

**ИМИТАЦИОННАЯ МОДЕЛЬ ПРОЦЕССА АНАЛИТИЧЕСКОЙ ОБРАБОТКИ  
СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМЫ  
ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ  
КОМПЬЮТЕРНЫХ АТАК ДЛЯ ОЦЕНКИ ОПЕРАТИВНОСТИ ЕЕ  
ФУНКЦИОНИРОВАНИЯ**

**И.Д. Королев, В.И. Попов, Е.С. Вызулин (Краснодар)**

**Введение**

Информационная безопасность подвержена постоянному изменению. С целью поддержания своей актуальности развиваются и адаптируются сами системы защиты. Количество источников информации, от которых поступают данные по текущему состоянию защищенности, растет с каждым днем. В то же время, с ростом инфраструктуры сложно уследить общую картину происходящего в ней и, если своевременно не реагировать на возникающие угрозы информационной безопасности (УИБ) и не предотвращать их, пользы не будет даже от сотни систем обнаружения компьютерных атак (КА).

Для своевременного реагирования возникающих УИБ и предотвращения инцидентов информационной безопасности (ИИБ) создана государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) на информационные ресурсы РФ.

В силу распространения новых УИБ и распределенных во времени КА становятся необходимым создание новых моделей обнаружения КА на ранней стадии, а также прогнозирования появления ИИБ, в том числе, распределенных во времени.

**Основная часть**

С целью оценки выигрыша времени реализации процессов функционирования информационно-аналитической подсистемы (ИАП) ведомственного сегмента (ВС) СОПКА проведен вычислительный эксперимент, который позволяет получить количественную оценку эффективности процессов функционирования ИАП ВС СОПКА, выраженных через оперативность, основанного на теории моделирования, теории эксперимента, математической статистики и теории экспертных оценок [3, 6, 9, 14, 15].

Оперативность и качество статистических работ моделей зависят от развития технологии сбора, передачи, обработки и хранения информации.

Для реализации оценки оперативности полученной модели в настоящей статье проводится описание процесса имитационного моделирования объекта и вычислительный эксперимент по эффективности разработанной модели.

Под вычислительным экспериментом в данной статье понимается метод изучения процессов функционирования ИАП ВС СОПКА, а именно: процессов анализа, обобщения информации и принятия решения, с помощью математического и имитационного моделирования. Он предполагает, что вслед за построением математической модели проводится ее численное исследование, позволяющее «проиграть» поведение исследуемого объекта в различных условиях или в различных модификациях [4].

Эффективность – это связь между достигнутым результатом и использованными ресурсами или свойство процесса давать результат при заданных ограничениях на используемые ресурсы. Критерий эффективности – совокупность условий (правил), определяющих пригодность или оптимальность процесса для установленных целей.

Показатель эффективности – численное выражение эффективности для данного процесса в соответствии с установленной целью.

На рисунке 1 представлена классификация параметров эффективности мониторинга, а также ее показателей и критериев [8].



Рис.1 – Детализация факторов, воздействующих на эффективность мониторинга ИИБ

Для проведения оценки оперативности процесса анализа учитывается время, затрачиваемое на корреляцию СИБ в ИАП ВС СОПКА; для проведения оценки оперативности процесса обобщения информации учитывается время, затрачиваемое на поиск СИБ в БД СИБ ВС СОПКА; для проведения оценки оперативности процесса принятия решения учитывается время, затрачиваемое на прогнозирование ИИБ в ИАП ВС СОПКА.

Цель эксперимента – получение статистических данных о времени, затрачиваемом на процессы: анализа, обобщения и принятия решения, при требуемой точности измерений и при минимально необходимом количестве опытов с сохранением статистической достоверности результатов эксперимента.

Исходя из системного анализа и его подходов к исследованию сложных систем, с целью получения количественных оценок, которые могут быть использованы для сравнения существующей и разработанной ИАП, применяется методика оценки оперативности процессов функционирования, состоящая из нескольких этапов:

1. сбор и подготовка исходных данных;
2. определение показателей и критериев оценки оперативности процессов функционирования существующей и разработанной ИАП;
3. построение математических моделей процессов функционирования существующей и разработанной ИАП;
4. планирование эксперимента;
5. разработка имитационных моделей процессов функционирования существующей и разработанной ИАП;
6. проведение вычислительного эксперимента;
7. анализ результатов проведенных расчетов и формулирование выводов по результатам эксперимента.

