
УДК [351.741:004.89](477)

Д. Ю. УЗЛОВ,

*кандидат технических наук,
начальник управления информационно-аналитического обеспечения
ГУМВД Украины в Харьковской области;*

В. М. СТРУКОВ,

*кандидат технических наук, доцент,
заведующий кафедрой информационных технологий и защиты информации
факультета права и массовых коммуникаций
Харьковского национального университета внутренних дел;*

А. Б. ГРИГОРОВИЧ,

*начальник отдела управления информационно-аналитического обеспечения
ГУМВД Украины в Харьковской области;*

А. И. ПЕТРУСЕНКО,

*старший инженер-программист управления информационно-аналитического обеспечения
ГУМВД Украины в Харьковской области;*

С. Н. ДОСКАЛЕНКО,

*инженер-программист управления информационно-аналитического обеспечения
ГУМВД Украины в Харьковской области*

ПРИМЕНЕНИЕ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ КРИМИНАЛЬНОГО АНАЛИЗА В РЕАЛЬНОМ ВРЕМЕНИ (RICAS) ДЛЯ АНАЛИТИЧЕСКОГО СОПРОВОЖДЕНИЯ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ И ДОСУДЕБНОГО РАССЛЕДОВАНИЯ

Исследована проблема повышения эффективности информационно-аналитической работы в органах внутренних дел путём создания интеллектуального технологического инструментария нового поколения. Проанализировано современное состояние информационно-аналитического обеспечения органов внутренних дел Украины и сформулированы его характерные особенности. Выполнен обзор зарубежных автоматизированных средств информационно-аналитической работы, выделены их достоинства и недостатки. В качестве решения сформулированных проблем предложено использовать геоинформационную интеллектуальную систему криминального анализа в реальном времени – Real-time Intelligence crime analytics system (RICAS). Описаны её назначение, функциональные возможности, методики выполнения криминального анализа средствами системы, преимущества по сравнению с существующими аналогами и новизна.

Ключевые слова: информационно-аналитическое обеспечение, органы внутренних дел, геоинформационная интеллектуальная система реального времени, криминальный анализ, функциональные возможности, новизна, преимущества.

Uzlov, D.Y., Strukov, V.M., Grigorovich, A.B., Petrusenko, A.I. and Doskalenko, S.N. (2015), "Use of Real-time Intellectual criminal analytics system (RICAS) for analytical support of operative and search activities and pre-trial investigation" ["Primenenie intellektual'noj sistemy kriminal'nogo analiza v real'nom vremeni (RICAS) dlja analiticheskogo soprovozhdenija operativno-rozysknoj dejatel'nosti i dosudebnogo rassledovaniya"], *Pravo i Bezpeka*, No. 2, pp. 132–139.

Постановка проблемы. Современное состояние информационно-аналитического обеспечения органов внутренних дел имеет следующие характерные особенности:

1) в базах данных ОВД накоплено огромное количество данных о криминально значимых лицах и событиях, измеряемое сотнями миллионов записей, и их количество ежедневно возрастает;

2) обработка этих данных выполняется, как правило, с помощью несложных операций без привлечения наукоемких методов и технологий, что не позволяет осуществлять аналитический анализ по выявлению скрытых или неявных связей между лицами и событиями в имеющихся огромных массивах данных;

3) анализ запросов, которые поступают в подразделения информационно-аналитического обеспечения деятельности органов внутренних дел, показывает, что большая часть из них является запросами на поиск преступлений по аналогии и лиц, совершивших аналогичные преступления. Существующая автоматизированная система обработки таких запросов (интегрированная информационно-поисковая система – ИИПС) позволяет получать списки, размеры которых иногда составляют сотни преступлений и тысячи лиц. Дальнейшая обработка осуществляется вручную путём классификации или кластеризации по каким-либо критериям (предопределённым или заранее неизвестным). Этот процесс является достаточно сложным и трудоёмким, зависит от квалификации исполнителя, не автоматизирован, требует специальных навыков работы с ИИПС и поэтому обладает такими принципиальными недостатками:

1) объективно низкой эффективностью ручной обработки большого текстового массива;

2) невысокой вероятностью выявления в полученном большом текстовом массиве возможных внутренних взаимосвязей между событиями и лицами;

3) невозможностью выявления связей между элементами полученного списка (лицами и событиями) и аналогичными данными, которые не попали в этот список или в явном или

неявном виде хранятся в других массивах данных системы.

