Сергей Д. Кулик
*Национальный исследовательский ядерный университет «МИФИ»,*
*Каширское ш., 31, г. Москва, 115409, Россия*
*e-mail: sedmik@mail.ru, https://orcid.org/0000-0002-9578-9010*

# ПРИМЕНЕНИЕ СИСТЕМНОГО АНАЛИЗА ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

*DOI: http://dx.doi.org/10.26583/bit.2019.1.03*

*Аннотация.* В работе основное внимание сосредоточено на важных элементах системного анализа, таких как принципы, показатели и критерий эффективности системы. Цель данной работы – показать возможность применения системного анализа и системного подхода в области информационной безопасности. Для этой области специально выделен третий принцип теории систем и системного анализа, посвященный максимальной эффективности работы системы, и 15-й принцип системного подхода, связанный с оптимальной эффективностью. В работе успешно использованы необходимые принципы и методы системного анализа, а также разработан программный комплекс для применения системного анализа при исследовании показателя эффективности. На данное программное средство получено свидетельство Федеральной службы по интеллектуальной собственности Российской Федерации. Элементы системного анализа рассматриваются как необходимый инструмент для решения важных практических задач системного анализа в области информационной безопасности. Введен показатель и критерий эффективности системы, связанный с разностью приведенных затрат, проведен анализ показателя на демонстрационном примере. Выделены области значений параметров, при которых значение показателя эффективности меньше или больше нуля, зафиксировано, что с ростом интенсивности работы контроля доступа растет показатель эффективности. В заключении делается вывод о необходимости уделять больше внимания основным элементам системного анализа и системного подхода в области информационной безопасности.

*Ключевые слова: системный анализ, система, показатель эффективности, критерий эффективности, информационная система, информационная безопасность.*

*Для цитирования: КУЛИК, Сергей Д. ПРИМЕНЕНИЕ СИСТЕМНОГО АНАЛИЗА ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], p. 25-35, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1177>. Дата доступа: 19 feb. 2019. doi:http://dx.doi.org/10.26583/bit.2019.1.03.*

Sergey D. Kulik
*National Research Nuclear University MEPhI,*
*Kashirskoye shosse, 31, Moscow, 115409, Russia*
*e-mail: sedmik@mail.ru, https://orcid.org/0000-0002-9578-9010*

## System analysis for evaluating the effectiveness of tools for information security

*DOI: http://dx.doi.org/10.26583/bit.2019.1.03*

*Abstract.* The paper focuses on important elements of system analysis such as principles, indicators and criteria of system efficiency. The aim of this work is to show the possibility of applying system analysis and system approach in the field of information security. In this field the 3rd principle of the theory of systems and systems analysis (the maximum efficiency of the system) and the 15th principle of the systems approach, associated with optimal efficiency, are specially highlighted. The main focus is on the effectiveness of the system, which can be assessed using special indicators. We have used the necessary principles and methods of system analysis, as well as special software for applying the elements of system analysis for the performance indicators. In this case special software is considered as a tool for solving problems of system analysis in the field of information security. We introduced an indicator and criterium of system efficiency associated with the difference in reduced costs. The result of the optimization of the information security effectiveness indicator is demonstrated on a special example. The researchers use the system analysis elements. Researchers solve optimization problems. Recommendations were developed for solving typical educational problems. It is concluded that it is necessary to pay more attention in the framework of the educational process to the elements of system analysis.

*Keywords: system analysis, system, indicator of effectiveness, criterion of effectiveness, information system, information security.*
*For citation: KULIK, Sergey D. System analysis for evaluating the effectiveness of tools for information security. IT Security (Russia), [S.l.], p. 25-35, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1177>. Date accessed: 19 feb. 2019. doi:http://dx.doi.org/10.26583/bit.2019.1.03.*

## Введение

В настоящее время различным вопросам информационной безопасности уделяется большое внимание. Об этом свидетельствуют многие публикации, например, [1 - 4]. Важные вопросы «Больших данных», облачных технологий и электронного обучения [1, 3, 4] не остаются в стороне от современных исследований. В работах [5, 6] рассмотрены специальные средства для обеспечения информационной безопасности и фактографические системы. В статьях [7, 8] рассмотрены вопросы обеспечения информационной безопасности автомобильных сетей связи (VANET) и обеспечение киберустойчивости на базе технологии программно-конфигурируемых сетей. Для повышения эффективности работы автоматизированных средств обеспечения информационной безопасности (АСОИБ) в работе [5] предлагается для подсистемы контроля доступа использовать фактографическую систему. При этом методам и средствам системного анализа в области информационной безопасности уделяется недостаточно внимания. Следует отметить стандарт ISO/IEC TR 27016, который посвящен экономике и оценке затрат на информационную безопасность (ИБ). В работе [6], на базе принципов системного анализа и системного подхода [9 - 12] введены необходимые частные показатели, связанные с оценкой эффективности средств ИБ и фактографических информационных систем. Данная работа, опираясь на [12, 14, 15], также показывает возможность применения системного анализа в сфере ИБ. Для этого рассматриваются различные затраты и показатели [16 - 19], связанные с ними. Цель данной работы – показать возможность применения системного анализа и системного подхода в области информационной безопасности.

