С. Д. Кулик, К. И. Ткаченко, А. А. Кондаков, С. И. Ткаченко

ЭФФЕКТИВНОЕ ФОРМИРОВАНИЕ ФАКТОГРАФИЧЕСКИХ ДАННЫХ ДЛЯ АВТОМАТИЗИРОВАННЫХ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специалистами среди информационных систем принято выделять класс автоматизированных систем, которые получили название «автоматизированные фактографические информационно-поисковые системы» (АФИПС) [1–8]. Автоматизированные информационные системы формирования фактографических данных (АИСФФД) рассматривают также как разновидность фактографических систем: в них имеется человек-оператор (например, специалист в области *информационной безопасности* (ИБ)) и реализован алгоритм генерирования фактографических данных [5, 6]. Для повышения эффективности работы автоматизированных средств обеспечения информационной безопасности (АСОИБ) предлагается использовать в их составе именно фактографическую подсистему. Одна из главных задач, решаемых этой подсистемой, — эффективное формирование фактографических данных и реализация фактографического поиска по запросу пользователя [3, 4]. Данная статья — прямое продолжение работы [6], целью которой является дальнейшее исследование эффективности работы АИСФФД в составе АСОИБ. Предлагаемые АСОИБ имеют несколько режимов работы [6].

Первый режим работы напрямую связан с защитой информации (данных) в документе. Пользователь составляет документ и скрепляет его своей подписью (возникают сам бумажный документ и его электронная копия (ЭлД), эта копия содержит и подпись пользователя (признаки почерка), бумажный документ и его копия получают один и тот же регистрационный номер в АСОИБ). Документ защищен подписью и признаками почерка.

Второй режим работы связан с проверкой подлинности бумажного документа, имеющего необходимый регистрационный номер. При поступлении такого документа по регистрационному номеру извлекается его электронная копия ЭлД и выполняется анализ этих документов (проводится сравнение признаков почерка бумажного документа и ЭлД) и принимается решение о подлинности поступившего документа.

Третий режим работы связан с оценкой эффективности работы эксперта (например, специалиста в области ИБ), который получает тестовое задание и формирует свой ответ на него в виде ЭлД, поступающего в АСОИБ (объектами этого задания являются биометрические признаки). По результату выполненного задания либо принимается решение о прекращении испытания и происходит последующая выдача окончательного ответа на выход АСОИБ, либо с помощью АИСФФД формируется следующее новое задание. По результатам тестирования эксперта принимается решение о подготовленности эксперта работать в составе АСОИБ. С опорой на последовательный анализ разработан вариант динамического тестирования испытуемого [6]. Экспериментальная проверка и исследование алгоритма динамического тестирования испытуемого показали, что алгоритм работоспособен и может быть применен для АСОИБ [6]. Одной из областей применения полученных результатов и предлагаемой АСОИБ может быть криминалистика [5, 6, 7, 8, 9].

Четвертый режим работы связан с фактографическим поиском в АСОИБ [3, 4]. Для реализации этого режима выполнен предварительный анализ достигнутых результатов в этой области. Как показали исследования, технологии информационного поиска давно достигли высокого уровня и позволяют работать с большими объемами данных. Тем не менее имеющиеся механизмы можно развивать и совершенствовать дальше, увеличивая эффективность такого важного инструмента, как обработка и поиск информации. Это особенно актуально в современных условиях, когда объемы

информационных данных постоянно растут, а вместе с этим увеличивается и ценность полезной и актуальной информации. Современные технологии позволяют обеспечить высокую вычислительную мощность при работе с большими объемами данных за счет мощной аппаратной составляющей, но можно увеличивать производительность поисковых систем и на программном уровне, используя эффективные алгоритмы поиска. В связи с этим главная задача данного режима связана с созданием эффективной фактографической поисковой системы с применением технологии интеллектуального составления запроса и глубокого анализа обрабатываемых данных. В перспективе данная система может дополнить собой функционал любой информационной системы, увеличив ее производительность и эффективность, что особенно актуально для обеспечения информационной безопасности.

