МВС України

Харківський національний університет внутрішніх справ

Кафедра інформаційних технологій та захисту інформації

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Матеріали
Науково-практичного семінару

м. Харків, 27 травня 2015 року

Харків
2015

Застосування інформаційних технологій у правоохоронній діяльності: матеріали наук.-практ. семінару, м. Харків, 27 травня 2015 р. / МВС України, Харк. нац. ун-т внутр. справ. – Х.: ХНУВС, 2015. - 88 с.

У збірнику висвітлено погляди науковців та практиків щодо актуальних питань розробки і впровадження компонентів інформаційних технологій в діяльності правоохоронних органів, інформаційної безпеки в діяльності ОВС, проблем підготовки кадрів для інформаційно-аналітичних підрозділів ОВС.

УДК [351.74:004] (477)(08)
ББК 67.9(4УКР)301.163я43
Н34

ОРГКОМІТЕТ:

голова – проректор Головко Олександр Миколайович;

заступник голови – завідувач кафедри інформаційних технологій та захисту інформації факультету права та масових комунікацій Струков Володимир Михайлович;

секретар – доцент кафедри інформаційних технологій та захисту інформації факультету права та масових комунікацій Євстрат Дмитро Іванович;

члени оргкомітету:

- професор кафедри інформаційних технологій та захисту інформації факультету права та масових комунікацій Яковлев Сергій Всеволодович;
- начальник відділу зв'язків з громадськістю полковник міліції Щербакова Ірина Василівна;
- начальник відділу організації наукової роботи підполковник міліції Мірошниченко Оксана Станіславівна;
- начальник інформаційно-технічного відділу підполковник міліції Полховський Олександр Миколайович;
- начальник відділу організації служби підполковник міліції Тарасенко Віталій Миколайович;
- начальник відділу матеріального забезпечення Копаниця Олексій Вікторович;
- директор загальної бібліотеки Процких Тамара Олексіївна.

Друкується за рішенням оргкомітету відповідно до доручення Харківського національного університету внутрішніх справ від 15 квітня 2015 року № 38

ЗМІСТ

УДК 343.9
ОЛЕКСАНДР МИКОЛАЙОВИЧ ГОЛОВКО
Доктор юридичних наук, професор, проректор Харківського національного університету внутрішніх справ

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Однією з найхарактерніших рис сьогодення є стрімкий перехід людства із сфери матеріальних відношень у сферу віртуальних відношень у кіберпросторі. За даними ООН число людей, що мають можливість регулярно користуватися Інтернетом, сягнуло до 3 мільярдів. Загальна кількість власників мобільних телефонів та смартфонів перевищує 6 мільярдів. Все більше фінансово-розрахункових операцій здійснюється з використання електронних засобів витісняючи готівкові розрахунки. Таким чином, основним компонентом інфраструктури віртуальних відносин у кіберпросторі є комп'ютерні і телекомунікаційні мережі. Їх дедалі більше як інструменти скоєння злочинів використовують злочинці. Відповідним чином поступово змінюється і структура злочинності. В таких умовах зростає значення оперативності реакції правоохоронних органів на скоєні злочини та ефективність їх виявлення і розслідування. Значною мірою забезпечення успішного розв'язання цих завдань залежить від ефективної роботи інформаційних підрозділів органів внутрішніх справ зі зміщенням акцентів у бік саме аналітичної роботи.

Завдання системного реформування органів внутрішніх справ (ОВС), що має на меті якісне підвищення ефективності їх роботи по боротьбі зі злочинністю, охороні громадського порядку і захисту прав громадян, передбачає якісне реформування існуючого інформаційного забезпечення, яке має відповідати змінам структури ОВС і відповідати вирішуваним ними завданням.

На сьогоднішній день в ОВС розроблені і активно використовуються цілий ряд інформаційних систем («ІБД», «Розшук», «Арсенал» та ін.), що складають загальну систему інформаційного забезпечення ОВС. В існуючому вигляді вона забезпечує вирішення наступних завдань:

- надання можливості оперативного отримання співробітникам або підрозділам ОВС інформації в повному, систематизованому і зручному для використання вигляді для розкриття, розслідування та попередження злочинів і пошуку злочинців;
- збір, обробка та узагальнення оперативно-довідкової, аналітичної, статистичної та контрольної інформації для оцінки ситуації та прийняття обґрунтованих оптимальних рішень на всіх рівнях управління ОВС;
- вдосконалення організаційно-кадрового та інформаційного забезпечення підрозділів;
- інтеграція та систематизація інформаційних обліків ОВС на всіх рівнях, а також створення умов для їх ефективного використання.

У рамках здійснюваної в даний час в Україні реформи МВС змінюється парадигма правоохоронної системи. Ліквідується цілий ряд існуючих підрозділів і створюються нові з іншими завданнями і функціями.

У цих умовах система інформаційного забезпечення ОВС також повинна бути адекватно перебудована з тим, щоб відповідати зміненим завданням і умовам.

Реформа інформаційної системи ОВС повинна розвиватися за наступними напрямками:

- визначення цілей і завдань модернізації системи інформаційного забезпечення ОВС;
- розробка нормативно-правових актів, що визначають порядок і механізм модернізації;
- розробка та впровадження системи стратегічного планування і управління процесами інформатизації ОВС України;

- розробка інформаційних підсистем (підзадач) для нових підрозділів ОВС та їх інтеграція в існуючу систему;
- вдосконалення телекомунікаційної складової з метою забезпечення виконання нових завдань реформованої системи ОВС;
- модернізація існуючої системи захисту інформації;
- підготовка особового складу до змін у загальній системі інформаційного забезпечення, а також навчання співробітників нових підрозділів грамотному використанню інформаційних систем для вирішення оперативно-службових завдань;
- підготовка персоналу для супроводу, адміністрування та технічного обслуговування інформаційних підсистем;
- модернізація існуючої технічної бази відповідно до зміненими вимогами.

Вирішення цих завдань забезпечить створення сучасної інформаційної системи ОВС, що сприятиме реалізації державної політики у сфері реформування системи правоохоронних органів та боротьби зі злочинністю.

УДК 65.012.8 + 004

МИКОЛА МИЛЕНТІЙОВИЧ ЗАЦЕРКЛЯНИЙ
Доктор технічних наук, професор, професор кафедри інформаційної та економічної безпеки навчально-наукового інституту підготовки фахівців для підрозділів кримінальної міліції Харківського національного університету внутрішніх справ
ВОЛОДИМИР МИХАЛОВИЧ СТРУКОВ
Кандидат технічних наук, доцент, завідувач кафедри інформаційних технологій та захисту інформації факультету права та масових комунікацій Харківського національного університету внутрішніх справ

СУЧАСНИЙ СТАН КАДРОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ ПІДРОЗДІЛІВ ОВС УКРАЇНИ

В даний час інформаційна служба як і всі підрозділи органів внутрішніх справ України переживає складний період реформування. Цей процес зачіпає

різні аспекти діяльності. По-перше, ось уже другий рік як служба перестала отримувати кадрову підтримку з ХНУВС - випускників спеціальності «комп'ютерні науки», підготовлених як в технічному, так і в міліцейському аспекті. Ці фахівці найбільшою мірою були пристосовані працювати в інформаційно-аналітичних підрозділах органів внутрішніх справ відразу після закінчення вузу як з точки зору мотивації так і з точки зору технічної та міліцейській підготовленості. Зараз випускники ХНУВС цієї спеціальності займають ключові посади фахівців у більшості обласних інформаційно-аналітичних підрозділів. Таких спеціалістів на сьогодні вкрай не достатньо не тільки на територіальному, а й на регіональному рівні, про що свідчать керівники практично всіх інформаційно-аналітичних підрозділів у регіонах, з якими традиційно науковці ХНУВС підтримують тісні ділові зв'язки. В цьому переконуються і викладачі, які проводять заняття в рамках підвищення кваліфікації працівників інформаційно-аналітичних підрозділів: посади не тільки інспекторів, а й інженерів-програмістів, особливо на територіальну рівні в деяких випадках займають психологи та учителі російської мови і літератури, а іноді "спеціалісти " із середньою освітою (11 класів). Потреба в спеціалістах для інформаційно-аналітичних підрозділів збільшилася після прийняття нового кримінально-процесуального кодексу і введення в експлуатацію інформаційної системи "Єдиний реєстр досудових розслідувань".