## 1. Системный анализ и системный подход

В теории систем и системного анализа [11, с. 12] к настоящему времени выработаны необходимые шесть принципов. Очень кратко эти принципы можно представить следующим образом:

1. Набор элементов системы представляется как целое (запрещается представлять систему как простое объединение элементов).
2. Свойства системы не является суммой свойств элементов этой системы (система имеет свойства (или свойство), которых нет у ее частей).
3. Необходимо стремиться к максимальной эффективности работы системы (достаточно часто применяют какой-то экономический показатель).
4. Нельзя представлять систему в виде автономной системы (требуется учет внешних связей, при этом система анализируется как некоторая часть какой-то более общей системы).
5. Анализируемую систему можно делить на какие-то части.
6. Систему необходимо анализировать на всех этапах ее жизненного цикла.

Достаточно полно основные принципы системного подхода представлены в работе [10]. Более кратко следуя работам [9, 10, 12] некоторые наиболее важные из них для области информационной безопасности представлены в табл. 1.

*Таблица 1. Основные принципы системного подхода*

| № | Название | Краткие пояснения |
|---|---|---|
| 1. | Принцип целеполагания | Цель системы задается вне ее (т.е. задается над системой). Эта цель определяет поведение системы. Полагают, что целеполагание — процесс выработки цели |
| 2. | Принцип обратной связи | Реакция системы на воздействие должна минимизировать отклонение системы от траектории к цели (полагают [12], что игнорирование обратной связи неизбежно приведет к потере управляемости) |
| 3. | Принцип целеустремленности | Система стремится к заданной цели |
| 4. | Принцип оптимального разнообразия | Предельно организованные и предельно неорганизованные системы мертвы |
| 5. | Принцип эмерджентности | Система как целое имеет свойства, которых нет у ее частей |
| 6. | Принцип согласия | Цели элементов (например, подсистем) не должны противоречить [12] цели системы |
| 7. | Принцип причинности | Любое изменение состояния системы связано с некоторой совокупностью условий (причинами), порождающих это изменение |
| 8. | Принцип «черного ящика» | Внутреннее содержание исследуемого объекта не рассматривается |
| 9. | Принцип многообразия | Чем многообразнее система, тем она устойчивее. Этот принцип отражает закон необходимого разнообразия У. Р. Эшби [9, с.41 - 42] |
| 10. | Принцип энтропии | Изолированная (закрытая) система погибает [12] |
| 11. | Принцип отсутствия лишнего | Лишний элемент системы погибает [12] |
| 12. | Принцип агонии | Ничто не гибнет без борьбы [12] (гибель элементов системы сопровождается нанесением ей вреда) |
| 13. | Принцип сохранения количества материи | Количество материи (вещества и энергии), поступающей в систему, равно количеству материи, образующейся в результате деятельности (функционирования) этой системы |
| 14. | Принцип нелинейности | Реальные системы всегда нелинейные [12] |
| 15. | Принцип оптимальной эффективности | Максимальная эффективность функционирования системы достигается на грани устойчивости этой системы |
| 16. | Принцип слабой связи | Связи между элементами системы должны быть достаточно слабыми для обеспечения живучести и необходимо прочными для сохранения целостности системы |
| 17. | Принцип Глушкова | Любой многомерный критерий качества какой-либо системы может быть сведен к одномерному выходом в системы более высокого порядка (надсистемы) [12] |
| 18. | Принцип относительной случайности | Случайность в данной системе может оказаться строго детерминированной зависимостью в надсистеме [12] |
| 19. | Принцип детерминизма | Причина изменения состояния системы всегда лежит вне системы [12] |
| 20. | Принцип полноты связей | Связи в системе должны обеспечивать достаточно полное взаимодействие подсистем [12] |

В системном анализе достаточно часто применяется и поясняется принцип № 8 (табл. 1), когда внутреннее содержание исследуемого объекта (элемента системы) не рассматривается. В данной работе он также используется (содержимое элементов системы не раскрывается и не поясняется). Анализ третьего принципа системного анализа, связанного с необходимостью стремиться к максимальной эффективности работы системы, и 15-го принципа системного подхода, связанного с оптимальной эффективностью (табл. 1), показывает, что надо как-то с помощью показателей оценивать затраты и затем их минимизировать. Кратко остановимся на этом.