Остановимся кратко на третьем режиме работы АСОИБ. Для этого рассмотрим АИСФФД и ее эффективность в составе АСОИБ.

Для функционирования современного общества разрабатываются и используются различные информационные системы (ИС). Как правило, любая ИС предоставляет какие-то выходные данные (содержащие информацию) потребителю в ответ на его запрос (содержащий входные данные). Далее в рассматриваемых ИС будем выделять 4 группы данных (рис. 1):

1. $V_{вх}$ — входные данные;
2. $V_{вых}$ — выходные данные;
3. $V_{внБД}$ — внутренние данные, которые постоянно хранятся в системе, например, в виде *базы данных* (БД);
4. $V_{внОП}$ — внутренние временные данные, которые постоянно не хранятся в системе, например, в *оперативной памяти* (ОП) или в хранилище на *внешнем запоминающем устройстве* и т. п.

Те ИС, что на выходе формируют *фактографические данные* (ФД) и при этом эти данные не являются теми, что постоянно хранятся в системе, а формируются только в процессе работы ИС, будем называть *ИС формирования фактографических данных* (ИСФФД).

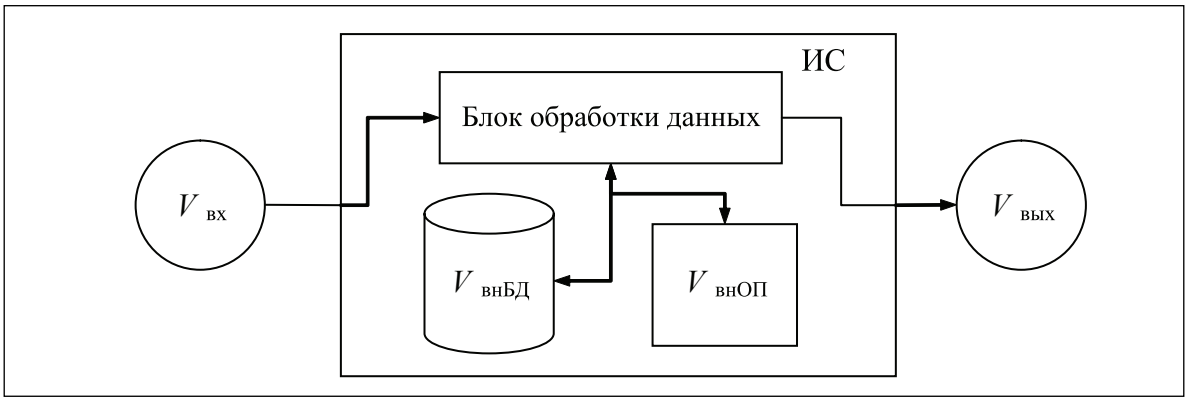

Рис. 1. Укрупненная и обобщенная схема ИС

Системы, в которых формирование фактографических данных выполняется обязательно при участии человека-оператора (далее — просто оператор), будем называть *автоматизированными информационными системами формирования фактографических данных*, или сокращенно — АИСФФД. Эти АИСФФД являются разновидностью фактографических систем: в них имеется человек-оператор и реализован алгоритм генерирования фактографических данных.

Реализация решения прикладных задач, связанных с формированием ФД, осуществляется на практике посредством специализированных информационных систем. В рамках данной работы будут рассматриваться только те информационные системы, в которых (по запросу пользователя) происходит формирование фактографических данных (в этом-то и состоит основная специфика таких систем).

Причем под запросом пользователя понимается сформированное определенным образом требование к информационной системе о получении определенных *объектов*, необходимых пользователю. В некоторых случаях в роли *объектов* могут выступать и сами ФД. Укрупненная, краткая схема АИСФФД для АСОИБ представлена на рис. 2. В состав АИСФФД входят пользователь, администратор, то есть человек-оператор (или группа операторов), *информационная подсистема*, реализованная с помощью средств вычислительной техники. АИСФФД содержит блок генерирования фактографических данных (то есть ГФД), в котором реализован алгоритм генерирования ФД.