По-друге, як відомо, через різке падіння курсу гривні заробітна плата фахівців, які отримують її в доларовому еквіваленті, стала в кілька разів(!) перевищувати заробітну плату фахівців, зайнятих у бюджетній сфері. Природним чином це прискорило відтік висококваліфікованих IT-спеціалістів в приватні структури саме з бюджетних організацій. З чого однозначно випливає, що при нинішньому рівні заробітної платі і умовах служби не доводиться очікувати напливу великої кількості талановитих молодих фахівців із цивільних технічних вузів. По-третє, фінансування саме розвитку більшості бюджетних організацій (у тому числі і органів внутрішніх

справ) в силу відомих причин зараз обмежене. І якщо ФБР мало можливість собі дозволити витратити 1 мільярд доларів тільки на комп'ютерну програму динамічного розпізнавання облич (так само як і китайський департамент фінансового моніторингу), то ДІАЗ МВС України в основному може розраховувати лише на зарубіжну фінансову підтримку, оскільки основне бюджетне фінансування направлене на реорганізацію міліції.

Як один з можливих компромісних варіантів розв'язання цієї проблеми – поновлення набору на спеціальність «Компютерні науки» у варіанті 2+2: 2 роки навчання за кошти кандидатів, 2 роки – навчання за бюджетні кошти.

УДК 343.9
ДМИТРИЙ ЮРЬЕВИЧ УЗЛОВ
К.т.н., начальник Управления информационно-аналитического обеспечения ГУ МВД Украины в Харьковской области, полковник милиции
АЛЕКСЕЙ БОРИСОВИЧ ГРИГОРОВИЧ
Начальник отдела Управления информационно-аналитического обеспечения ГУ МВД Украины в Харьковской области, капитан милиции
АРТЕМ ИВАНОВИЧ ПЕТРУСЕНКО
Старший инженер программист управления информационно-аналитического обеспечения ГУ МВД Украины в Харьковской области, старший лейтенант милиции
АЛЕКСАНДР АЛЕКСАНДРОВИЧ ТАРАСЕНКО
Инспектор Управления информационно-аналитического обеспечения ГУМВД Украины в Харьковской области, лейтенант милиции

ИСПОЛЬЗОВАНИЕ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ КРИМИНАЛЬНОГО АНАЛИЗА В РЕАЛЬНОМ ВРЕМЕНИ (RICAS) В КАЧЕСТВЕ ПЛАТФОРМЫ АНАЛИТИЧЕСКОГО ПОИСКА И КРИМИНАЛЬНОГО ИССЛЕДОВАНИЯ.

Анализ запросов, которые поступают в подразделения информационно-аналитического обеспечения, показывает, что основными являются запросы поиска преступлений по аналогии и лиц совершивших аналогичные преступления. Существующая система запросов ИИПС позволяет выводить

списки, размеры которых иногда составляют сотни преступлений и тысячи лиц. Дальнейшая обработка осуществляется путём классификации или кластеризации, по каким либо критериям (предопределенным или заранее неизвестным). Данный процесс является не тривиальным, зависит от квалификации исполнителя, не автоматизирован и требует специальных навыков работы с ИИПС и СУБД.

Задачи кластеризации и классификации, решаемые технологией Text Mining, для выделения криминально значимой информации приобретают новое качество при одновременном использовании с технологией Visual Mining. При этом в качестве инструментария визуализации предлагается использование Интеллектуальной системы криминального анализа в реальном времени – Real-time Intelligence crime analytics system (RICAS), которая позволит связать географическое пространство, время и события в одном визуальном пространстве отображения.

Построение системы обусловлено следующим:

- 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;

- любые субъект и объект преступления имеют привязки к географическим координатам в текстовом формате (адрес прописки, проживания, регистрация предприятия, места работы, регистрации транспортного средства, оружия и т.д.);

- криминальные события, субъекты и объекты могут иметь взаимосвязи, которые легче обнаружить путем 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.

Данные утверждения позволяют при применении технологий Data Mining, Text Mining, Visual Mining, Link Analyzes производить следующие операции с потоками входных данных:

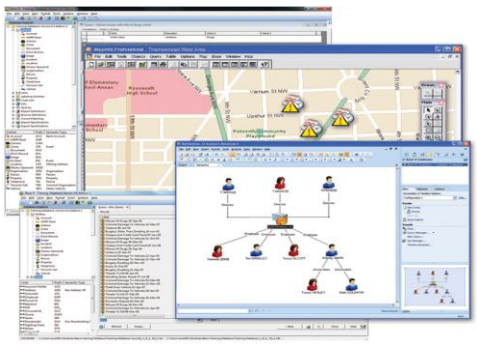
- кластеризации объектов по одному или нескольким признакам, которые имеют общие пространственно-временные характеристики;

- создание временной ленты событий по определенному географическому месту (ретроспективный анализ событий места происшествия);

- группировка объектов и субъектов вокруг события;

- анализ связей лиц, объектов, событий.

Проведенный анализ существующих решений показал наличие определенных программных продуктов, которые позволяют частично решать описываемые задачи. Существует решение от корпорации IBM для задач правоохранительных органов – I2. Данный продукт позволяет отображать данные имеющиеся в хранилище, создаваемом под оболочкой I2 в формате хранения продуктов IBM, на собственных картах и проводить анализ связей данных.



Продукт 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, продукт не обеспечивает возможность связать географическое пространство, время, событие в одном визуальном пространстве отображения.

CRIMEVIEW Server - используется в полицейском департаменте города Глендейл (Калифорния). Основан на картографической платформе ESRI.Основной принцип - анализ зон с максимальным уровнем уличной преступности. Изменение маршрутов патрулирования в выявленные зоны.