---

В данной статье рассмотрено имитационное моделирование процессов функционирования существующей и разработанной ИАП ВС СОПКА и оценка полученных на его основе выходных данных эффективности, выраженной через оперативность.

На первом этапе осуществляется сбор и подготовка исходных данных. Для получения реального времени по исходным данным, затрачиваемого на процессы: анализа СИБ, обобщения информации и принятия решения по ИИБ – проводится опрос экспертов, компетентных в данной области. В качестве экспертов выступают специалисты по ИБ, которые имеют непосредственное отношение к настройкам системы, анализу СИБ и выявления ИИБ на объекте СОПКА. Экспертам предлагается сформировать перечень возможных СИБ и распределить их по ИИБ, сформировать и упорядочить цепочки СИБ в порядке очередности их поступления, тем самым, создать правила корреляции.

На основе временных показателей, принятых от экспертов и вычисления степени согласованности их мнений, можно судить о том, что полученные данные являются достоверными. Выбор конкретных исходных данных основан на проведенном анализе времени, затрачиваемого на процессы функционирования ИАП ВС СОПКА, и обосновывается реальными объемами поступающих СИБ и выявленных ИИБ.

Свойства, которые характеризуют процесс функционирования (поведение) системы, можно назвать операционными свойствами или свойствами операции, поскольку искусственные системы создаются для выполнения конкретных операций.

В общем случае оценка операционных свойств проводится как оценка двух аспектов: исхода (результатов) операции и алгоритма, обеспечивающего получение результатов. Качество исхода результатов и алгоритм, обеспечивающий получение результатов, оцениваются по показателям качества операции, к которым относят результативность, ресурсоемкость и оперативность. В совокупности результативность, ресурсоемкость и оперативность порождают комплексное свойство – эффективность процесса – степень его приспособленности к достижению цели [1].

Исходя из ограничений и неизменной архитектуры оцениваемых систем, оценка процессов функционирования существующей и разработанной ИАП ВС СОПКА будет осуществляться через оперативность, которая определяется расходом времени, потребного для достижения цели операций. Оценка оперативности будет произведена в соответствии с заданными показателями и критериями. Архитектура ЭВМ для дальнейших расчетов принимается за константу.

В качестве показателя будет использоваться время работы процессов функционирования существующей и разработанной ИАП. В качестве критериев оперативности будет использоваться минимальный аргумент времени работы процессов функционирования существующей и разработанной ИАП ВС СОПКА.

Оперативность – это способность системы управления преобразовывать информацию в соответствии с темпом изменения ситуации. Критерии оценки оперативности задаются ограничениями на длительность цикла управления. Если ввести допущения, что все процессы, составляющие цикл управления, выполняются последовательно, а их длительности являются детерминированными величинами, то длительность цикла управления в системе находится как

$$t_{\text{раб}} = \sum t_p,$$

где  $t_p$  – время на выполнение одного результата исследования.

Под вычислительным экспериментом понимается метод изучения процессов функционирования существующей и разработанной ИАП ВС СОПКА, а именно

анализа, обобщения информации и принятия решения, с помощью математического и имитационного моделирования. Он предполагает, что вслед за построением математической модели проводится ее численное исследование, позволяющее «проиграть» поведение исследуемого объекта в различных условиях или в различных модификациях [4].

Обработка данных в ИАП ВС СОПКА выполняет задачи анализа СИБ, обобщения информации и принятия решения должностным лицом системы управления [2], с учетом времени, затрачиваемое на корреляцию СИБ, поиск информации в БД, выдачу уведомлений (прогнозирования) о наступающем ИИБ для принятия решения.