Перечисленные недостатки со временем усугубляются тем, что ежедневно объёмы хранящейся информации растут, пополняясь вновь поступающими данными.

Криминальный анализ в своём обыденном понимании является систематическим изучением уровня преступности, концентрации мест совершённых преступлений по видам и иным параметрам. Необходимо различать два вида криминального анализа – аналитический поиск и аналитическое исследование. В то же время эти два вида криминального анализа в зависимости от поставленной задачи всегда будут дополнять друг друга. На данный момент авторам не известны системы криминального анализа, позволяющие в едином пространстве отображения соединить эти два вида анализа. Большинство из них имеют большое количество инструментов для визуального криминального анализа, но инструментов для аналитического поиска у них нет.

Целью этой статьи является исследовать проблему повышения эффективности информационно-аналитической работы в органах внутренних дел путём создания интеллектуального технологического инструментария нового поколения. Для этого, исходя из анализа современного состояния информационно-аналитического обеспечения ОВД Украины, выполним обзор зарубежных автоматизированных средств информационно-аналитической работы и предложим решение сформулированных проблем.

Изложение основного материала. Анализ существующих в этой сфере решений показал, что на данный момент за рубежом существуют автоматизированные системы, которые позволяют частично решать описываемые задачи.

Система *I2* разработана корпорацией *IBM* для решения задач правоохранительных органов. Эта система позволяет отображать данные, имеющиеся в хранилище, создаваемом под оболочкой *I2* в формате хранения продуктов *IBM*, на собственных картах и выполнять анализ связей данных.

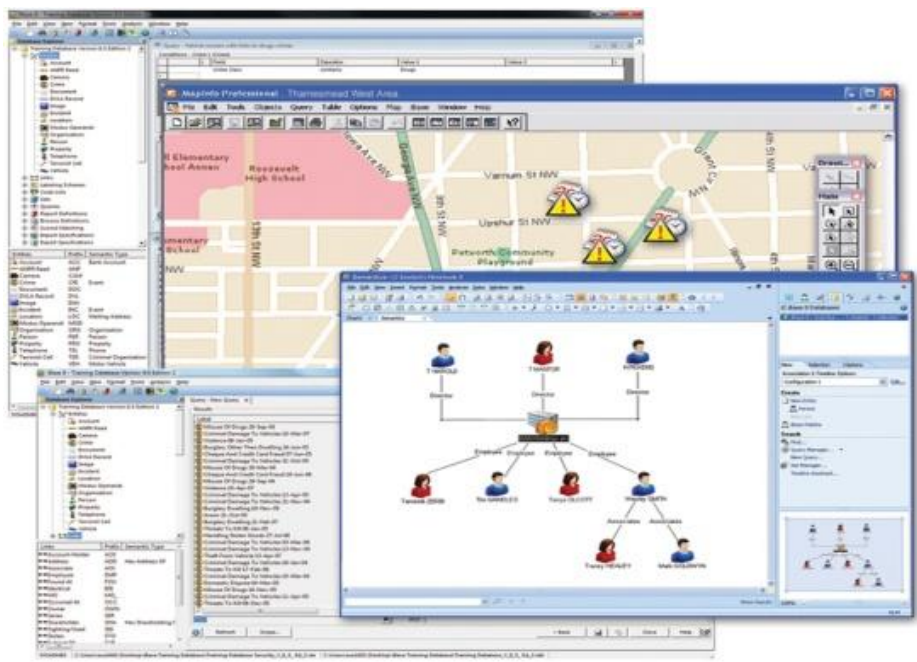


Рис. 1

Система имеет высокие требования к аппаратной части, сложность в разворачивании и обучении, большую стоимость и, самое главное, необходимость перехода на хранение данных в формат продукта, т. е. необходимость отказа от существующей ИИПС ОВД Украины. Вместе с тем система не обеспечивает возможность связать географическое пространство, время и событие в одном визуальном

пространстве отображения.