## 2. Оценка затрат, показатели и критерий эффективности

При выполнении системного анализа для сравнения вариантов систем часто используются приведенные затраты. Далее будем следовать работам [15 - 20], частично опираться на принцип № 17 и постараемся вместо многомерного критерия качества системы использовать критерий меньшей размерности, например, двумерный для демонстрационного примера.

Стандарт ISO/IEC TR 27016 [19] посвящен проблемам экономики и оценки затрат на информационную безопасность. В работе [20] выполнен сравнительный анализ нескольких методов оценки затрат, основанных на:

- рекомендациях ISO/IEC TR 27016:2014;
- модели Guido Schryen;
- методике TEI (компании Forrester Consulting);
- классическом методе оценки инвестиционного проекта.

В табл. 2 представлен краткий сравнительный анализ различных подходов к оценке выгод и затрат на ИБ. Из табл. 2 следует, что стандарт ISO/IEC TR 27016 имеет больше преимуществ по сравнению с другими подходами. Поэтому окончательную финальную оценку следует выполнять согласно рекомендациям этого стандарта ISO/IEC TR 27016. Полный расчет оценки затрат на информационную безопасность достаточно трудоемкий. Поэтому предлагается на начальном этапе выполнять приближенную оценку эффективности затрат. Предварительную приближенную оценку предлагается выполнять следующим образом.

Затраты на реализацию системы контроля доступа в сфере ИБ (обозначим их показателем – $K_0$) необходимо учитывать при анализе ее конкурирующих вариантов. Действительно, с одной стороны, вложив больше средств на приобретение более быстродействующих накопителей и средств распознавания и принятия решений, можно существенно улучшить временные и иные характеристики системы и тем самым повысить ее эффективность.

*Таблица 2. Сравнительный анализ подходов к оценке выгод и затрат на ИБ* [20]

| **Параметр для сравнения** | **Классический подход** | **TEI** | **Модель Guido Schryen** | **ISO/IEC TR 27016:2014** |
|---|---|---|---|---|
| Учет бизнес-требований | Нет | Нет | Нет | Да |
| Учет ограничений безопасности | Нет | Нет | Да | Да |
| Учет бюджетных ограничений | Нет | Нет | Да | Да |
| Оценка рисков | Нет | Да | Нет | Да |
| Количественная оценка показателей экономической эффективности инвестиций | Да | Да | Нет | Нет |
| Многокритериальность | Да | Да | Нет | Да |
| Наличие методики количественной оценки затрат и выгод | Да | Да | Нет | Нет |

С другой стороны, вложенные затраты должны окупиться в течение заданного срока окупаемости, который обозначим показателем $T_{окуп}$. При оценке экономической эффективности технических систем выполняют анализ различных затрат [18], при этом эффективность вложенных затрат на реализацию определяется сроком их окупаемости. Известно, что величина показателя $E_н$, обратная к $T_{окуп}$, есть нормативный коэффициент эффективности (окупаемости) затрат, который для некоторых отраслей при $E_н$=0.15 соответствует сроку окупаемости в 6 – 7 лет. На практике значения показателя $K_0$ можно получить путем анализа отчетных финансовых документов для существующих систем (поскольку уже известны затраты на их реализацию) или расчетным путем с использованием средств моделирования для проектируемых систем.

Приведенные затраты системы контроля доступа в сфере информационной безопасности, например, для АСОИБ, за один год, в течение которого обрабатывается $A_0$ запросов к ней, определяются следующим известным образом [17, 18]:

$$З_i = \tilde{S}_i + E_н \cdot \tilde{K}_i , \quad (1)$$

где используемые показатели означают следующее:

при $i$=1, $З_i$=$З_1$ – это затраты *базового* варианта системы на обработку $A_0$ запросов;

при $i$=0, $З_i$=$З_0$ – это затраты *нового* варианта системы на обработку $A_0$ запросов;

$\tilde{S}_i$ – усредненные затраты на эксплуатацию системы контроля доступа;

$\tilde{K}_i$ – затраты на разработку, изготовление и внедрение системы контроля доступа.

На практике, разность затрат $\Delta З$ следует вычислять для двух вариантов систем информационной безопасности, поставленных в сопоставимые условия для их сравнения. Эти условия либо заданы в техническом задании (ТЗ), либо выбираются разработчиком системы по согласованию с заказчиком.

Воспользуемся результатами работ [17, 18]. Из них следует, что показатель разности приведенных затрат $Э_0 = \Delta З = З_1 - З_0$ вычисляют с помощью показателя $A_0$ и показателей приведенных затрат на единицу конечного результата КР (продукции) для каждого из двух сравниваемых вариантов систем контроля доступа в сфере информационной безопасности, где $A_0$ –это показатель годового объема производства КР.