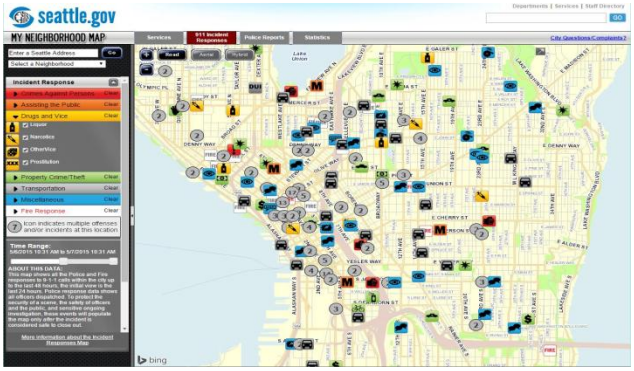
My Neighborhood Map System - используется в городе Сиэтл (Вашингтон). Состоит из модулей:

911 INCIDENT RESPONSES MAP

POLICE REPORTS MAP

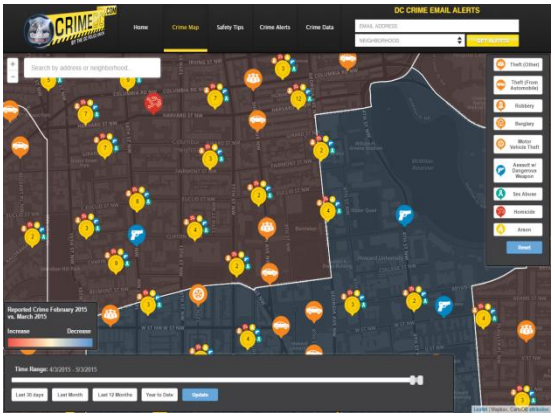
MONTHLY CRIME STATISTICS MAP

Основное назначение - визуализация поступающих сообщений о преступлениях, и отчетов полиции.



CRIMEDC - используется в полицейском департаменте города Вашингтон.

Основное назначение - предоставление общественности данных о совершенных преступлениях.



Большинство рассмотренных систем, представляют из себя решения для **информирования общественности.**

Предлагаемая система RICAS предлагает качественно новый метод и механизм представления данных, являясь надстройкой к существующей ИИПС ОВД Украины, и открывает возможности использования математических инструментов технологий DATA MINING, VISUAL MINING и OLAP.

Назначение системы:

- Повышение эффективности использования информационных учетов в оперативно-розыскной деятельности сотрудников ОВД, деятельности по охране общественного порядка

- Уменьшение времени реакции на поступающую информацию о преступлениях и правонарушениях, и как следствие, более эффективное их раскрытие по горячим следам и профилактика.

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

Платформа для работы аналитиков с такими видами криминального анализа, как: crime pattern analysis (анализ криминальной обстановки), generalprofile analysis (анализ общего профиля), case analysis (анализ конкретного расследования), comparativ analysis (сравнительный анализ), offender group analysis (анализ групповой преступности), specific profile analysis (анализ особенностей профиля), investigation analysis (анализ расследований).

Решаемые задачи:

- Визуализация геоинформационных данных и событийных цепочек.
- Составление поведенческого профиля преступника или преступной группы.
- Кластеризация событий.
- Кластеризация преступников.
- Связывание кластеров событий с кластерами преступников.

Применение RICAS на массивах данных ИИПС показало эффективность работы в качестве инструмента для исследования нераскрытых преступлений, выделения поведенческого профиля преступников по раскрытым преступлениям, общего анализа криминогенной ситуации по заданной территории и видам преступлений.

Список литературы:

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 // Інтелектуаль-ні системи та прикладна лінгвістика: Матеріали III Всеукраїнської науково-практичної конференції. – Харків : НТУ «ХПІ», 2014. – С. 13-15.

3) Узлов Д. Ю. Використання поведінкового профілю для виявлення ознак кіберзлочинності / Д. Ю. Узлов // Використання інноваційних технологій у попередженні злочинів : матеріали науково-практичного семінару. – Харків : МВС України, ХНУВС, 2012. – С. 161-164.
4) Узлов Д. Ю. 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. – Харків : ПП «Технологічний Центр», 2014. – № 3/2 (69). – С. 4-8.
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. Ad-vanced Analytic & Information Sharing Technologies / C. Westphal. – New York : CRC Press Taylor & Francis Group, 2009. – 440 p.

УДК 343.9
ЛЕПЁХИН АЛЕКСАНДР НИКОЛАЕВИЧ
кандидат юридических наук, доцент, начальник кафедры правовой информатики Академии МВД Республики Беларусь

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ РАБОТА В ОРГАНАХ ВНУТРЕНИХ ДЕЛ: ИСТОРИКО-ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ

Вопросы информационного обеспечения служебной деятельности всегда имели актуальное значение для органов внутренних дел Республики Беларусь. Рассматривая исторический аспект создания и функционирования информационных (информационно-аналитических) служб в структуре Министерства внутренних дел, следует отметить, что датой отсчета в истории информационных подразделений системы МВД считается 1

сентября 1921 года, когда на заседании коллегии НКВД Советской Социалистической Республики Белоруссия, было принято решение об организации Статистического бюро при Наркомате внутренних дел.

21 апреля 1924 года было утверждено Положение о Статистическом бюро, которое вошло в состав административно-организационного управления наркомата. Следует отметить, что на протяжении XX века информационно-аналитическая работа в деятельности органов внутренних дел развивалась относительно медленно и не совсем эффективно.

Развитие информационных технологий в XXI веке, безусловно, повлияло на активное их внедрение в деятельность Министерства внутренних дел Республики Беларусь. Руководством МВД принято решение, что структура органов внутренних дел должна отвечать современным реалиям жизни, поэтому в феврале 2001 года информационно-аналитический центр МВД преобразуется в центральное информационно-аналитическое управление МВД.

Очевидно, что в современном мире информационно-аналитическая работа как составная часть управленческой деятельности не может осуществляться «факультативно», она неизбежно требует функционального выделения, организационного оформления и специализации по функциям сбора, накопления, обработки, выдачи, анализа и реализации информации в интересах подготовки вариантов решений на различных уровнях. Это и составляет сущность понятия информационно-аналитической работы в органах внутренних дел.

В феврале 2004 года центральное информационно-аналитическое управление МВД переименовывается в информационно-аналитическое управление МВД, подчиненное непосредственно Министру внутренних дел.

Новым этапом в деятельности органов внутренних дел и всей правоохранительной системы стало введение в действие единой государственной системы регистрации и учета правонарушений, которая способствовала совершенствованию правового регулирования этой

деятельности и существенно улучшила организацию сети передачи данных в органах внутренних дел. Каждый сотрудник милиции по выделенным каналам связи получил доступ к республиканским банкам данных, что способствовало оперативному получению информации о зарегистрированных правонарушениях. Данные об этом поступают в МВД в течение часа, статистические сведения о регистрации и предварительном расследовании преступлений формируются в автоматическом режиме ежесуточно в разрезе каждого органа внутренних дел. Это способствовало оперативному формированию и предоставлению статистических сведений.

Следующим этапом развития информационно-аналитической работы в органах внутренних дел следует считать принятие Инструкции о порядке функционирования оперативно-справочных картотек информационно-аналитических подразделений органов внутренних дел Республики Беларусь, которая определила порядок функционирования оперативно-справочных картотек информационно-аналитических подразделений органов внутренних дел Республики Беларусь. В соответствии с Инструкцией сотрудники информационных подразделений предоставляют органам уголовного преследования, судам, другим государственным органам и иным организациям, а также физическим лицам сведения, находящиеся в едином государственном банке данных о правонарушениях, оперативно-справочных и архивных картотеках, о привлечении лиц к уголовной и административной ответственности, судимости, времени и месте отбывания наказания, реабилитации, розыске.

В 2009 году информационно-аналитическое управление переименовывается в информационный центр МВД Республики Беларусь и становится структурным подразделением Штаба МВД.