Для оценки оперативности процессов функционирования существующей и разработанной ИАП ВС СОПКА необходимо ввести следующие коэффициенты:

$K_{\text{опер.анализа}}$  – коэффициент оперативности процесса анализа СИБ;

$K_{\text{опер.об.инф.}}$  – коэффициент оперативности процесса обобщения информации о СИБ;

$K_{\text{опер.пр.реш.}}$  – коэффициент оперативности процесса принятия решения об ИИБ.

Каждому параметру присваивается свой вес, соответствующий важности параметра в зависимости от условий эксплуатации, состояний ИТКС, а также способа управления. В соответствии с вербально-числовой шкалой Харрингтона, влияющей на принятие решения, устанавливается уровень соответствия каждого параметра, влияющего на принятие соответствующего решения информационной системой, выраженный числовым значением и вводятся критерии оценки оперативности.

На основе проведенного анализа существующих технических решений, способных функционировать в составе подсистемы источников СИБ, разработана модель обработки СИБ существующей и разработанной ИАП ВС СОПКА, состоящая из процессов анализа, обобщения информации и принятия решения [7]. Для определения оперативности обработки данных в ИАП ВС СОПКА с использованием разработанных методик модель можно представить в следующем виде:

$$T_{\text{обработки СИБ}} = T_{\text{анализа}} + T_{\text{обобщения}} + T_{\text{принятия решения}}, \quad (1)$$

где  $T_{\text{анализа}} = T_C$  – время, затрачиваемое ИАП на анализ СИБ, которое зависит от критерия  $C$ , где  $C$  – это корреляция СИБ;

$T_{\text{обобщения}} = T_S$  – время, затрачиваемое ИАП на обобщение информации о СИБ, которое зависит от критерия  $S$ , где  $S$  – это поиск информации в БД;

$T_{\text{принятия решения}} = T_I$  – время, затрачиваемое ИАП на выдачу уведомлений о наступающем ИИБ для принятия решения должностным лицом, где показатель время зависит от критерия  $I$  – выявления ИИБ на ранних стадиях его наступления.

Дополнительно вводится допущение об ограниченности критериев оценки оперативности процессов функционирования существующей и разработанной моделей ИАП в рамках статьи. Задача оценки оперативности процессов функционирования существующей и разработанной моделей ИАП сводится к поиску минимального аргумента функций анализа, обобщения и принятия решения.

С учетом введенных допущений определяются параметры в виде:

$$T_{\text{анализа}} = \min_i T_{C_i}, \quad T_C = \{T_{C_i}\} \quad (2)$$

$$T_{\text{обобщения}} = \min_i T_{S_i}, \quad T_S = \{T_{S_i}\} \quad (3)$$

$$T_{\text{пр.решения}} = \min_i T_{I_i}, \quad T_I = \{T_{I_i}\} \quad (4)$$

Тем самым, минимизация процесса обработки СИБ в ИАП ВС СОПКА зависит от процессов корреляции СИБ, поиска СИБ в БД и выявления ИИБ (прогнозирования) – которые являются основными задачами предлагаемых методик и может быть записана в виде:

$$T_{\text{обработки\_СИБ\_сущ}} > T_{\text{обработки\_СИБ\_предл}} \rightarrow \min.$$

Далее вводится частный показатель коэффициента оперативности ИАП ВС СОПКА  $K_{\text{опер.}}$  в виде:

$$K_{\text{опер.}} = \frac{T_{\text{сущ.}} - T_{\text{предл.}}}{T_{\text{сущ.}}} \cdot 100\% \quad (5)$$

где  $T_{\text{предл.}}$  – время, затрачиваемое на частную обработку СИБ в каждом из процессов ИАП ВС СОПКА с применением разработанной методики;

$T_{\text{сущ.}}$  – время, затрачиваемое на частную обработку СИБ в каждом из процессов ИАП ВС СОПКА при использовании существующих методик.

Далее определяется количество опытов для каждого рассматриваемого случая, необходимых для получения достоверных результатов.

Исходные данные и выходные параметры определены в рамках 1-го, 2-го и 3-го этапов разработанной методики оценки. Причем так, как входные потоки транзактов в имитационных моделях процессов функционирования существующей и разработанной ИАП распределены по нормальному закону, считается, что и выходные потоки транзактов также распределены по нормальному закону [5].