Система **CRIMEVIEW Server** используется в полицейском департаменте города Глендейл (Калифорния), основана на картографической платформе **ESRI**. Основной принцип – анализ зон с максимальным уровнем уличной преступности. Основное назначение – изменение маршрутов патрулирования в выявленные зоны.

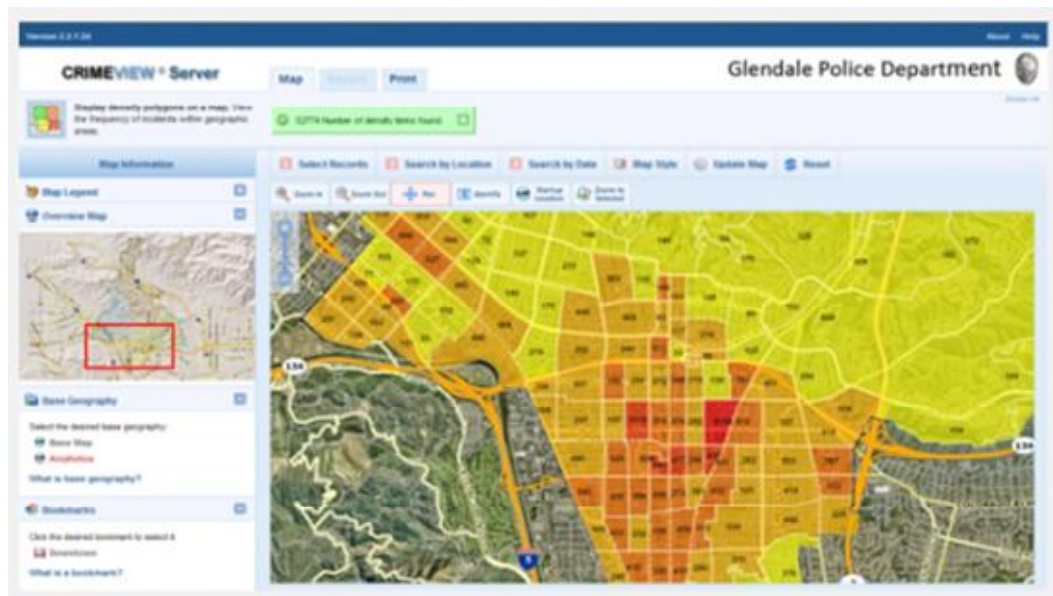


Рис. 2

Система **My Neighborhood Map System** используется в городе Сिएтл (Вашингтон). Основное назначение – визуализация поступающих сообщений о преступлениях и отчётов

полицейских. Состоит из модулей:
 – **911 INCIDENT RESPONSES MAP**,
 – **POLICE REPORTS MAP**,
 – **MONTHLY CRIME STATISTICS MAP**.

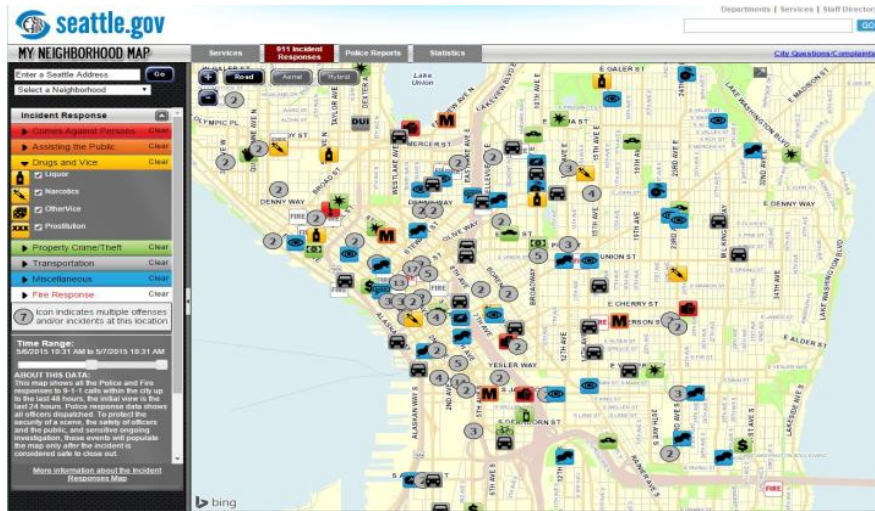


Рис. 3

Система **CRIMEDC** используется в полицейском департаменте города Вашингтон. Основное

назначение – предоставление общественности данных о совершённых преступлениях.