Задачами данного подразделения являются:

формирование и обеспечение функционирования единой государственной системы регистрации и учета правонарушений;

формирование единого государственного банка данных о правонарушениях;

сбор, обработка, обобщение, накопление, хранение и предоставление розыскной, профилактической, оперативно-справочной и архивной информации;

накопление, хранение и предоставление статистической информации о правонарушениях;

предоставление в установленном порядке:

государственным органам и иным организациям Республики Беларусь, а также физическим лицам сведений о правонарушениях;

органам, ведущим уголовный процесс, другим государственным органам и иным организациям, а также физическим лицам сведений о привлечении лиц к уголовной или административной ответственности, судимости, времени и месте отбывания наказания, реабилитации, розыске, находящихся в едином государственном банке данных о правонарушениях и оперативно-справочных картотеках.

Вместе с тем, следует отметить, что лишение самостоятельного статуса информационно-аналитического подразделения МВД Республики Беларусь имело, в целом, недостаточно конструктивные последствия. Поскольку из названия подразделения и его задач были исключены аналитические функции, что отрицательно отразилось на решении задач, стоящих перед органами внутренних дел Республики Беларусь, так как основы управления обуславливают не только получение и накопление информации, но и ее анализ и предоставление руководству для принятия соответствующих управленческих решений. В этой связи, в настоящее время, в отдельных подразделениях Министерства внутренних дел Республики Беларусь уже созданы информационно-аналитические подразделения, решающие задачи в рамках данного направления и, вполне закономерно, ставиться вопрос о создании информационно-аналитического подразделения Министерства, решающего задачи сбора, накопления и анализа информации с учетом

современных требований, а не, собственно, статистического подразделения, предметом деятельности которого являлись отдельные показатели преступности и их сравнение с предыдущими периодами.

Таким образом, информационно-аналитическая работа является связующим звеном для всех подразделений органов внутренних дел, как с точки зрения вертикальных связей, так и связей горизонтальных. Предметная область такой работы представляет собой отображение всей сферы функциональной ответственности органов внутренних дел и охватывает информационное поле, отражающее обобщенную деятельность всей правоохранительной системы страны. И, поскольку, основные объекты предметной области информационно-аналитической работы безусловно относятся к большим и сложным системам, они требуют использования адекватного научно-теоретического аппарата, специального комплекса информационно-аналитических методов, соответствующего обеспечения необходимой материально-технической базой, прежде всего, вычислительной и другой техникой, предметно ориентированным персоналом, а также разработки, апробации и практического внедрения единой автоматизированно-управленческой системы.

УДК 004.75
Ю.П.ГОРЕЛОВ
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та захисту інформації Харківського національного університету внутрішніх справ
П.Є.МИНКО
кандидат фізико-математичних наук, доцент, декан факультета ФСЕУ ХарРІ НАДУ при Президентові України

ДО ПИТАННЯ РОЗРОБКИ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ НАВЧАННЯ

Одним з найбільш перспективних напрямків в галузі створення комп'ютерних засобів навчання є розробка й впровадження навчаючих

систем на основі принципів та методів штучного інтелекту. Інтелектуальні навчаючі системи (ІНС) дозволяють значно підвищити ефективність навчання за рахунок використання досягнень інженерії знань і керування процесом навчання на основі знань різних класів.

Аналіз можливостей сучасних інформаційних технологій, психологічних механізмів сприйняття й переробки інформації людиною та структурних елементів існуючих технологій навчання дозволяє сформулювати ряд вимог до функцій, складу та структури ІНС.

ІНС повинна мати наступні можливості:

1. Використання різних методів навчання. Вибір конкретного методу здійснюється на основі знань системи про цілі навчання, про цілі сеансу роботи, модель студента і знань про методи навчання.
2. Використання різних форм подання інформації студенту (комп'ютерна графіка, засоби мультимедіа та ін.).
3. Реалізація різних форм взаємодії зі студентом, у т.ч. адаптивний цілеспрямований природно-мовний діалог.
4. Адаптація до рівня знань, пізнавальним можливостям та іншим параметрам студента на основі його моделі.
5. Керування процесом взаємодії зі студентом, що складається у створенні та реалізації керуючих впливів на основі оцінки рівня засвоєння навчального матеріалу.
6. Наявність розвинених засобів подання, зберігання та формування різних класів знань, механізмів виводу, та синтезу планів досягнення цілей.

Сукупність цих вимог дозволяє виділити наступні основні компоненти ІНС: база знань, інтелектуальний інтерфейс, підсистема міркувань, підсистема планування та керування навчанням, підсистема тестування, підсистема формування знань, підсистема сполучення із програмними й апаратними засобами.

Основою функціонування зазначених підсистем є обробка різних класів знань, представлених як у декларативної, так й у процедурної формах.

База знань ІНС містить наступні класи знань: знання про предметну область, лінгвістичні знання, знання про організацію навчання, моделі користувачів, знання про діалог, знання про цілі і способах реалізації різних дій, знання про свої можливості, знання про форми подання інформації користувачеві. Знання про предметну галузь включає опис семантики понять й об'єктів, взаємозв'язків між ними й алгоритмів виконання різних дій. Лінгвістичні знання й знання про діалог становлять основу функціонування інтелектуального інтерфейсу, що реалізує режим інтерактивного діалогу як у процесі навчання, так й у режимі формування знань користувачем-експертом. Знання про організацію навчання й форми подання інформації користувачеві становлять моделі навчання, що лежать в основі реалізації відповідних стратегій навчання. Моделі навчання, а також знання про цілі і способи виконання дій та своїх можливостей використовуються в підсистемі планування та керування навчанням.

Як модель адаптації пропонується оверлейна модель знань й умінь студента, у якій уміння представляються у вигляді множини операцій і приписаних їм значень, що характеризують ступінь освоєння операції.

На основі оверлейної моделі вмінь забезпечується адаптивне керування процесом навчання. Система на основі аналізу поточного стану вмінь для наступного кроку вибирає навчальне завдання певного рівня, забезпечує процес освоєння матеріалу, проводить тест, по його підсумках вносить зміни в модель студента, і корегує процес навчання.

Навчальний матеріал представляється у вигляді сукупності навчальних об'єктів (НО) і набору відносин. Навчальний об'єкт є структурним компонентом з певною адресою, що забезпечує можливість посилання й переходу на об'єкт із інших компонентів, блоку змісту БЗ, покажчика, словника (глосарія), тезауруса та контролюючого тесту або навчального завдання.

Структура матеріалу представлена у вигляді графа, вершинам якого відповідають об'єкти, а ребрам - відносини між ними. Виділено відносини трьох типів: ієрархічні, переглядові, семантичні.

Основа оверлейної моделі вмінь студента представляється у вигляді вектора $P(k)=[P_1(k), P_2(k), ..., P_j(k), ..., P_J(k)]$, де $P_j(k)$ – імовірність правильного застосування операції j-го типу, що обчислюється з використанням байесовського підходу за результатами рішення навчального завдання на k-ом кроці навчання. Для кожного навчального завдання встановлюється взаємозв'язок використовуваних операцій і понять на основі матриці відповідності. У процесі навчання на основі тестів визначаються оцінки засвоєння й незасвоєння операцій і понять на кожному кроці.

По завершенні виконання завдань у випадку наявності помилок формується повідомлення, що містить перелік посилань на НО та сторінки, де вони містяться, з вказівкою студенту повернутися до повторного вивчення представленого в них навчального матеріалу. Перелік сторінок впорядковується за зниженням оцінок незасвоєння, тобто студенту пропонується для вивчення в першу чергу ті сторінки, які гірше засвоєні.

