Eds.). M: Mashinostroenie; 1988. 328 p. (In Russ.)]
7. FSTEK RF. Rukovodyashchii dokument. Kontseptsiya zashchity sredstv vychislitel'noi tekhniki i avtomatizirovannykh sistem ot nesanktsionirovannogo dostupa k informatsii. URL: https://fstec.ru/component/attachments/ download/299 (data obrashcheniya: 26.02.2018). [FSTEK of the Russian Federation. Guidance document. The concept of protecting computer facilities and automated systems from unauthorised access to information. URL: https://fstec.ru/component/attachments/download/299 (access date: 26.02.2018). (In Russ.)]
8. GOST 28806-90 Kachestvo programmnykh sredstv. Terminy i opredeleniya. URL: http://www.kimmeria.nw.ru/standart/glosys/gost_28806_90.pdf (data obrashcheniya: 23.02.2018). [GOST 28806-90 The quality of software. Terms and Definitions. URL: http://www.kimmeria.nw.ru/standart/glosys/gost_28806_90.pdf (access date: 23.02.2018). (In Russ.)]
9. ISO/IEC TR 9126-2:2003 Software engineering – Product quality – Part 2: External metrics. URL: https://www.iso.org/standard/22750.html (access date: 26.02.2018).]
10. ISO/IEC TR 9126-3:2003 Software engineering – Product quality – Part 3: Internal metrics. URL: https://www.iso.org/standard/22891.html (access date: 26.02.2018).
11. ISO/IEC TR 9126-4:2004 Software engineering – Product quality – Part 4: Quality in use metrics. URL: https://www.iso.org/standard/39752.html (access date: 26.02.2018).
12. SZI "Strazh NT". Rukovodstvo administratora. URL: http://www.guardnt.ru/download/doc/admin_guide_nt_3_0.pdf (data obrashcheniya: 23.02.2018). [SZI "Strazh NT". Administrator's guide. URL: http://www.guardnt.ru/download/doc/admin_guide_nt_3_0.pdf (access date: 23.02.2018). (In Russ.)]
13. Sistema zashchity informatsii ot nesanktsionirovannogo dostupa "Strazh NT". Opisanie primeneniya. URL: http://www.rubinteh.ru/public/opis30.pdf (data obrashcheniya: 23.02.2018). [System to protect information from unauthorised access "Strazh NT". Description of the application. URL: http://www.rubinteh.ru/public/opis30.pdf (access date: 23.02.2018). (In Russ.)]
14. Lipaev V. V. Kachestvo programmnykh sredstv. Metodicheskie rekomendatsii. Pod.red. A. A. Polyakova. M.: Yanus-K; 2002. 400 s. [Lipaev V. V. The quality of software. Guidelines. A. A. Polyakov (Ed.). M.: Yanus-K; 2002. 400 p. (In Russ.)]
15. Boem B., Braun Dzh., Kaspar Kh. i dr. Kharakteristiki kachestva programmnogo obespecheniya. M.: Mir; 1981. 208

s. [Boem B., Braun Dzh., Kaspar Kh. et al. Characteristics of software quality. M.: Mir; 1981. 208 p. (In Russ.)]
16. Chernikov B.V., Poklonov B.E. Otsenka kachestva programmnogo obespecheniya: Praktikum: uchebnoe posobie. M.: ID "FORUM": INFRA-M; 2012. 400 s. [Chernikov B.V., Poklonov B.E. Evaluation of software quality: Workshop: a tutorial. M.: ID "FORUM": INFRA-M; 2012. 400 p. (In Russ.)]
17. Gerasimenko V.A., Malyuk A.A. Osnovy zashchity informatsii Moskva: MIFI; 1997. 537 s. [Gerasimenko V.A., Malyuk A.A. Fundamentals of Information Security: MIFI; 1997. 537 p. (In Russ.)]
18. GOST R 50922–2006 Zashchita informatsii. Osnovnye terminy i opredeleniya. M.: Standartinform; 2006. 12 s. [GOST R 50922–2006 Information protection. Basic terms and definitions. M.: Standartinform; 2006. 12 p. (In Russ.)]
19. Yusupov R.M., Musaev A.A. Osobennosti otsenivaniya effektivnosti informatsionnykh sistem i tekhnologii. Trudy SPIIRAN. 2017; 2(51):5 - 34. [Yusupov R.M., Musaev A.A. Features of the evaluation of the effectiveness of information systems and technologies. Collected works of SPIIRAN. 2017; 2(51):5 - 34. (In Russ.)]
20. Wang H., Fang D., Li J., Chang Y., Yu L. The Research and Discussion on Effectiveness Evaluation of Software Protection. 12th International Conference on Computational Intelligence and Security (CIS) Year: 2016. P. 628 – 632.
21. Wang H., Fang D., Wang N., Tang Z., Chen F., Gu Y. Method to Evaluate Software Protection Based on Attack Modeling. IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing Year: 2013 P. 837 – 844.
22. GOST 25010–2015 Trebovaniya i otsenka kachestva sistem i programmnogo obespecheniya (SQuaRE). Modeli kachestva sistem i programmnykh produktov URL: http://ingraf.su/wp-content/uploads/GOST-R-ISO-MEK-25010-2015.pdf (data obrashcheniya: 21.02.2018). [GOST 25010–2015 Requirements and assessment of the quality of systems and software (SQuaRE). Models of quality of systems and software products. URL: http://ingraf.su/wp-content/uploads/GOST-R-ISO-MEK-25010-2015.pdf (access date: 21.02.2018). (In Russ.)]
23. McCall J.A., Richards P.K., Walters G.F. Factors in Software Quality: Metric Data Collection and Validation. Final Technical Report. Vol. 2. National Technical Information Service, Springfield. 1977.
24. McCall J.A., Richards P.K., Walters G.F. Factors in Software Quality: Preliminary Handbook.
25. FEA Consolidated Reference Model Document.
26. Drovnikova I.G., Meshcheryakova T.V., Popov A.D, Rogozin E.A., Sitnik S.M. Matematicheskaya model' otsenki effektivnosti sistem zashchity informatsii s ispol'zovaniem preobrazovaniya Laplasa i chislennogo metoda Givensa. Trudy SPIIRAN. 2017;3(52):234 - 258. [Drovnikova I.G., Meshcheryakova T.V., Popov A.D, Rogozin E.A., Sitnik S.M. A mathematical model for evaluating the effectiveness of information security systems using the Laplace transform and the Givens numerical method. Collected works of SPIIRAN. 2017;3(52):234 – 258. (In Russ.)]

Сведения об авторах:

Качаева Гюльханум Ибадулаховна – кандидат экономических наук, заведующая кафедрой информационной безопасности.

Попов Антон Дмитриевич – адъюнкт.

Рогозин Евгений Алексеевич – доктор технических наук, профессор, кафедра автоматизированных информационных систем.

Information about the author.

Gyulkhanum I. Kachaeva– Cand. Sci.(Economics), Head of the Information Security Department.

Anton D. Popov– Adjunct.

Evgeny A. Rogozin – Dr. Sci. (Technical), Prof., Department of Automated information systems.

Конфликт интересов
Авторы заявляют об отсутствии конфликта интересов.

Поступила в редакцию 23.12.2017.
Принята в печать 31.01.2018.

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

Received 23.12.2017.
Accepted for publication 31.01.2018.