Далее, следуя работе [17, с. 18 – 19], при $A_0 \neq 0$ последовательно получаем:

$$Э_0 = \Delta З = З_1 - З_0 = \left(\tilde{S}_1 - \tilde{S}_0\right) - E_н\left(\tilde{K}_0 - \tilde{K}_1\right) = \left(\tilde{S}_1 - \tilde{S}_0\right) - E_н \cdot K_0 = A_0\left(\frac{\tilde{S}_1}{A_0} - \frac{\tilde{S}_0}{A_0}\right) - E_н \cdot K_0 \quad (2)$$

или при $C_1 = \frac{\tilde{S}_1}{A_0}$, $C_0 = \frac{\tilde{S}_0}{A_0}$, $K_0 = \tilde{K}_0 - \tilde{K}_1$

справедливо:

$$Э_0 = A_0 \cdot \left(C_1 - C_0\right) - E_н \cdot K , \quad (3)$$

где

$C_1$ – показатель усредненных эксплуатационных затрат базового варианта системы контроля доступа для информационной безопасности на обработку одного запроса;

$C_0$ – показатель усредненных эксплуатационных затрат предлагаемого варианта системы контроля доступа для информационной безопасности на обработку одного запроса.

По знаку и величине $Э_0$ будем судить об эффективности предлагаемого варианта системы по отношению к базовому варианту. Далее будем опираться на этот подход.

Для системы контроля доступа в сфере информационной безопасности, например для АСОИБ, в качестве базового варианта следует выбирать либо ручную систему контроля доступа, либо существующую автоматизированную систему контроля доступа, которую хотят заменить на новый вариант, либо ту систему контроля доступа, которая задана в ТЗ.

Кратко остановимся на капитальных затратах. Для оценки показателя $K_0$ в области информационной безопасности будем использовать подход, аналогичный тому, что описан в работах [15, с. 38].

Затраты $K_0$ на реализацию всей системы определяются следующим выражением:

$$K_0 = R_{01} + R_{02} + R_{03} + \{R_{04} - R_{05}\}, \quad (4)$$

$$R_{01} = \sum_{i=1}^{m} K_{0i},$$

где

$R_{01}$ – общие затраты: на все $m$ блоков системы;

$R_{02}$ – предпроизводственные затраты: на обследование объекта автоматизации, на разработку технического задания, на проектирование системы и т.п. [15];

$R_{03}$ – другие затраты: на реализацию операций, которые включены в состав системы, но не участвуют непосредственно в формировании КР;

$R_{04}$ – остаточная стоимость ликвидируемого (высвобождающегося) оборудования, устройств и т.п., которые при внедрении системы не нашли применения и реализация которых невозможна [15];

$R_{05}$ – остаточная стоимость неликвидируемого (высвобождающегося) оборудования, устройств и т.п., которые при внедрении системы нашли применение или реализация которых возможна [15];

$K_{0i}$ – затраты на реализацию $i$-го блока системы контроля доступа.

Отметим, что в целом такой подход с помощью затрат $R_{04}$ и $R_{05}$ позволяет учесть два факта. Первый – это то, что часть старого, неликвидируемого оборудования, может иногда использоваться в новом варианте системы, и тем самым уменьшаются на $R_{05}$ необходимые общие затраты $K_0$ на всю систему в целом. Второй — это то, что часть высвобождающегося оборудования пришлось ликвидировать, так как оно не нашло применения в новом варианте системы, реализацияе его по каким-то причинам невозможна, и тем самым увеличиваются на $R_{04}$ общие затраты $K_0$ на всю систему в целом. Отметим, что возможен случай, когда затраты $R_{04} = 0$ или $R_{05} = 0$ на реализацию системы заданы в ТЗ. Сформулируем необходимый критерий эффективности системы (т.е. правило) в сфере информационной безопасности:

Если $Э_0>0$, то предлагаемый вариант системы контроля доступа эффективнее по сравнению с базовым вариантом системы.

Если $Э_0<0$, то предлагаемый вариант системы контроля доступа является неэффективным по сравнению с базовым вариантом системы.

Если $Э_0=0$, то предлагаемый вариант системы контроля доступа – такой же по эффективности, как и базовый вариант системы.

Далее полагаем, что при изменении $N$ и $A_0$ затраты $K_0$ не меняются. Это возможно, если затраты $K_0$ выделяются и используются с учетом граничных (максимальных) значения для количества информационных элементов $N$ и годового объема производства $A_0$.