Розробка й впровадження ІНС, що реалізують такий підхід, у рамках створення системи дистанційного навчання дозволяє підвищити швидкість та якість навчання.

УДК 378.14
К.Е. ПЕТРОВ
доктор технічних наук, професор, професор кафедри інформаційних технологій та захисту інформації, Харківській національний університет внутрішніх справ
Д.О.РУДЕНКО
кандидат технічних наук, доцент, доцент кафедри інформатики, Харківський національний університету радіоелектроніки

БЕЗПЕКА ВИКОРИСТАННЯ WEB- СЕРВЕРІВ ТА ЗАСТОСУВАНЬ

На сьогодні уразливості в Web-застосуваннях, як і раніше, залишаються одним з найбільш поширених недоліків забезпечення захисту інформації. Попри те, що уразливості Web-застосувань неодноразово описані в «науково-популярній» і спеціалізованій літературі, досить рідко зустрічається опис превентивних захисних механізмів, що знижують ризики використання цих вразливостей.

Недооцінка серйозності ризику реалізації загроз інформаційній безпеці з використанням Web-застосувань, доступних з боку мережі Internet, можливо, є одним з головних чинників низького рівня захищеності більшості з них. За даними статистики, в 2013 році на 63% сайтах були виявлені критичні уразливості за допомогою яких можна здійснити успішну атаку на Web-застосування або сервер. Найбільша кількість Web-застосувань, що містять вразливості високої міри ризику, була виявлена серед Web-застосувань, що належать засобам масової інформації, де у 80% випадків рівень уразливості виявився критичним [1].

Більшість організацій, що приділяють багато уваги оформленню своїх сайтів, іноді нехтують основними принципами їх безпечного існування. Нещодавні атаки на Web-сайти показали, що працездатність серверів може бути порушена навіть в результаті перевантаження одного або декількох сервісів.

Для правильної організації захисту Web-сервера і при створенні безпечно працюючого Web-застосування необхідно розуміти як виникають

уразливості і яким чином вони можуть бути використані.

Звичайно самий кращий захист – це відсутність вразливостей. Тому ще на етапі первинного налаштування політики безпеки Web-сервера або написання Web-застосування необхідно враховувати, які дії може здійснити зловмисник для злому, і заздалегідь вжити певні заходи. Адже тільки сам розробник повинен точно знати, які дані повинні поступати і як вони повинні оброблятися, а які дані на сервер потрапити ні в якому разі не повинні. Тому перед розробкою Web-застосування рекомендується розробити модель порушника і модель загроз. Але у будь-якому випадку, коли додаток вже написано, необхідно захищати його і Web-сервер, на якому додаток знаходиться.

Захист Web-сервера – це комплекс організаційних і технічних заходів. Тому для правильної організації захисту Web-сервера в першу чергу необхідно з'ясувати, які уразливості є присутніми в Web-застосуваннях і політиці безпеки Web-сервера. Проведення аудиту дозволяє виявити помилки і оцінити захищеність Web-застосування, а також отримати набір рекомендацій щодо посиленню захисту.

Найбільш поширеними підходами до технологічного аудиту є тест на проникнення (показова демонстрація дій порушника) і «традиційний» аудит (аналіз параметрів конфігурації Web-сервера і застосування сканера вразливостей). Останнім часом виділяється ще один тип аудиту – активний, який поєднує в собі можливості обох підходів і усуває деякі їх недоліки.

Аудит повинен проводитися регулярно, оскільки постійно виявляються нові уразливості операційних систем, на яких розміщуються Web-сервери; знаходяться нові методи атак на Web-застосування; допрацьовуються сканери вразливостей; відбуваються збої в політиці безпеки. Після закінчення аудиту надаються рекомендації щодо модернізації системи мережевого захисту, які дозволяють усунути небезпечні уразливості і тим самим підвищити рівень захищеності інформаційної системи від дій зовнішнього порушника. Природно, що найкращим методом боротьби з

вразливостями є виправлення коду Web-застосування і грамотне налаштування політики безпеки. Але зустрічаються ситуації, коли змінити само Web-застосування немає можливості або відсутні права на налаштування політики безпеки на Web-сервері. Тобто одними організаційними заходами проблему безпеки розв'язати неможливо. У таких випадках доводиться застосовувати технічні заходи для захисту, тобто встановлювати сторонні засоби для забезпечення захисту інформаційної системи.

Одним із засобів усунення вразливостей і одночасно профілактичним заходом є встановлення Web Application Firewall (WAF). WAF є програмним або апаратним міжмережним екраном для Web-застосувань. Такого роду міжмережний екран встановлюється перед Web-застосуванням і надає ширші можливості, ніж звичайні програмні екрани для системи. WAF в змозі контролювати усі об'єкти, які можуть бути доступні користувачам – URL, що вводяться, а також параметри запитів GET і POST. Також міжмережний екран не дозволяє користувачам запускати об'єкти, що не належать до Web-ресурсу [2].

Можна виділити такі три рівні безпеки для сервера.

Рівень 1. Мінімальний рівень безпеки – модернізація наявного програмного забезпечення; єдині налаштування (політика) для усіх серверів.

Рівень 2. Опір вторгненню – встановлення зовнішнього міжмережного екрану; видалене адміністрування систем безпеки; обмеження на використання скриптів; захист Web-серверів з використанням фільтрації пакетів; навчання персоналу і розмежування прав доступу.

Рівень 3. Виявлення атак і послаблення їх дії – розподіл привілеїв; апаратні системи захисту; внутрішній міжмережний екран; мережні системи виявлення вторгнень; системи виявлення вторгнень, що розміщуються на серверах (хостах).

Незважаючи на усі спроби реалізувати безпечну конфігурацію, неможливо добитися гарантованого виключення усіх вразливостей. Тим

більше що Web-сервер, захищений від зовнішніх атак, може бути виведений з ладу порушенням роботи одного з сервісів. В цьому випадку важливо отримувати оперативну інформацію про подібні події, для мінімізації наслідків атаки або швидкого відновлення працездатності сервісу.

На теперішній час нормальне функціонування Web-сервера, підключеного до мережі Internet, практично неможливе, якщо не приділяти належну увагу питанням забезпечення його інформаційної безпеки. Ця проблема може бути вирішена шляхом використання комплексного підходу до захисту ресурсів сервера від можливих атак. Для цього до складу комплексу засобів захисту сервера повинні входити системи антивірусного захисту, контролю цілісності, виявлення вторгнень, розмежування доступу, криптографічного захисту, а також підсистема управління. При цьому кожна з систем повинна бути оснащена елементами власної безпеки.

Література:

1. Статистика уязвимостей Веб-приложений (2013 год) [Електронний ресурс]. - Режим доступу URL: http://www.ptsecurity.ru/download/PT_Web_application_vulnerability_2014_rus.pdf.

2. Web Application Firewall [Електронний ресурс]. - Режим доступу URL: https://www.owasp.org/index.php/Web_Application_Firewall.