АИСФФД в составе АСОИБ работает следующим образом. На вход поступает от пользователя запрос на формирование объектов по ФД. Администратор выполняет необходимые настройки и следит за работой системы, а также выполняет роль эксперта. Блок, в котором реализован, например, программно ГФД по поступившему запросу выполняет генерирование требуемых ФД, которые при необходимости помещаются в ФБД.

Результат работы ГФД используется затем блоком формирования объектов для формирования объектов, которые в итоге передаются на выход системы для пользователя АСОИБ.

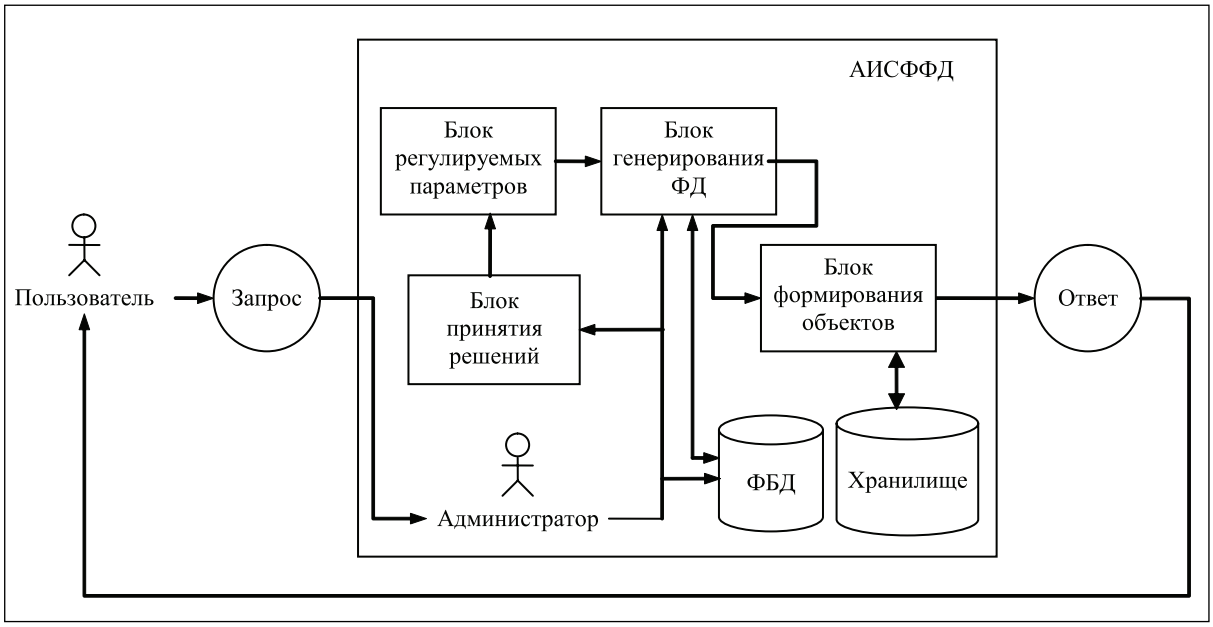

Рис. 2. Укрупненная, краткая схема АИСФФД для АСОИБ

На практике одна из возможных реализаций блока ГФД выполнена с помощью специализированных программных средств PNDeveloper, PNRunner и БД Oracle Database 11g Express Edition Release 11.2.0.2.0, имеющих в своем составе необходимый интерпретатор команд, реализующий интерпретацию программ, написанных на языке PNL (Programs Network Language — Язык сетевых программ). Данный программный комплекс позволяет эффективно с точки зрения временных затрат разработчика и затрат на обслуживание и содержание полученной АСОИБ реализовать поставленную задачу. Эффективность достигается, в частности, за счет встроенных в язык PNL конструкций для понятного и безопасного манипулирования данными базы данных, а также архитектурных особенностей программного комплекса. К преимуществам архитектуры можно отнести простоту развертывания программного комплекса, например, клиентская часть состоит из одного исполняемого файла и нескольких временных файлов, которые создаются уже в ходе работы этого исполняемого файла и не требуют дополнительных действий с точки зрения администрирования. Таким образом, для подключения еще одной рабочей станции достаточно скопировать и запустить один исполняемый файл, для запуска которого не требуются какие-либо сторонние библиотеки, в том числе клиента Oracle Database, кроме стандартных библиотек