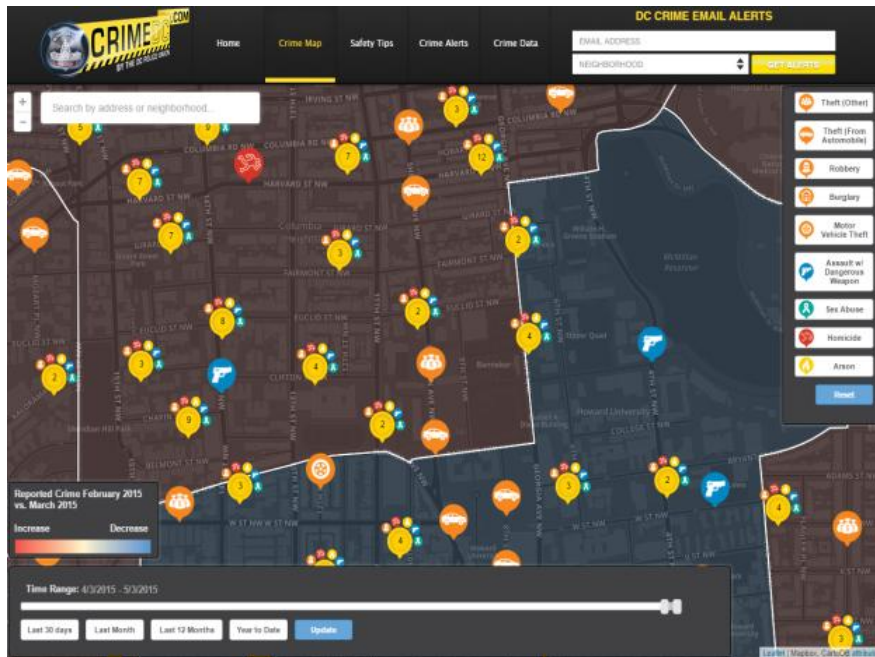


Рис. 4

Большинство рассмотренных систем предлагают решения для **информирования общественности** и, что принципиально важно, предполагают не интеграцию в уже действующие системы, а установку их как независимых систем.

Использование методов и алгоритмов кластеризации и классификации технологии *Text Mining* для выделения криминально значимой информации совместно с технологией *Visual Mining* в режиме реального времени обеспечивает возможность выполнения аналитической работы по профилактике и расследованию преступлений в автоматизированном

режиме на качественно новом уровне [1]. Эта возможность реализована в интеллектуальной системе криминального анализа в реальном времени – **Real-time Intelligence crime analytics system (RICAS)**, которая позволяет связать географическое пространство, время, лица и события в одном визуальном пространстве отображения.

В основу построения системы положены такие факторы:

– любая криминально значимая информация содержит данные о месте совершения преступного деяния, которые могут быть отражены либо в текстовом формате в виде адреса

либо в географических координатах и времени совершения;

- любой субъект или объект преступления имеет привязку к географическим координатам в текстовом формате (адрес прописки, проживания, регистрация предприятия, места работы, регистрация транспортного средства, оружия и т. д.);

- криминальные события, субъекты и объекты могут иметь взаимосвязи, которые легче обнаружить путём анализа визуального отображения в едином пространстве представления (на одной карте). Например, если в месте совершения разбойного нападения проживают лица, ранее привлекавшиеся за аналогичные преступления, то существует большая вероятность совершения ими данного деяния;

- отображение в едином пространстве событий, растянутых во времени (происходящих в разное время), позволяет обнаружить скрытые закономерности визуально.