УДК 343.9
ДМИТРИЙ ЮРЬЕВИЧ УЗЛОВ
К.т.н., начальник Управления информационно-аналитического обеспечения ГУМВД Украины в Харьковской области, полковник милиции
АЛЕКСЕЙ ВЯЧЕСЛАВОВИЧ ВЛАСОВ
Заместитель начальника Управления информационно-аналитического обеспечения ГУМВД Украины в Харьковской области, подполковник милиции
РУСЛАН ВАДИМОВИЧ БОРОВИК
Главный специалист Управления информационно-аналитического обеспечения ГУМВД Украины в Харьковской области, старший лейтенант милиции
СТАНИСЛАВ НИКОЛАЕВИЧ ДОСКАЛЕНКО
Инженер-программист Управления информационно-аналитического обеспечения ГУМВД Украины в Харьковской области, лейтенант милиции

ОСНОВНІ ПРИНЦИПИ ФУНКЦІОНУВАННЯ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ КРИМІНАЛЬНОГО АНАЛІЗУ В РЕАЛЬНОМУ ЧАСІ (RICAS)

Криминальный анализ в своем обыденном понимании является систематическим изучением уровня преступности, концентрации мест совершенных преступлений по видам и иным параметрам. Необходимо различать два вида криминального анализа – это аналитический поиск и аналитическое исследование. В тоже время эти два вида криминального анализа, в зависимости от поставленной задачи всегда будут дополнять друг друга. На данный момент не было систем криминального анализа, позволяющих в едином пространстве отображения соединить эти два вида анализа. Большинство из подобных продуктов имеют огромное количество инструментов для визуального криминального анализа, но инструментов для аналитического поиска у них нет.

Специфика деятельности полиции и других органов, задействованных в расследовательной и розыскной деятельности, всегда охватывала широкий спектр фигурируемых исходных данных. Событие (преступление), которое будет подлежать аналитическому поиску, зачастую имеет три компоненты:

пространственная, временная и описательная. Следовательно, анализ события будет носить пространственно-временной характер.

Зачастую, базируясь на многозначной логике, и имея достаточное количество описательных компонент, можно с достаточно высокой вероятностью идентифицировать то или иное событие с любой точки зрения. В теории, так или иначе, абсолютно все события, происходящие во Вселенной взаимосвязаны. Остается лишь узнать базовую логику, связывающую все динамические процессы. В теории оперативно-розыскной деятельности такая логика детализирована с точки зрения криминального процесса и логики предикатов. Так, внезапная вспышка квартирных краж в одном районе однозначно может быть объяснена тем, что недавно из мест лишения свободы был освобожден субъект, ранее осужденный за этот же вид краж, проживающий в этом же районе. Но это лишь часть логических умозаключений, которые можно строить, имея в наличии Большие данные. Такое простое логическое заключение, на самом деле, очень сложно сделать, имея лишь стопки необработанных бумаг. Естественно, в последнее время вся информация обо всех происшествиях вносится в базы данных органов внутренних дел, однако инструментов позволяющих эффективно анализировать подобную информацию попросту не было. Появилась необходимость создать нечто новое, но в тоже время и хорошо забытое старое. Самым обыденным примером будет огромная статическая карта возле стола сотрудника полиции, на которой отмечены места, где совершены преступления, и возможные фигуранты. Безусловно, это невероятно удобный инструмент, но у него нет доступа к записям, несущих потенциально полезную информацию.

На современном этапе развития информационно-аналитических технологий появилось четкое осознание того, что инструменты криминального анализа, поиска, построения связей, анализа поведенческого профиля и прочих аналитических методик, должны быть единой целой

системой, предоставляющей аналитику полный спектр решений, 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, включающие в себя методы аналитического поиска, что является очень приоритетным для возможности раскрытия преступлений как по горячим следам, так и преступлений прошлых лет. Так же система включает в себя элементы базовой криминальной аналитики.

Основой аналитической работы в системе является визуальный анализ. Обеспечивается он отображением всех необходимых данных в едином информационно-географическом пространстве. Система позволяет проводить следующие виды анализа: Crime pattern analysis, General profile analysis, Methods analysis, Case analysis, Comparative analysis, Offender group analysis, Specific profile analysis, Investigation analysis. Используя все эти виды анализа интегрально, появляется возможность видеть картину целиком - предикативно и постфактум.

Т.к. система является надстройкой над существующими базами данных, она может принимать 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 по лицам, участвовавших в разных событиях. Второй - визуальный поиск связей. В процессе вывода структурированной информации в визуальную среду отображения, становятся очевидными связи типа "место совершения-подельник-преступник", "преступление-подозреваемый-подельники". Инструментарий позволяет с легкостью настраивать связи и пополнять ими базу данных.

Интеллектуальный контекстный анализ. Система 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 автоматизированной классификации или "тегирования". Анализируются все события, связанные с лицом и его подельниками, что позволяет анализировать групповую преступность по разнообразным направлениям, что порождает анализ поведенческого профиля группы.

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. Все функции выполняются мгновенно и позволяют максимально быстро визуализировать информацию и проводить аналитическую работу.

Система включает в себя визуальный темпоральный анализ. Отображение хронологии произошедших событий и временное разграничение позволяет оперативно выявлять скрытые пространственно-временные закономерности между разными событиями.

Следует сформулировать основные принципы, на которых строится работа интеллектуальной системы криминального анализа в реальном времени.

Принцип поведенческого профилирования: наиболее постоянным и точным, с точки зрения, психологии преступника, является его поведенческий профиль. Он отображает многие параметры деятельности преступника - привычный способ совершения преступления, места совершения и прочие мелкие зависимости, которые в совокупности соответствуют только единому профилю.

Наличие тех или иных **поведенческих признаков**, с определенной долей вероятности могут свидетельствовать о том, что данный субъект может быть причастен к событию. 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 единых событиях.

Именно поэтому принцип группового поведенческого анализа является очень важным. Он позволяет определять подельников, сообщников, казалось бы, без явных связей между собой.

Для выявления подобного рода связей используется алгоритм поиска скрытых закономерностей.

Принцип поиска скрытых закономерностей. Скрытые закономерности с высокой долей вероятности всегда могут идентифицировать связь между преступником и всеми совершенными им преступлениями. 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, базируясь на интеллектуальном ядре обработки семантики. Семантический анализ является основополагающим, поскольку связи построены не всегда явно и их следует искать в контексте.

Принцип семантической целостности. Зачастую все события и поведенческие профили преступников описаны словесно. Поэтому интеллектуальный модуль обработки семантики является основополагающим.

Он раскрывает широкие возможности анализа скрытых закономерностей и контекстного поиска. Безусловно, отталкиваясь от разнообразия компьютерных "почерков", модуль откалиброван разнообразнейшими словарными соответствиями.

Принцип визуального анализа. Основополагающим в RICAS есть принятие решения аналитиком, следовательно, визуальная компонента является очень важной.

Все вязи между субъектами и объектами отображены визуально и на гео-информационной подложке, при этом учитывается классификационные признаки и аналитические данные.

Принцип прозрачности. Безусловно, все процессы анализа и сбора данных в аналитической деятельности системы являются прозрачными и открытыми для лиц, имеющих доступ. Так, базируясь на логике предикатов можно доказать каким образом было выведено то или иное утверждение.

Этот же принцип касается публичных карт преступной напряженности, позволяющих в секунды анализировать места концентрации опасных мест.

Мультиплатформенность и простота. Система разрабатывалась с использованием современных, оптимизированных технологий в веб-пространстве. Ее можно использовать на любых стационарных и мобильных устройствах при наличии защищенного канала связи. Интерфейс системы не перегружает пользователя.