операционной системы семейства Windows x32/x64. При необходимости программный комплекс можно настроить таким образом, чтобы все данные между распределенными по сети компонентами системы передавались в защищенном виде. Для защиты передаваемой информации используются, в частности, следующие алгоритмы и протоколы. Для аутентификации сервера используется протокол аутентификации сторон на основе алгоритмов электронно-цифровой подписи RSA или DSA. Для создания общего секрета (сеансового ключа) используется алгоритм Диффи — Хеллмана (DH). Для шифрования передаваемых данных используется симметричное шифрование, алгоритмы AES, Blowfish или 3DES. Целостность передачи данных проверяется с помощью HMAC-SHA1/HMAC-MD5. Для сжатия шифруемых данных может использоваться алгоритм LempelZiv (LZ77), который обеспечивает такой же уровень сжатия, что и архиватор ZIP.

Тестирование специалиста в области информационной безопасности выполняется с помощью специально сгенерированных задач. Специалист решает эти задачи (принимает решение по ним). По результатам тестирования принимается решение о подготовленности специалиста для АСОИБ. Под базовой задачей в данной работе понимается задача, послужившая прототипом для генерирования (формирования) необходимого набора аналогичных вариантов задач (или заданий). Выбор конкретной базовой задачи зависит от практической области применения АСОИБ. Рассмотрим АИСФФФД и АСОИБ без указания этой конкретной области, то есть в самом общем случае. Опираясь на работы [11, 12], введем следующие показатели эффективности:

K — количество сформированных заданий;

$t_Г$ — усредненные временные затраты вычислительных средств на формирование (генерирование) одного варианта базовой задачи и решения к ней для АСОИБ;

$t_Т$ — усредненные временные затраты человека-оператора на составление *условий* (текста) одного задания;

$\hat{T}_А$ — оценка общих временных затрат АИСФФФД для формирования K заданий;

$\hat{T}_Р$ — оценка общих временных затрат человека-оператора (эксперта) для формирования K заданий вручную для АСОИБ;

$\hat{S}_А$ — оценка приведенных общих денежных затрат АИСФФФД на формирование K заданий для АСОИБ (эксплуатационные затраты);

$\hat{S}_Р$ — оценка приведенных общих денежных затрат (эксплуатационные затраты) на формирование человеком-оператором (экспертом либо экспертом и администратором) K заданий вручную для АСОИБ.

В общем случае полагаем, что:

$\hat{T}_A = f_A(K, t_Г, ...)$; $\hat{T}_P = f_P(K, t_T, ...)$; $\hat{S}_A = F_A(K, t_Г, ...)$; $\hat{S}_P = F_P(K, t_T, ...)$.

Учитывая специфику АИСФФФД для АСОИБ, введем необходимый критерий эффективности.

Предлагается следующий критерий эффективности АИСФФФД для АСОИБ:

при выполнении условия

$$\begin{cases} \hat{T}_A < \hat{T}_P \\ \hat{S}_A < \hat{S}_P \end{cases}, \text{ или } \begin{cases} \hat{T}_A \le \hat{T}_P \\ \hat{S}_A < \hat{S}_P \end{cases}, \text{ или } \begin{cases} \hat{T}_A < \hat{T}_P \\ \hat{S}_A \le \hat{S}_P \end{cases}$$

полагают, что АИСФФФД для АСОИБ при формировании K заданий, каждое из которых формируется по одному и тому же алгоритму, является **более эффективной** по сравнению с вариантом формирования этих же K заданий вручную (то есть ручным вариантом ИСФФФД).