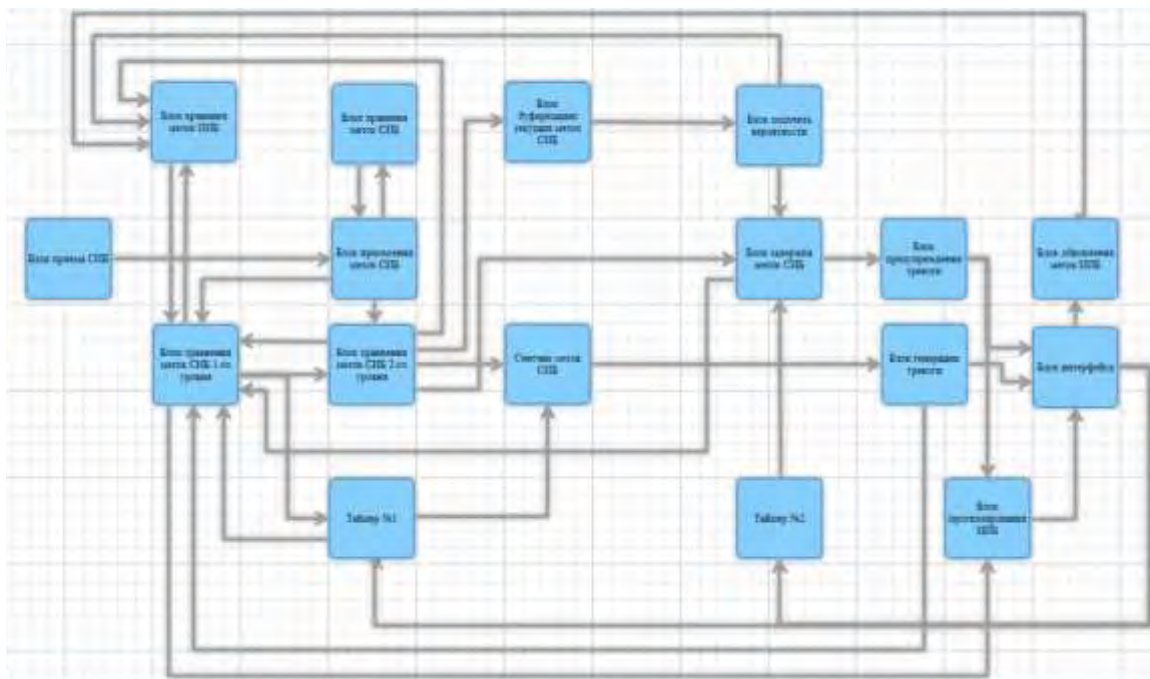


Рис.2 – Имитационная модель функционирования ИАП ВС СОПКА

С использованием разработанных на языке моделирования GPSS ИС «Модуль моделирования процессов функционирования объекта КИИ» [10], «Блок имитационного моделирования процессов функционирования объекта критической информационной инфраструктуры» [11], «Блок имитационного моделирования процессов обработки и хранения данных» [12], «Имитационная модель системы хранения и аналитической обработки данных в многомерной базе данных» [13], проводились серии из 30 вариантов вычислений в каждом из рассматриваемых случаев



(анализ СИБ, обобщение информации о СИБ и процесс принятия решения об ИИБ) при фиксированных и изменяемых значениях общих параметров разработанных методик с входящими в них алгоритмами.

Эксперимент осуществляется на основе имитационного модуля, построенного в рамках разработки имитационных моделей [10, 11, 12, 13] процессов функционирования существующей и разработанной ИАП ВС СОПКА.

Результаты эксперимента сведены в таблицах 1-3.

Таблица 1 – Результаты вычислений времени процесса обработки 1 ИИБ из  $N$  СИБ по существующим и разработанной методикам (сущ. и пред.)