УДК 343.982.33
ДМИТРО ВІКТОРОВИЧ ДАБІЖА
ад'юнкт кафедри криміналістики та судової медицини
Національна академія внутрішніх справ

ІНТЕГРОВАНА ІНФОРМАЦІЙНО-ПОШУКОВА СИСТЕМИ ОВС УКРАЇНИ ЯК ОСНОВА ЕФЕКТИВНОЇ ПРОТИДІЇ ЗЛОЧИННОСТІ

Новітні засоби зв'язку та системи комунікацій стирають кордони між країнами й націями. Цифрові технології принципово змінюють не тільки можливості зв'язку, але й технології обміну товарами, послугами, знаннями, управління виробничими, соціально-економічними й політичними процесами у житті колективів, регіонів та країн. Стає реальною ймовірність управління

суспільним розвитком у глобальному просторі [1, с. 1–2]. Сьогодні у деяких країнах, у тому числі й в Україні, вирішується низка завдань із підвищення ефективності та якості діяльності всіх ланок державного управління за допомогою сучасних інформаційних технологій, зокрема, діяльності правоохоронних органів. Так, за допомогою використання Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України у 2013 році безпосередньо розкрито працівниками оперативних підрозділів 33,5 тис. (або 12,7%), слідчих підрозділів 1,9 тис. (або 0,7%), інших підрозділів 20,3 тис. (або 7,7%) кримінальних правопорушень. У 2014 році розкрито працівниками оперативних підрозділів 29,3 тис. (або 13,2%), слідчих підрозділів 1,0 тис. (або 0,5%), інших підрозділів 18,8 тис. (або 8,5%) кримінальних правопорушень.

Профілактика, розкриття та розслідування кримінальних правопорушень та інші завдання, які вирішують правоохоронні органи, потребують вдосконалення криміналістичної техніки й методів на основі сучасних досягнень науки і практики, розроблення та впровадження комп'ютеризованих систем, або, за вдалим висловом М. Я. Швеця, застосування інформаційного, програмного та комп'ютерного озброєння працівника правоохоронних органів [2, с. 5]. Водночас, окрім зазначеного вище «комп'ютерного розвитку» правоохоронних органів, відбувається також якісна зміна злочинного світу: у своїй протиправній діяльності кримінальні структури активно використовують сучасні досягнення науки і техніки, комп'ютерні системи та новітні інформаційні технології. Тому сучасний правоохоронець має володіти знаннями на такому рівні, який би надавав йому можливість орієнтуватись у сукупності інформаційних систем незалежно від їх цільового призначення та відомчої належності, щоб за необхідності отримати інформацію, яка сприятиме вирішенню питань кримінального провадження [3].

В цьому аспекті не аби яку роль відіграють досягнення в сфері інформаційно-аналітичного забезпечення службової діяльності ОВС,

висвітлення яких має стати запорукою ефективного розслідування кримінальних правопорушень.

Так, фахівцями Департаменту інформаційно-аналітичного забезпечення МВС України здійснено заходи щодо розроблення і введення в експлуатацію інформаційних підсистем. Їх можливості використання зазначені у методичних рекомендаціях щодо алгоритму дій користувачів з організації формування Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України [4]. Зокрема у розділах надано опис інформаційних підсистем:

-«Єдиний облік» – містяться відомості щодо заяв і повідомлень про вчинені кримінальні правопорушення та інших подій, викладених у заявах (повідомленнях, рапортах) та зареєстрованих у черговій частині ОВС;

- «Доставлені до ЧЧ ОВС» – обліковуються відомості про випадки затримання осіб працівниками ОВС, а також інформація про надання затриманим особам безоплатної вторинної правової допомоги;

- «Злочин» – містяться відомості про нерозкриті кримінальні правопорушення, учинені на території обслуговування ОВС;

-«Особа» – обліковуються особи, які вчинили правопорушення та щодо яких здійснюється профілактична робота працівниками ОВС;

-«Розшук» – містятьсявідомості про осіб, які переховуються від органів влади, ухиляються від відбування покарання, зникли безвісти;

-«Пізнання» – обліковуються відомості про безвісно зниклих осіб, невпізнані трупи, осіб, які не можуть надати про себе відомості в силу хвороби або малолітнього віку, та інших категорій осіб, що розшукуються;

-«Угон» – містятьсяданіпро транспортні засоби, що розшукуються, про виявлені безгосподарні (у тому числі – викрадені та втрачені державні номерні знаки транспортних засобів);

-«Викрадені (втрачені) документи» – містяться відомості про викрадені, втрачені документи (бланки документів), паспортні документи померлих громадян України, не зданих до органів ДМС, паспортні документи, визнані

недійсними, паспортні документи осіб, які знаходяться у розшуку, та які мають індивідуальні заводські (фабричні) номери;

-«Річ»– містяться відомості про викрадені, вилучені з ознаками підробки, заборонені або обмежені в обігу у громадян і службових осіб, безгосподарні, що знайдено або вилучено з камер схову вокзалів, портів, аеропортів та зданих до ОВС речі, у тому числі – мобільні телефони;

- «Антикваріат» – містяться відомості про викрадені, вилучені культурні цінності, що належать до об'єктів матеріальної і духовної культури та мають художнє, історичне, етнографічне та наукове значення;

-«Кримінальна зброя» – обліковуються відомості про зброю, викрадену, втрачену, знайдену, здану до ОВС, вилучену працівниками ОВС із числа тієї, що незаконно зберігалася, яка має індивідуальні заводські (фабричні) номери або номери деталей;

-«Зареєстрована зброя»– містяться відомості про зброю, яка має індивідуальні заводські (фабричні) номери, перебуває у користуванні громадян, підприємств, установ, організацій, господарських об'єднань, яким надано відповідно до законодавства дозвіл на її придбання, зберігання, носіння, перевезення, та яка обліковується підрозділами дозвільної системи ОВС;

-«Адміністративне правопорушення» – обліковуються відомості про зареєстровані в ОВС адміністративні правопорушення, за матеріалами яких уповноваженими на те працівниками ОВС складено протоколи про адміністративні правопорушення;

-«Мігрант» – обліковуються відомості про іноземців та осіб без громадянства, які порушили встановлені законодавством правила в'їзду, виїзду, перебування в Україні і транзитного проїзду через її територію, а також громадян України, які порушили встановлені законодавством правила в'їзду іноземців та осіб без громадянства в Україну, їх виїзду з України і транзитного проїзду через її територію;

-«Корупція» – обліковуються відомості про зареєстровані кримінальні та адміністративні корупційні правопорушення, осіб, які їх учинили, та результати розгляду цих правопорушень у судах;

-«Кримінальна статистика» – обліковуються відомості про кримінальні правопорушення, осіб, які їх учинили або підозрюються в їх учиненні, досудове розслідування за якими здійснюється слідчими ОВС;

-«ЄДРПОУ» – містяться відомості про юридичних осіб всіх форм власності та форм господарювання, відокремлені підрозділи юридичних осіб, що знаходяться на території України, а також відокремлені підрозділи юридичних осіб України, що знаходяться за її межами;

- «Домашній арешт» – містяться відомості про осіб, щодо яких ОВС України здійснюється виконання ухвал слідчого судді, суду про обрання запобіжного заходу у вигляді домашнього арешту та про зміну раніше обраного запобіжного заходу на запобіжний захід у вигляді домашнього арешту та щодо яких працівниками ОВС здійснюється контроль за їх поведінкою;

Крім цього, розроблено програмне забезпечення та методичні рекомендації щодо порядку роботи з електронною карткою обліку доручень на проведення слідчих (розшукових) дій для інформаційної підсистеми «Слідство: доручення» – обліковуються відомості про надання та виконання доручень слідчих щодо проведення слідчих (розшукових) дій за розпочатими кримінальними провадженнями, яка функціонує з 1 січня 2015 року [5].