С учётом этих факторов в представляемой системе программно реализованы адаптированные алгоритмы технологий *Data Mining*, *Text Mining* и *Visual Mining*, *Link Analyzes*, которые обеспечивают выполнение следующих операций с потоками входных данных:

- кластеризация объектов по одному или нескольким признакам, имеющим общие пространственно-временные характеристики;

- создание временной ленты событий для определённого географического места (ретроспективный анализ криминальных событий, произошедших в заданный период времени в районе места исследуемого происшествия);

- группировка объектов и субъектов вокруг события;

- анализ связей лиц, объектов, событий.

Система *RICAS* позволяет выполнять операции анализа, обработки и представления данных на качественно новой технологической основе, выполнена как надстройка (оболочка) существующей ИИПС ОВД Украины и, что принципиально важно, позволяет при её внедрении не удалять старую систему или приостанавливать её функционирование, а просто и безболезненно существенно улучшать её функциональность и эффективность.

Назначение системы:

- повышение эффективности использования информационных учётов в оперативно-розыскной деятельности сотрудников ОВД, досудебном расследовании, деятельности по охране общественного порядка;

- уменьшение времени реакции на поступающую информацию о преступлениях и пра-

вонарушениях и, как следствие, более эффективное их раскрытие по горячим следам;

- профилактика и предупреждение преступлений;

- повышение качества и своевременности управленческих решений руководителей всех уровней ответственности.

На современном этапе развития информационно-аналитических технологий появилось чёткое осознание того, что инструменты криминального анализа, поиска, построения связей, анализа поведенческого профиля и прочих аналитических методик должны быть единой целостной системой, предоставляющей аналитику полный спектр инструментов, необходимых для построения причинно-следственных связей.

Real-time Intelligence crime analytics system (RICAS) – это первая интеллектуальная система криминального анализа данных, которая объединила в едином пространстве отображения основные и наиболее передовые методы и методики криминального анализа и аналитического поиска в реальном времени, что позволяет значительно повысить эффективность и результативность раскрытия преступлений по горячим следам и не раскрытых ранее преступлений.

Аналитическая работа в системе выполняется в автоматизированном режиме: на первом этапе по поступившему в систему запросу с помощью разработанных алгоритмов аналитического поиска автоматически осуществляется поиск, результаты которого отображаются в текстовой форме и на географической карте; на втором этапе оператором в ручном режиме осуществляется визуальный анализ полученных данных и принимается окончательное решение либо системе задаются дополнительные уточняющие запросы.

Система позволяет оператору выполнять многие виды криминального анализа:

- анализ криминальной обстановки (*crime pattern analysis*);

- анализ общего профиля (*generalprofile analysis*);

- анализ конкретного расследования (*case analysis*);

- сравнительный анализ (*comparativ analysis*);

- анализ групповой преступности (*offender group analysis*);

- анализ особенностей профиля (*specific profile analysis*);

- анализ расследований (*investigation analysis*).

Используя все эти виды анализа интегрально, появляется возможность видеть картину целиком – предикативно и постфактум, т. е. систему событий, лиц, объектов, связанных причинно-следственными связями в пространстве и времени.

Поскольку система является надстройкой над существующими базами данных, она может отображать как явно указанные связи между лицами, так и строить визуальные связи между лицами, которые, на первый взгляд, между собой не связаны. Система использует несколько алгоритмов поиска связей. Первый алгоритм – рекурсивный поиск взаимосвязей фигурантов, участвовавших в разных событиях. Второй – визуальный поиск связей. В процессе вывода специальным образом структурированной информации в визуальную среду отображения становятся очевидными связи типа «место совершения – подельник – преступник», «преступление – подозреваемый – подельники».

Инструментарий системы базируется на тематических моделях и методах интеллектуального семантического анализа, визуального темпорального анализа, анализа поведенческого профиля, анализа скрытых закономерностей.

Интеллектуальный семантический анализ включает в себя мощное ядро по работе с семантикой. Анализ неструктурированных данных происходит в режиме реального времени. Для унификации поисковых функций и построения поведенческого профиля используется алгоритм классификации или «тегирования», а также антиципационный алгоритм (схема предвосхищения) – цель поиска известна заранее [2].