## 3. Программное средство для оценки эффективности системы

Для выполнения оценки эффективности системы контроля доступа можно применить программное средство [21], которое предназначено для выполнения оценки эффективности подобных систем при выполнении системного анализа. Это программное средство разработано на языке VBA для операционной системы Microsoft Windows (объем программы 143 Кб). На данное программное средство успешно получено свидетельство Федеральной службы по интеллектуальной собственности Российской Федерации. Область применения средства – исследование показателя эффективности, например,

информационной фактографической системы [14, 16] в составе системы контроля доступа для АСОИБ. Основные функции: вычисление показателя эффективности и проверка корректности введенных исходных данных для его вычисления в демонстрационном примере, выдача необходимых сообщений пользователю о работе программы, выдача сообщений о некорректных введенных данных для вычисления показателя эффективности информационной фактографической системы. Это средство позволяет выполнять расчет приведенных затрат по формуле (3). Покажем, как можно использовать это средство на упрощенном примере для демонстрации возможности оценки эффективности системы при следующих исходных данных:

$$C_1 = T_1 + t_1 N\,,\quad C_0 = T_0 + t_0 N\,, \tag{5}$$

где

$t_0 = 0.01$ у.е. – затраты *нового* варианта системы на обработку одной записи;

$t_1 = 1$ у.е. – затраты *базового* варианта системы на обработку одной записи;

$T_0 = 20$ у.е. – прочие затраты *нового* варианта системы;

$T_1 = 2$ у.е. – прочие затраты *базового* варианта системы;

$N$ — количество записей (информационных элементов), например, изображений лиц, допущенных к работе с носителями защищаемой информации, или сигнатур вредоносных программ в поисковых файлах системы информационной безопасности.

Согласно принципу № 14 реальные системы всегда нелинейные. Показатели эффективности этих систем могут быть выражены нелинейными функциями, например, позиномами, которые частично представлены в работе [13]. Однако в простейшем случае для демонстрационных целей можно использовать линейные функции, как например в формуле (5). Опираясь на принцип № 7 (табл. 1) полагаем, что изменение состояния системы связано с некоторой совокупностью условий (причинами), порождающих это изменение. Причины в данном случае порождают изменения состояния системы, которые отражаются в изменениях показателей $N$ и $A_0$. Исследуем, как зависит показатель $Э_0$ от $N$ и $A_0$. Результаты оценки приведенных затрат $Э_0$ в условных единицах при различных значениях показателей $N$ и $A_0$ представлены в табл. 3, 4, 5.

*Таблица 3. Оценка $Э_0$ в условных единицах при различных значениях $N$ и $A_0$ (при указанных парах значений $N$ и $A_0$ система неэффективна)*

| **N** | **$A_0$** | | | | |
|---|---|---|---|---|---|
| | **10** | **20** | **30** | **40** | **50** |
| **1000** | -740280 | -730560 | -720840 | -711120 | -701400 |
| **2000** | -730380 | -710760 | -691140 | -671520 | -651900 |
| **3000** | -720480 | -690960 | -661440 | -631920 | -602400 |
| **4000** | -710580 | -671160 | -631740 | -592320 | -552900 |
| **5000** | -700680 | -651360 | -602040 | -552720 | -503400 |
| **6000** | -690780 | -631560 | -572340 | -513120 | -453900 |
| **7000** | -680880 | -611760 | -542640 | -473520 | -404400 |
| **8000** | -670980 | -591960 | -512940 | -433920 | -354900 |
| **9000** | -661080 | -572160 | -483240 | -394320 | -305400 |
| **100000** | -651180 | -552360 | -453540 | -354720 | -255900 |

*Таблица 4. Оценка $Э_0$ в условных единицах при различных значениях $N$ и $A_0$ (при указанных парах значений $N$ и $A_0$ система может быть как эффективна, так и неэффективна)*

| $N$ | $A_0$ | | | | |
|---|---|---|---|---|---|
| | **100** | **200** | **300** | **400** | **500** |
| **1000** | -652800 | -555600 | -458400 | -361200 | -264000 |
| **2000** | -553800 | -357600 | -161400 | 34800 | 231000 |
| **3000** | -454800 | -159600 | 135600 | 430800 | 726000 |
| **4000** | -355800 | 38400 | 432600 | 826800 | 1221000 |
| **5000** | -256800 | 236400 | 729600 | 1222800 | 1716000 |
| **6000** | -157800 | 434400 | 1026600 | 1618800 | 2211000 |
| **7000** | -58800 | 632400 | 1323600 | 2014800 | 2706000 |
| **8000** | 40200 | 830400 | 1620600 | 2410800 | 3201000 |
| **9000** | 139200 | 1028400 | 1917600 | 2806800 | 3696000 |
| **100000** | 238200 | 1226400 | 2214600 | 3202800 | 4191000 |