Будем полагать, что формирование заданий человеком-оператором вручную является более эффективным, чем формирование этих же заданий с помощью АИСФФФД для АСОИБ при выполнении следующего условия:

$$\begin{cases}\hat{T}_A > \hat{T}_P \\ \hat{S}_A > \hat{S}_P\end{cases}, \text{ или } \begin{cases}\hat{T}_A \geq \hat{T}_P \\ \hat{S}_A > \hat{S}_P\end{cases}, \text{ или } \begin{cases}\hat{T}_A > \hat{T}_P \\ \hat{S}_A \geq \hat{S}_P\end{cases},$$

а при выполнении условия:

$$\begin{cases}\hat{T}_A = \hat{T}_P \\ \hat{S}_A = \hat{S}_P\end{cases}$$

АИСФФД и ручной вариант ИСФФД являются эквивалентными. Далее будем предполагать, что при выполнении условия:

$$\begin{cases}\hat{T}_A < \hat{T}_P \\ \hat{S}_A \geq \hat{S}_P\end{cases} \text{ или } \begin{cases}\hat{T}_A > \hat{T}_P \\ \hat{S}_A \leq \hat{S}_P\end{cases} \text{ или } \begin{cases}\hat{T}_A \geq \hat{T}_P \\ \hat{S}_A < \hat{S}_P\end{cases} \text{ или } \begin{cases}\hat{T}_A \leq \hat{T}_P \\ \hat{S}_A > \hat{S}_P\end{cases}$$

появляется **зона неопределенности**, то есть принять решение об эффективности одного из возможных вариантов только по этим двум показателям *не представляется возможным*.

Далее рассматриваем 2 ручных варианта и один автоматизированный вариант ИСФФД для АСОИБ. Ручные варианты отличаются только тем, что в первом случае все ручные операции выполняются одним очень квалифицированным и высокооплачиваемым специалистом — экспертом. Во втором случае все ручные операции выполняются двумя группами специалистов: 1-я группа — это очень квалифицированные и высокооплачиваемые специалисты (эксперты), а 2-я группа — это менее квалифицированные и низкооплачиваемые специалисты (помощники эксперта).

Для сравнительного анализа на языке Python [10] выполнено математическое моделирование эффективности различных вариантов ИСФФД для АСОИБ по основным показателям $\hat{S}_A$, $\hat{T}_A$ и $\hat{S}_\rho$, $\hat{T}_\rho$. Некоторые важные результаты этого моделирования при t_T = 10 мин. и t_T = 0,05 мин. представлены в таблицах 1 и 2.

Таблица 1. Оценка эффективности ИСФФД для АСОИБ (затраты времени в мин. на K заданий)

Показатель		**Эффективность варианта**						
K		**1**	**5**	**8**	**…**	**100**	**…**	**1000**
Ручной вариант ИСФФД для АСОИБ								
$\hat{T}_P$	$\hat{T}_{P1}$	62,6	111,1	147,5	…	12626	…	121717
	$\hat{T}_{P2}$	71,1	149,5	208,2	…	20103	…	196392
Автоматизированный вариант ИСФФД для АСОИБ								
$\hat{T}_A$		1369	137,1	137,3	…	142,1	…	189,5
$G_{P,A} = \min\{\hat{T}_{P1}, \hat{T}_{P2}\} / \hat{T}_A$		0,5	0,8	1,1	…	8,9	…	64,2

Из таблицы 1 видно, что на модельных данных при K = 1000 показатель $G_{P,A}$ = 64,2, то есть автоматизированный вариант ИСФФД для АСОИБ более чем в 50 раз быстрее, чем аналогичный ручной вариант системы.

Таблица 2. Оценка эффективности ИСФФД для АСОИБ (денежные затраты в руб. на K заданий)