	1 ИИБ из				
СИБ	50	100	200	500	1000
$T_{\text{анализа\_сущ, сек}}$	93,5	187	374	935	1870
$T_{\text{обобщения\_сущ, сек}}$	12,25	24,5	49	122,5	245
$T_{\text{прин.реш. сущ, сек}}$	22,7	45,4	90,8	227	454
$T_{\text{анализа\_пред, сек}}$	74,8	149,6	299,2	748	1496
$T_{\text{обобщения\_пред, сек}}$	11,1475	22,295	44,59	111,475	222,95
$T_{\text{прин.реш. пред, сек}}$	20,43	40,86	81,72	204,3	408,6

Таблица 2 – Результаты вычислений времени процесса обработки 2 ИИБ из  $N$  СИБ по существующим и разработанной методикам (сущ. и пред.)

	2 ИИБ из				
СИБ	50	100	200	500	1000
$T_{\text{анализа\_сущ, сек}}$	187	374	748	1870	3740
$T_{\text{обобщения\_сущ, сек}}$	24,5	49	98	245	490
$T_{\text{прин.реш. сущ, сек}}$	45,4	90,8	181,6	454	908
$T_{\text{анализа\_пред, сек}}$	149,6	299,2	598,4	1496	2992
$T_{\text{обобщения\_пред, сек}}$	22,295	44,59	89,18	222,95	445,9
$T_{\text{прин.реш. пред, сек}}$	40,86	81,72	163,44	408,6	817,2

Таблица 3 – Результаты вычислений времени процесса обработки 4 ИИБ из  $N$  СИБ по существующим и разработанной методикам (сущ. и пред.)

	4 ИИБ из				
СИБ	50	100	200	500	1000
$T_{\text{анализа\_сущ, сек}}$	374	748	1496	3740	7480
$T_{\text{обобщения\_сущ, сек}}$	49	98	196	490	980
$T_{\text{прин.реш. сущ, сек}}$	90,8	181,6	363,2	908	1816
$T_{\text{анализа\_пред, сек}}$	299,2	598,4	1196,8	2992	5984
$T_{\text{обобщения\_пред, сек}}$	44,59	89,18	178,36	445,9	891,8
$T_{\text{прин.реш. пред, сек}}$	81,72	163,44	326,88	817,2	163,44

Имея исходные данные для условия процесса обработки СИБ (анализа СИБ, обобщения информации о СИБ и процесса принятия решения об ИИБ по критериям корреляции СИБ, поиска СИБ в БД и выявления ИИБ (прогнозирования)

соответственно), производятся вычисления частных показателей коэффициентов оперативности (5) процесса обработки СИБ по разработанной методике:

$$K_{\text{опер.анализа}} = \frac{T_{\text{анализа.сущ.}} - T_{\text{анализа.предл.}}}{T_{\text{анализа.сущ.}}} \cdot 100\% = 20\%$$

$$K_{\text{опер.о о щения}} = \frac{T_{\text{о о щения.сущ.}} - T_{\text{о о щения.предл.}}}{T_{\text{о о щения.сущ.}}} \cdot 100\% = 9\%$$

$$K_{\text{опер.прин.решения}} = \frac{T_{\text{прин.решения.сущ.}} - T_{\text{прин.решения.предл.}}}{T_{\text{прин.решения.сущ.}}} \cdot 100\% = 10\%$$

Оценка оперативности полученных результатов характеризуется значением комплексного показателя оперативности процесса обработки СИБ, представляющего собой комбинацию частных показателей оперативности. Для вычисления значения комплексного показателя оперативности используется следующая формула:

$$K_{\text{компл.о р.СИБ}} = \frac{K_{\text{опер.анализа}} + K_{\text{опер.о о щения}} + K_{\text{опер.прин.решения}}}{N} = \frac{20\% + 9\% + 10\%}{3} = 13\%,$$

где  $N = \overline{1, N}$ .

Следовательно, комплексный показатель оперативности процесса обработки СИБ при использовании разработанных методик повышается на 13% в отличие от существующих.

Далее осуществляется анализ результатов проведенных расчетов и формулирование выводов по результатам эксперимента.

Из проведенного эксперимента следует, что с увеличением числа ИИБ в СИБ, согласно существующей и разработанной ИАП ВС СОПКА, коэффициент комплексного показателя оперативности процесса обработки СИБ разработанных методик на 13% лучше существующих методик.