*Таблица 5. Оценка $Э_0$ в условных единицах при различных значениях $N$ и $A_0$ (при указанных парах значений $N$ и $A_0$ система эффективна)*

| $N$ | $A_0$ | | | | |
|---|---|---|---|---|---|
| | **800** | **850** | **900** | **950** | **1000** |
| **1000** | 27600 | 76200 | 124800 | 173400 | 222000 |
| **2000** | 819600 | 917700 | 1015800 | 1113900 | 1212000 |
| **3000** | 1611600 | 1759200 | 1906800 | 2054400 | 2202000 |
| **4000** | 2403600 | 2600700 | 2797800 | 2994900 | 3192000 |
| **5000** | 3195600 | 3442200 | 3688800 | 3935400 | 418200 |
| **6000** | 3987600 | 4283700 | 4579800 | 4875900 | 5172000 |
| **7000** | 4779600 | 5125200 | 5470800 | 5816400 | 6162000 |
| **8000** | 5571600 | 5966700 | 6361800 | 6756900 | 7152000 |
| **9000** | 6363600 | 6808200 | 7252800 | 7697400 | 8142000 |
| **100000** | 7155600 | 7649700 | 8143800 | 8637900 | 9132000 |

Результаты табл. 3, 4, 5 дают общее представление об эффективности системы контроля доступа для информационной безопасности. Например, из табл. 4 видно, что существует область значений показателей $N$ и $A_0$, при которых значение $Э_0$ меньше нуля, и существует другая область значений показателей $N$ и $A_0$, при которых значение $Э_0$ больше нуля (данная область значений в табл. 4 выделена). Таким образом, так как при $N>8000$ показатель $Э_0>0$, то предлагаемый вариант системы эффективнее по сравнению с базовым вариантом системы.

Так как при $N \le 3000$ и $A_0 \le 200$ показатель $Э_0<0$, то предлагаемый вариант системы является неэффективным по сравнению с базовым вариантом системы.

Из табл. 4 следует, что пограничные пары значений ($N$, $A_0$), при которых значение $Э_0>0$, представлены следующим набором этих пар:

(8000, 100), (4000, 200),
(3000, 300), (2000, 400), (2000, 500).

В табл. 4 значения показателя $N$ изменяются с шагом 1000, а показателя $A_0$ – с шагом 100. На практике шаг изменения значений этих показателей может быть более мелкий, например 10. Это позволит более точно определить пограничные значения $N$ и $A_0$ при которых значение $Э_0$ больше нуля.

Из табл. 3, 4, 5 можно заметить, что чем с большей интенсивностью система контроля доступа работает (т.е. чем больше значение показателя $A_0$), тем больше значение показателя $Э_0$. Этот же результат нетрудно получить путем аналитического исследования средствами математического анализа выражения, представленного формулой (5).

Таким образом, достаточно оперативно выбрать вариант системы с помощью предварительной приближенной оценки затрат, далее этот вариант можно проанализировать уже более полно с помощью рекомендаций стандарта ISO/IEC TR 27016.

## Заключение

Рассмотрены важные принципы теории систем, системного анализа и системного подхода для применения их в области информационной безопасности. Для этой области специально выделен третий принцип теории систем, и системного анализа, посвященный максимальной эффективности работы системы и также еще отмечен 15-й принцип системного подхода, связанный с оптимальной эффективностью. Кратко рассмотрена эффективность системы контроля доступа, которая может быть оценена с помощью показателя приведенных затрат $Э_0$. В рамках представленного примера показана возможность оценки эффективности системы в области информационной безопасности. Для этого выполнено исследование показателя $Э_0$ при различных значениях показателей количества информационных элементов $N$ и годового объема производства $A_0$. Для рассматриваемого примера было показано, что существует область значений показателей $N$ и $A_{0,}$ при которых значение $Э_0$ меньше нуля, и существует другая область значений этих показателей, при которых значение $Э_0$ больше нуля. Было зафиксировано, что с ростом интенсивности работы контроля доступа растет показатель эффективности.

Для успешного применения средств системного анализа разработаны необходимые рекомендации для решения типовых задач, связанных с оценкой эффективности рассматриваемой системы. При организации выполнения системного анализа в области информационной безопасности необходимо больше уделять внимания основным элементам системного анализа, например, его третьему принципу и системному подходу, например его 15-му принципу.