Показатель		**Эффективность варианта**						
K		**1**	**47**	**58**	**…**	**500**	**…**	**1000**
Ручной вариант ИСФФД для АСОИБ								
$\hat{S}_P$	$\hat{S}_{P1}$	25763	54812	61759	…	340889	…	656646
	$\hat{S}_{P2}$	25699	49339	54993	…	282144	…	539103
Автоматизированный вариант ИСФФД для АСОИБ								
$\hat{S}_A$		54498	54500	54501	…	5452,1	…	5454,4
$\Delta_{P,A} = \min\{\hat{S}_{P1}, \hat{S}_{P2}\} - \hat{S}_A$		$\Delta_{P,A}<\mathbf{0}$	$\Delta_{P,A}<\mathbf{0}$	$\Delta_{P,A}>0$	…	$\Delta_{P,A}>0$	…	$\Delta_{P,A}>0$
$\widetilde{G}_{P,A} = \min\{\hat{S}_{P1}, \hat{S}_{P2}\} / \hat{S}_A$		$\approx 0,47$	$\approx 0,9$	≈ 1	…	$\approx 5,2$	…	$\approx 9,88$

Анализ данных таблицы 2 убедительно показывает, что на модельных данных с ростом K увеличивается $\widetilde{G}_{P,A}$ эффективность АИСФФД для АСОИБ по денежным затратам и при $K = 10^3$ показатель $\widetilde{G}_{P,A}$ может достигать почти 10, то есть АИСФФД примерно в **10** раз эффективнее ручного варианта аналогичной системы (или, иными словами, на АИСФФД требуется в 10 раз меньше денежных затрат). При выполнении некоторых ограничений достигнутой эффективности АИСФФД может быть достаточно для реализации АСОИБ.

Эти полученные на модельных данных результаты показывают, что на практике можно выполнить аналогичные исследования уже для конкретных исходных данных заданного практического применения АИСФФД для АСОИБ по двум основным показателям, таким как эксплуатационные и временные затраты.

Выводы

Таким образом, очень кратко представлена идея построения АИСФФД для АСОИБ. Кратко представлена концепция построения АСОИБ. Предложен вариант возможной схемы для реализации АИСФФД. С опорой на последовательный анализ, для АСОИБ предложен вариант динамического тестирования испытуемого (человека-оператора) АИСФФД [6]. Намечены пути реализации фактографического поиска в АСОИБ. На данном этапе получены результаты, которые способствуют эффективному решению задачи обеспечения информационной безопасности. В процессе выполненной работы и проведенных исследований были успешно получены необходимые охранные документы РОСПАТЕНТа [7, 8, 9].

СПИСОК ЛИТЕРАТУРЫ:

1. *Кулик С. Д.* Учет человека-оператора, работающего вне контура АФИПС // Безопасность информационных технологий. 2002. № 4. С. 79–86.
2. *Кулик С. Д.* Учет человека-оператора в контуре АФИПС // Безопасность информационных технологий. 2003. № 2. С. 30–39.
3. *Кулик С. Д.* Разработка и исследование модели АФИПС // Безопасность информационных технологий. 2004. № 2. С. 65–73.
4. *Кулик С. Д.* Исследование поискового робота для фактографического поиска // Научно-техническая информация. 2003. Сер. 2. № 3. С. 21–27.
5. *Кулик С. Д., Ткаченко К. И.* Разработка генераторов для обеспечения информационной безопасности // Безопасность информационных технологий. 2010. № 1. С. 87–89.

6. *Кулик С. Д., Ткаченко К. И., Никонец Д. А.* Средства обеспечения информационной безопасности и экспериментальное исследование эффективности почерковедческих методик // Безопасность информационных технологий. 2013. № 2. С. 57–69.
7. *Кулик С. Д.* Патент на полезную модель № 23701, Российская Федерация (RU), кл. МПК[7] G07 D7/00. Устройство для объединения уголовных дел, определения фальшивых банкнот, ценных бумаг и документов при раскрытии преступлений в криминалистике. Заявка № 2001134790/20; Заяв. 26.12.2001; Зарегистр. 27.06.2002; Приоритет от 26.12.2001; Опубл. Бюл. № 18. Ч. 2. – 399 с. (РОСПАТЕНТ).
8. *Кулик С. Д.* Патент на изобретение № 2208837, Российская Федерация (RU), кл. МПК[7] G06 F17/30. Устройство для имитационного моделирования значений функции выхода АФИПС криминалистического назначения. Заявка № 2001129139/09; Заяв. 30.10.2001; Зарегистр. 20.07.2003; Приоритет от 30.10.2001; Опубл. 20.07.2003; Бюл. № 20. Ч. 3. С. 752–753. (РОСПАТЕНТ).
9. *Кулик С. Д., Кондаков А. А., Зырянова О. В.* Свидетельство на программу Российской Федерации № 2012615520 “Special simple solver of puzzles v.1.0” (S-S-S-Puz). Заявка № 2012613177; Заяв. 24.04.2012; Зарегистр. 19.06.2012. (РОСПАТЕНТ).
10. *Лутц М.* Программирование на Python. Том I. 4-е изд. Пер. с англ. СПб.: Символ-Плюс, 2011. – 992 с.
11. *Черноруцкий И. Г.* Методы принятия решений. СПб.: БХВ-Петербург, 2005. – 416 с.
12. *Вентцель Е. С.* Исследование операций: задачи, принципы, методология. М.: Высшая школа, 2001. – 208 с.