Семантическое ядро системы позволяет строить сложные поисковые запросы, включающие в себя всевозможные динамические и статические компоненты – ограничение по времени, методу совершения преступления, дислокации и т. д. [3]. Все функции выполняются мгновенно и позволяют максимально быстро визуализировать информацию и выполнять аналитическую работу.

Визуальный темпоральный анализ. Отображение хронологии произошедших событий и временное разграничение позволяют оперативно выявлять скрытые пространственно-временные закономерности между различными событиями.

Анализ поведенческого профиля. Наиболее постоянным и точным с точки зрения психологии преступника является его поведенческий профиль. Он отображает многие параметры деятельности преступника – привычный способ совершения преступления, ме-

ста совершения и прочие мелкие зависимости, которые в совокупности соответствуют одному профилю.

Наличие тех или иных поведенческих признаков с определённой долей вероятности могут свидетельствовать о том, что данный субъект может быть причастен к событию [4]. Из этого принципа формируется так называемый групповой поведенческий анализ. Безусловно, поведенческий профиль преступника никак не может существовать без влияния на других субъектов. Поэтому в криминальной практике часто заметны совпадения по тем или иным поведенческим параметрам у разных субъектов, когда-либо участвовавших в единичных событиях. Анализ группового поведенческого профиля позволяет определять подельников, сообщников без явных связей между собой.

Анализ скрытых закономерностей. Между лицами, каким-либо образом причастными к правонарушению, объективно существуют связи (родственные, по роду профессиональной деятельности, географические – по привязке к месту жительства, месту отбывания наказания и т. п.). Подобные связи существуют также между лицами и событиями, а также между различными событиями. Такие связи могут быть явными, опосредованными и скрытыми [5]. Кроме того, группа преступлений, совершённых одним и тем же лицом, обязательно имеет определённые характерные общие черты, которые явно не зафиксированы. Выявление таких скрытых закономерностей с высокой долей вероятности всегда может идентифицировать связь между преступником и всеми совершёнными им преступлениями [6]. Безусловно, некоторые события могут «выбиваться» из общего потока из-за своей спонтанности или внешних факторов. Однако, исходя из предыдущего принципа, такие проявления можно нивелировать.

В *RICAS* поиск скрытых закономерностей осуществляется, базирясь на интеллектуальном ядре обработки семантики. Семантический анализ является основополагающим, поскольку связи выражаются не всегда явно и их следует искать в контексте.

Выводы. Система *RICAS* разрабатывалась с использованием современных, оптимизированных технологий в веб-пространстве и поддерживает мультиплатформность. Её можно использовать на любых стационарных и мобильных устройствах при наличии защищённого канала связи; интерфейс системы не перегружает пользователя. Исходя из изложенного, предлагаем использовать указанную систему для решения сформулированных в статье проблем.

Список использованных источников

1. Ландэ Д. В. Интернетика : Навигация в сложных сетях: модели и алгоритмы / Д. В. Ландэ, А. А. Снарский, И. В. Безсуднов. – М. : Либроком (Editorial URSS), 2009. – 264 с.
2. Узлов Д. Ю. Використання методів і моделей інтелектуальної обробки неструктурованої криміналістичної інформації / Д. Ю. Узлов // Інтелектуальні системи та прикладна лінгвістика : матеріали III Всеукр. наук.-практ. конф. – Харків : НТУ «ХП», 2014. – С. 13–15.
3. Хайрова Н. Ф. Использование метода компараторной идентификации для динамического наполнения тезауруса оперативно-розыскной деятельности / Н. Ф. Хайрова, Д. Ю. Узлов, С. В. Петрасова // Східно-Європейський журнал передових технологій. – 2014. – № 3/2 (69). – С. 4–8.
4. Узлов Д. Ю. Використання поведінкового профілю для виявлення ознак кіберзлочинності / Дмитро Юрійович Узлов // Використання інноваційних технологій у попередженні злочинів : матеріали наук.-практ. семінару (м. Харків, 6 груд. 2012 р.) / МВС України, Харків. нац. ун-т внутр. справ. – Харків : ХНУВС, 2012. – С. 161–164.
5. Manning C. D. Introduction to Information Retrieval / C. D. Manning, P. Raghavan, H. Schütze. – Cambridge : Cambridge University Press, 2008. – 544 p.
6. Westphal C. Data Mining for Intelligence, Fraud and Criminal Detection. Advanced Analytic & Information Sharing Technologies / C. Westphal. – New York : CRC Press Taylor & Francis Group, 2009. – 440 p.