СПИСОК ЛИТЕРАТУРЫ:

1. Miloslavskaya N., "Security Intelligence Centers for Big Data Processing," 2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Prague, Czech Republic. 2017. P. 7 – 13. doi:10.1109/FiCloudW.2017.68
2. Miloslavskaya N. Security Operations Centers for Information Security Incident Management. Proceedings of the 4th International Conference «Future Internet of Things and Cloud» (FiCloud 2016). Vienna (Austria), 22-24 August 2016. P. 131 – 138. DOI: 10.1109/FiCloud.2016.26
3. Melnikov D., Petrov V., Miloslavskaya N., Durakovskiy A., Kondratieva T. Cybertrust in E-Learning Environment based on Network Time Synchronization. Proceedings of the 8th International Conference on Computer Supported Education (CSEDU 2016), 21-23 April 2016. Rome (Italy). P. 402 – 407. DOI: 10.5220/0005874904020407
4. Durakovskiy A.P., Melnikov D.A., Gorbatov V.S., Ivanenko V.G., Modestov A.A. Russian model of public keys and validation infrastructure as base of the cloud trust . Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016, 2016 P. 123 – 130. DOI: 10.1109/FiCloud.2016.25
5. Кулик Сергей Д. Специальные средства для обеспечения информационной безопасности. Безопасность информационных технологий, [S.l.], v. 22, n. 2, june 2015. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/114>. Дата доступа: 22 jan. 2019
6. Кулик, Сергей Д. Обеспечение информационной безопасности и фактографические системы. Безопасность информационных технологий, [S.l.], v. 22, n. 1, mar. 2015. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/199>. Дата доступа: 22 jan. 2019.
7. Зегжда П.Д., Иванов Д.В., Москвин Д.А., Иванов А.А. Применение рядов смежности для распознавания предфрактальных графов при оценке кибербезопасности VANET-сетей // Проблемы информационной безопасности. Компьютерные системы, 2018. № 1. С. 10 – 26.
8. Зегжда Д.П., Павленко Е.Ю. Обеспечение киберустойчивости программно-конфигурируемых сетей на основе ситуационного управления // Проблемы информационной безопасности. Компьютерные системы, 2018. № 1. С. 160 – 168.
9. Волкова В.Н. Системный анализ информационных комплексов. СПб.: Лань, 2016. С. 336.
10. Воронов М.В. Введение с системный анализ. Тирасполь: Полиграфист, 2011. С. 224.
11. Артюхин Г.А. Теория систем и системный анализ. Практикум принятия решений. Казань: КГАСУ, 2016. С. 165.
12. Ермак В.Д. Системы. Системные принципы. Системный подход // Социон, (1997, № 2; 1998, №1) — URL: http://socionicasys.org/biblioteka/statji/sistemnij-podhod (дата обращения: 20.11.2018).

13. Кулик Сергей Д. Элементы системного анализа для студентов старших курсов университета //Естественные и технические науки, 2018. № 11. С. 373 – 377.
14. Кулик Сергей Д. Последовательный анализ и нейронные сети в фактографических информационных системах //Нейрокомпьютеры: разработка, применение, 2018. № 9. С. 53 – 60.
15. Соколов А.В. Информационно-поисковые системы. М.: Радио и связь, 1981. С. 152.
16. Кулик Сергей Д. Нейросетевые алгоритмы и автоматизированные фактографические информационные системы //Нейрокомпьютеры: разработка, применение, 2015. № 12. С. 58 – 65.
17. Безсонов Н.В. Методическое пособие для расчета экономического эффекта от использования изобретений и рационализаторских предложений (инструктивно-методические). М.: ВНИИПИ, 1985. 104 с.
18. Кулик Сергей Д. Исследование эффективности фактографического поиска в информационных системах /Изд. «Радиотехника».–Деп. в ВИНИТИ 29.07.2004, №1326-В2004; Библ. Указат. №9(391).–М.: ВИНИТИ, Радиотехника, 2004. 251 с.
19. ISO/IEC TR 27016 Information technology - Security techniques - Information security management - Organizational economics (ISO/IEC TR 27016:2014).
20. Мирсанова О.А. К вопросу об оценке эффективности затрат на информационную безопасность. URL:https://www.academia.edu/18137465/ (дата доступа 21.01.2018).
21. Кулик Сергей Д. Государственная регистрация программы для ЭВМ RU2018663832. «Лабораторный программный комплекс для изучения элементов системного анализа: лабораторная работа №5 — исследование показателя эффективности информационной фактографической системы (ЛПК-ЛР-5)». — Заявка №2018661642; Заяв. 19.10.2018; Зарегистр. 06.11.2018; Бюл. №11. — (РОСПАТЕНТ) Режим доступа: http://www1.fips.ru/wps/portal/ofic_pub_ru/#page=document&type=doc&tab=PrEVM&id=63C77536-43E2-4182-B31F-FC101A2F273D.