Чем больше СИБ обрабатывает ИАП ВС СОПКА, тем нагляднее видна эффективность разработанных методик, выраженной через оперативность.

На рисунке 3 отображена диаграмма зависимости увеличения числа СИБ от времени обработки по существующим и разработанным методикам при обработке 1 ИИБ из  $N$  СИБ, необходимых для проведения эксперимента согласно исходных данных.



Рис. 3 – Диаграмма зависимости увеличения числа СИБ от времени обработки

---

На рисунке 3 видно, что на процессы корреляции СИБ, доступа к БД, а также выявления ИИБ по существующим методикам тратится намного больше времени по сравнению с разработанными методиками.

При увеличении числа СИБ и выявленных в них ИИБ объем обработанных СИБ, а также время на их обработку растет, однако коэффициент комплексного показателя оперативности процесса обработки СИБ разработанных от существующих методик повышается на 13%, что свидетельствует о высокой эффективности разработанных методик, выраженной через оперативность.

### **Вывод**

Оперативность процесса обработки СИБ при использовании разработанных методик составляет 13% в отличие от существующих. Также видно, что при увеличении объемов СИБ совместно с увеличением числа ИИБ в СИБ, согласно существующей и разработанной ИАП ВС СОПКА, коэффициент комплексного показателя оперативности процесса обработки СИБ разработанных от существующих методик остается стабильным и повышается на 13%. Чем больше СИБ обрабатывает ИАП ВС СОПКА, тем нагляднее видна эффективность разработанных методик, выраженной через оперативность.

Полученные результаты показывают, что при реализации процесса обработки СИБ в ИАП ВС СОПКА по существующим методикам тратится намного больше времени, чем при использовании разработанных методик.

### **Литература**

1. **Анфилатов В.С.** Системный анализ в управлении: учебное пособие / В.С. Анфилатов, А.А. Емельянов, А.А. Кукушкин; Под редакцией А.А. Емельянова – М.: Финансы и статистика, 2002 г. – 368 с.: ил. ISBN 5-279-02435-X. Глава 2.3.3. Показатели и критерии эффективности функционирования систем.
2. **Боговик А.В.** Теория управления в системах военного назначения / А.В. Боговик, В.В. Игнатов. – СПб.: ВАС, 2008. – 460 с.
3. **Брукинг А.** / Экспертные системы. Принципы работы и примеры: Пер. с англ./А. Брукинг, П. Джонс, Ф. Кокс и др.; Под ред. Р. Форсайта. – М.: Радио и связь, 1987. – 224с: ил. (Кибернетика).
4. **Горбунов-Посадов М.М.** Расширяемые программы: Учеб. пособие для студентов ун-тов, специализирующихся в обл. программирования / М. М. Горбунов-Посадов. – М.: Полиптих, 1999. – 336 с.: ил.; 22 см.; ISBN 5-901118-01-4.
5. **Каширин И.Ю.** Интерактивная аналитическая обработка данных в современных OLAP системах. И.Ю. Каширин, С.Ю. Семченков // Бизнес-информатика. № 2 (08), 2009 г. Анализ данных и интеллектуальные системы. Издательство: Национальный исследовательский университет «Высшая школа экономики» (Москва) ISSN: 1998-0663eISSN: 2587-8166.
6. **Кельберт М.Я.** Вероятность и статистика в примерах и задачах / М.Я. Кельберт, Ю.М. Сухов. – Москва: Изд-во МЦНМО, 2007. – 22 см. // т. 2: Марковские цепи как отправная точка теории случайных процессов и их приложения / [пер. с англ. Л. Сахно под ред. Ю. Мишуры]. 2010. – 559 с.: ил.; ISBN 978-5-94057-557-3.
7. Патент 193101 Российская Федерация, МПК G06F 21/55 (2013.01). Система аналитической обработки событий информационной безопасности / Королев И.Д., Попов В.И., Коноваленко С.А., Стадник А.Н., Захарченко Р.И. Заявитель, патентообладатель: Краснодарское высшее военное училище им. С.М. Штеменко. № 2019114527. Заявлен 13.05.2019 г., опублик. 14.10.2019 г. Бюл. № 29; 11 с.