Надійшла до редколегії 25.08.2015

УЗЛОВ Д. Ю., СТРУКОВ В. М., ГРИГОРОВИЧ О. Б., ПЕТРУСЕНКО А. І., ДОСКАЛЕНКО С. М. ЗАСТОСУВАННЯ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ КРИМІНАЛЬНОГО АНАЛІЗУ В РЕАЛЬНОМУ ЧАСІ (RICAS) ДЛЯ АНАЛІТИЧНОГО СУПРОВОДУ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ І ДОСУДОВОГО РОЗСЛІДУВАННЯ

Досліджено проблему підвищення ефективності інформаційно-аналітичної роботи в органах внутрішніх справ шляхом створення інтелектуального технологічного інструментарію нового покоління. Проаналізовано сучасний стан інформаційно-аналітичного забезпечення органів внутрішніх справ України та сформульовано його характерні особливості. Виконано огляд зарубіжних автоматизованих засобів інформаційно-аналітичної роботи, виділено їхні переваги і недоліки. Як вирішення сформульованих проблем запропоновано використовувати геоінформаційну інтелектуальну систему кримінального аналізу в реальному часі – Real-time Intelligence crime analytics system (RICAS). Описано її призначення, функціональні можливості, методики виконання кримінального аналізу засобами системи, переваги в порівнянні з існуючими аналогами і новизну.

Ключові слова: інформаційно-аналітичне забезпечення, органи внутрішніх справ, геоінформаційна інтелектуальна система реального часу, кримінальний аналіз, функціональні можливості, новизна, переваги.

UZLOV D. Y., STRUKOV V. M., GRIGOROVICH A. B., PETRUSENKO A. I., DOSKALENKO S. N. USE OF REAL-TIME INTELLECTUAL CRIMINAL ANALYTICS SYSTEM (RICAS) FOR ANALYTICAL SUPPORT OF OPERATIVE AND SEARCH ACTIVITIES AND PRE-TRIAL INVESTIGATION

The problem of improving the effectiveness of informational and analytical work within internal affairs agencies through the creation of intelligent technological tools of the new generation is studied in the article. The authors have analyzed the current state of informational and analytical support of Internal Affairs Agencies of Ukraine and have formulated its characteristic features. The overview of foreign automated means of information and analytical work is performed; their advantages and disadvantages are outlined. As a solution of the formulated problems the authors have offered to use geographic and information Real-time Intelligence crime analytics system (RICAS). Its purpose, functionality, methodical techniques of criminal analysis by the means of the system, advantages compared with existing analogues and novelty are described. The system has used methods and algorithms for clustering and classification of Text Mining technology to isolate criminally relevant information together with the technology of Visual Mining in real time, ensuring the ability to perform analytical work on the prevention and investigation of crimes in the automated mode on a qualitatively new level.

The RICAS allows us to perform the analysis, processing and presentation of data on a new technological basis; it is designed as an add (shell) of the existing integrated information and search system of Internal Affairs Agencies of Ukraine; and that is essential, it allows while its implementation do not delete the old system or suspend its operation, but simply and painless significantly improve its functionality and efficiency. The RICAS – is the first intelligence system of criminal analysis of data, which brings together in one space the main and the most advanced methods and techniques

of criminal analysis and analytical search in real time that can significantly increase the efficiency and effectiveness of solving crimes without delay and previously unsolved crimes.

Keywords: *informational and analytical support, internal affairs agencies, geographic and information intelligent real-time system, criminal analysis, analytical search, functional abilities, novelty, advantages.*