REFERENCES:

[1] Miloslavskaya N., "Security Intelligence Centers for Big Data Processing," 2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Prague, Czech Republic, 2017. P. 7 – 13. doi:10.1109/FiCloudW.2017.68
[2] Miloslavskaya N. Security Operations Centers for Information Security Incident Management. Proceedings of the 4th International Conference «Future Internet of Things and Cloud» (FiCloud 2016). Vienna (Austria), 22-24 August 2016. P. 131 – 138. DOI: 10.1109/FiCloud.2016.26
[3] Melnikov D., Petrov V., Miloslavskaya N., Durakovskiy A., Kondratieva T. Cybertrust in E-Learning Environment based on Network Time Synchronization. Proceedings of the 8th International Conference on Computer Supported Education (CSEDU 2016), 21-23 April 2016. Rome (Italy). P. 402 – 407. DOI: 10.5220/0005874904020407
[4] Durakovskiy A.P., Melnikov D.A., Gorbatov V.S., Ivanenko V.G., Modestov A.A. Russian model of public keys and validation infrastructure as base of the cloud trust . Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016, 2016 P. 123 – 130. DOI: 10.1109/FiCloud.2016.25.
[5] Kulik, Sergey D. Special Tools for Ensuring Information Security. IT Security (Russia), [S.l.], v. 22, n. 2, june 2015. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/114>. Date accessed: 22 jan. 2019. (in Russian).
[6] Kulik, Sergey D. Ensuring Information Security and Factographic Systems. IT Security (Russia), [S.l.], v. 22, n. 1, mar. 2015. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/199>. Date accessed: 22 jan. 2019. (in Russian).
[7] Zegzhda P.D., Ivanov D.V., Moskvin D.A., Ivanov A.A. Appliance of contiguity sequences for recognition of self-similar graphs for assessing VANET networks cybersecurity. Information Security Problems. Computer Systems, 2018. №1. P. 10 – 26. (in Russian).
[8] Zegzhda D.P., Pavlenko E.Y. Situational management for cyber-sustainability of software-defined networks. Information Security Problems. Computer Systems, 2018. № 1. P. 160 – 168. (in Russian).
[9] Volkova V.N. System analysis of information systems. SPb.: Lan', 2016. P. 336. (in Russian).
[10] Voronov M.V. Introduction with system analysis. Tiraspol: Polygraphist, 2011. P. 224. (in Russian).
[11] Artyukhin G.A. System theory and system analysis. Practical decision making. – Kazan': KGASU, 2016. P. 165. (in Russian).
[12] Ermak V.D. Systems System principles. System Approach. Sotsion, (1997, No. 2; 1998, No. 1). (in Russian). URL: http://socionicasys.org/biblioteka/statji/sistemnij-podhod (accessed: 20.11.2018).
[13] Kulik Sergey D. Elements of system analysis for students of senior courses of the university. Yestestvennyye i tekhnicheskiye nauki, 2018. № 11. P. 373 – 377 (in Russian).
[14] Kulik S.D. Sequential analysis and neural networks for factographic information systems. Neurocomputers, 2018. №9. P. 53 – 60. (in Russian).
[15] Sokolov A.V. Information retrieval systems. M.: Radio i svyaz', 1981. P. 152. (in Russian).
[16] Kulik Sergey D. Neural network algorithms and automated factographic information systems Neurocomputers, 2015. №12. P.58 – 65 (in Russian).

[17] Bezsonov N.V. Methodological manual for calculating the economic effect of the use of inventions and rationalization proposals (instructive and methodical). M.: VNIIPI, 1985. 104 p. (in Russian).
[18] Kulik Sergey D. Research of the effectiveness of factographic search in information systems / Ed. “Radiotekhnika”.- Dep. in VINITI July 29, 2004, № 1326-B2004; Bibl. Ukazat. №9 (391). – M.: VINITI, Radiotekhnika, 2004. 251 p. (in Russian).
[19] ISO/IEC TR 27016 Information technology - Security techniques - Information security management - Organizational economics (ISO/IEC TR 27016:2014).
[20] Mirsanova O.A. To the issue about efficiency assessment of expenses on information security [electronic resource]. URL: https://www.academia.edu/18137465/ (date accessed 21.01.2018) (in Russian).
[21] Kulik, Sergey D. Certificate for the program of the Russian Federation RU2018663832 «Laboratory research program for the study of the elements of system analysis: Part №5 - study of the effectiveness indicator of the information factographic system (LPK-LR-5)». Available at: <http://www1.fips.ru/wps/portal/ofic_pub_ru/#page=document&type=doc&tab=PrEVM&id=63C77536-43E2-4182-B31F-FC101A2F273D>. (in Russian).

*Поступила в редакцию – 16 декабря 2018 г. Окончательный вариант – 31 января 2019 г.*
*Received – December 16, 2018. The final version – January 31, 2019.*