REFERENCES:

1. *Kulik S. D.* Uchet cheloveka-operatora, rabotayushchego vne kontura AFIPS // Bezopasnost’ informatsionnykh tekhnologiy. 2002. № 4. P. 79–86.
2. *Kulik S. D.* Uchet cheloveka-operatora v konture AFIPS // Bezopasnost’ informatsionnykh tekhnologiy. 2003. № 2. P. 30–39.
3. *Kulik S. D.* Razrabotka i issledovaniye modeli AFIPS // Bezopasnost’ informatsionnykh tekhnologiy. 2004. № 2. P. 65–73.
4. *Kulik S. D.* Issledovaniye poiskovogo robota dlya faktograficheskogo poiska // Nauchno-tekhnicheskaya informatsiya. 2003. Series. 2. № 3. P. 21–27.
5. *Kulik S. D., Tkachenko K. I.* Razrabotka generatorov dlya obespecheniya informatsionnoy bezopasnosti // Bezopasnost’ informatsionnykh tekhnologiy. 2010. № 1. P. 87–89.
6. *Kulik S. D., Tkachenko K. I., Nikonets D. A.* Sredstva obespecheniya informatsionnoy bezopasnosti i eksperimental’noye issledovaniye effektivnosti pocherkovedcheskikh metodik // Bezopasnost’ informatsionnykh tekhnologiy. 2013. № 2. P. 57–69.
7. *Kulik S. D.* Patent for utility model №23701, Russian Federation (RU), G07 D7/00. Ustroystvo dlya obyedineniya ugolovnykh del, opredeleniya fal’shivykh banknot, tsennykh bumag i dokumentov pri raskrytii prestupleniy v kriminalistike. Zayavka № 2001134790/20; Zayavleno 26.12.2001; Zaregistrirovano 27.06.2002; Priority 26.12.2001; Bull. № 18. Part 2. P. 399. (ROSPATENT).
8. *Kulik S. D.* Patent for invention № 2208837, Russian Federation (RU), G06 F17/30. Ustroystvo dlya imitatsionnogo modelirovaniya znacheniy funktsii vykhoda AFIPS kriminalisticheskogo naznacheniya. Zayavka № 2001129139/09; Zayavleno 30.10.2001; Zaregistrirovano 20.07.2003; Priority 30.10.2001; Published 20.07.2003; Bull. № 20. Part 3. P. 752–753. (ROSPATENT).
9. *Kulik S. D., Kondakov A. A., Zyrianova O. V.* Certificate program at the Russian Federation № 2012615520 “Special simple solver of puzzles v.1.0” (S-S-S-Puz). Zayavka № 2012613177; Zayavleno 24.04.2012; Zaregistrirovano 19.06.2012. (ROSPATENT).
10. *Lutz M.* Programmirovaniye na Python. Tom I. 4-e izd. SPb.: Simvol-Plyus, 2011. – 992 p.
11. *Chernorutskiy I. G.* Metody prinyatiya resheniy. SPb.: BKHV-Peterburg, 2005. – 416 p.
12. *Wentzel E. S.* Issledovaniye operatsiy: zadachi, printsipy, metodologiya. M.: Vysshaya shkola, 2001. – 208 p.