- 
8. **Попов С.В.** Факторы, влияющие на эффективность мониторинга инцидентов информационной безопасности в автоматизированной банковской системе // С.В. Попов, В.Н. Шамкин // Научно-технический вестник Поволжья № 1, 2010 год, с. 145-148. ISSN: 2079-5920 – [Электронный ресурс]. – Режим доступа: <https://www.elibrary.ru/item.asp?id=16352220> (дата обращения 20.05.19 г).
  9. **Сагитова В.В.** Применение метода экспертных оценок для автоматизации аудита информационных систем персональных данных. – Текст: непосредственный // Вестник УГАТУ / В.В. Сагитова, В.И. Васильев. 2017. Т. 21, № 3 (73). С. 105–112. ISSN 2225-2789 (Online) – [Электронный ресурс]. – Режим доступа: <http://journal.ugatu.ac.ru/> (дата обращения: 15.06.2020).
  10. Свидетельство о государственной регистрации программы для ЭВМ № 2019617828 Российская Федерация. «Модуль моделирования процессов функционирования объекта КИИ» / И.Д. Королев, В.И. Попов, Р.И. Захарченко, Д.В. Леонов, С.А. Коноваленко, А.В. Андреев; заявитель и правообладатель И.Д. Королев, Р.И. Захарченко, Заявка № 2019616597; заявл. 11.06.2019; опубл. 20.06.2019, Реестр программ для ЭВМ. – 1 с.
  11. Свидетельство о государственной регистрации программы для ЭВМ № 2019618066 Российская Федерация. «Блок имитационного моделирования процессов функционирования объекта критической информационной инфраструктуры» / И.Д. Королев, В.И. Попов, Р.И. Захарченко, Д.В. Леонов, В.Д. Шмулевский, М.С. Санджиев; заявитель и правообладатель И.Д. Королев, Р.И. Захарченко, Заявка № 2019616621 заявл. 11.06.2019; опубл. 26.06.2019, Реестр программ для ЭВМ. – 1 с.
  12. Свидетельство о государственной регистрации программы для ЭВМ № 2020610190 Российская Федерация. «Блок имитационного моделирования процессов обработки и хранения данных» / И.Д. Королев, В.И. Попов, Р.И. Захарченко, Е.В. Алпеев, Е.С. Литвинов, Д.В. Леонов, Е.С. Зорькин; заявитель и правообладатель И.Д. Королев, Р.И. Захарченко, Заявка № 2019667312 заявл. 23.12.2019; опубл. 10.01.2020, Реестр программ для ЭВМ. – 1 с.
  13. Свидетельство о государственной регистрации программы для ЭВМ № 2020610191 Российская Федерация. «Имитационная модель системы хранения и аналитической обработки данных в многомерной базе данных» / И.Д. Королев, В.И. Попов, Р.И. Захарченко, Е.В. Алпеев, Е.С. Литвинов, Д.В. Леонов; заявитель и правообладатель И.Д. Королев, Р.И. Захарченко, Заявка № 2019667214 заявл. 23.12.2019; опубл. 10.01.2020, Реестр программ для ЭВМ. – 1 с.
  14. **Созинова Е.Н.** Применение экспертных систем для анализа и оценки информационной безопасности / Е. Н. Созинова. – Текст: непосредственный // Молодой ученый. – 2011. – № 10 (33). – Т. 1. – С. 64-66. – [Электронный ресурс]. – Режим доступа: <https://moluch.ru/archive/33/3766/> (дата обращения: 15.06.2020).
  15. **Трегуб И.В.** Технический анализ финансовых рынков [Текст]: учебник / И.В. Трегуб; Федеральное гос. образовательное бюджетное учреждение высш. проф. образования «Финансовый ун-т при Правительстве Российской Федерации» (Финансовый университет), Кафедра математического моделирования экономических процессов. – Москва: Финансовый ун-т, 2013. – 222 с.: ил. табл.; 20 см.; ISBN 978-5-7942-0993-8.