Автор сподівається, що представлений комплекс інформаційних систем знайде зацікавленість серед науковців та практичних працівників. Це сприятиме їх подальшому розвитку та вдосконаленню сучасних форм і криміналістичних методів протидії злочинності.

Список використаних джерел:

1. Арістова І. В. Управління інформаційними ресурсами органів внутрішніх справ України : організаційно-правовий аспект : [навчальний посібник] / І. В. Арістова, О. В. Сировой. – Харків, 2005. – С. 1–2.

2. Швець М. Я. Загальні концептуальні засади інформаційно-комп’ютерного озброєння ОВС / М. Я. Швець // Правова інформатика. – 2006. – № 4 (12). – С. 5–16.

3. Хахановський В. Г. Проблеми теорії і практики криміналістичної інформатики : монографія / В. Г. Хахановський. – К. : Вид. Дім „Аванпост-Прим”, 2010. – 382 с.

4. Методичні рекомендації щодо алгоритму дій користувачів з організації формування Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України: від 16.01.2014 № 727/3р.

5. Доручення МВС України «Про організацію обліку доручень слідчих щодо проведення слідчих (розшукових) дій»: від 03.12.2014 №25621/Ск.

УДК 65.012.8 + 004

МИКОЛА МИЛЕНТІЙОВИЧ ЗАЦЕРКЛЯНИЙ
Доктор технічних наук, професор, професор кафедри інформаційної та економічної безпеки навчально-наукового інституту підготовки фахівців для підрозділів кримінальної міліції Харківського національного університету внутрішніх справ

ВОЛОДИМИР МИХАЛОВИЧ СТРУКОВ
Кандидат технічних наук, доцент, завідувач кафедри інформаційних технологій та захисту інформації факультету права та масових комунікацій Харківського національного університету внутрішніх справ

ЩОДО ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ БОРОТЬБИ З КІБЕРЗЛОЧИНАМИ

Комп'ютерна інформація, що є об'єктом чи засобом вчинення комп'ютерного злочину, хоча і призначена для звичайних людей, може досліджуватися тільки відповідними фахівцями. Практично будь-яка робота з комп'ютерною інформацією вимагає спеціальних знань. А джерелом таких знань може бути тільки фахівець із комп’ютерної криміналістики.

Встановлювати факти, що стосуються комп'ютерної інформації, можна тільки на підставі відповідних досліджень.

Нетямущим людям може здатися, що багато дій над комп'ютерною інформацією не вимагають спеціальних знань. Дійсно, сучасні комп'ютери, програмне забезпечення призначені для широкого кола користувачів. І користувачі (в тому числі малокваліфіковані) успішно виконують звичайні завдання, такі як редагування текстів, відправлення та одержання електронної пошти, створення і друкування малюнків. Навіщо ж тут спеціальні знання?

Аби знайти відповідь на це запитання, згадаємо історію розвитку обчислювальної техніки. У 1960-х роках для роботи на ЕОМ потрібно було мати не просто спеціальні знання, а й бути програмістом. Потім були створені програми для розв’язування деяких типових задач і навик програміста перестав бути обов'язковим. Але управління роботою ЕОМ як і раніше було недоступним для неспеціаліста. У 1980-х роках з'явилися перші персональні комп'ютери, навчитися працювати з якими могла людина зі звичайними знаннями. Навчання все ж було потрібно. І це обмежувало ринок збуту персональних комп'ютерів. Але програмне забезпечення стрімко розвивалося. І одним із головних напрямків його розвитку було забезпечення простого, наочного, звичного для некваліфікованого користувача інтерфейсу. Орієнтація на масового покупця - запорука успіху для комерційного програмного забезпечення. Деякі сучасні операційні системи роблять освоєння персонального комп'ютера досить простим завданням, оскільки зводять «багатовимірне» управління до вибору зі списку дій, а замість технічних термінів оперують менш адекватними, але більш звичними для простої людини аналогами: «документ» замість «файл», «папка» замість «каталог», «відправлення повідомлення» замість «встановлення SMTP-сесії» тощо. Багато операцій автоматизовані за рахунок зниження функціональності. Чимало інших операції приховані від користувача. Все це стало можливим завдяки розвитку програмного забезпечення. Біти в

сучасних комп'ютерах точно такі ж, як і 40 років тому. І набір арифметично-логічних операцій процесора мало змінився. Удавана простота - це не більше як підняття користувача на більш високий рівень абстрагування від технічної реалізації операцій. Таке підняття зовсім не означає розуміння. Навпаки, простота управління досягається за рахунок зниження розуміння суті виконуваних дій.

Для користування сучасним комп'ютером спеціальні знання дійсно не потрібні. Це відбувається завдяки високому відчуження користувача від технічної реалізації обробки інформації. Між «верхнім шаром», тобто графічним інтерфейсом користувача, і «нижнім шаром», тобто бітовими масивами даних, лежить багато проміжних «шарів» із форматів, протоколів, драйверів, API, системних функцій і прикладних програм. Зокрема, такі рівні взаємодії між двома комп’ютерами описує семирівнева модель взаємодії відкритих систем – OSI (Open System Interconnection), розроблена в 1984 році Міжнародною організацією зі стандартизації (International Organization of Standardization - ISO).

На кожному з таких рівнів («шарів») залишаються сліди. Кожний «шар» вносить свою лепту у зміну комп'ютерної інформації, в утворення цифрових слідів. Для пошуку та вивчення цих слідів потрібні спеціальні знання.

Спеціаліст із комп’ютерної криміналістики покликаний дати висновок і роз'яснити питання. Те й інше передбачає пояснення неспеціалістам фактів і обставин із галузі спеціальних знань. Але чи завжди можливе таке пояснення?

Воно можливе лише тоді, коли якийсь процес незрозумілий без спеціальних знань, але його висновки знаходяться в знайомій області. Наприклад, неспеціаліст може не розуміти, що таке відбитки пальців і як їх знімають. Але висновок - людина дотикалася пальцями предмета - зрозумілий будь-кому. Неспеціаліст не може собі уявити, як працює транзистор. Але як користуватися радіозривачем - тут натиснув, там вибухнуло - це зрозуміло.

У галузі інформаційних технологій зустрічаються ситуації, коли не тільки механізм і процес лежать в області спеціальних знань, а там же знаходяться і висновки. Тому буває так, що спеціаліст із комп’ютерної криміналістики не може пояснити простими словами не тільки чому, а й те, що, власне, сталося.

Наприклад, візьмемо таке злодіяння, як втручання в процес показу рекламних банерів. Спеціаліст навряд чи зможе роз'яснити суду механізм підміни адреси банерного сервера через DNS-записи. А наслідки цього діяння - користувачі побачать на веб-сторінках рекламу, вміщену туди без їх бажання і без прямої санкції власника веб-сторінки замість іншої реклами, яка теж була розміщена там же без бажання користувачів і без прямої санкції власника веб-сторінки - все знаходяться у віртуальному світі і не може бути роз'ясненим без попереднього роз'яснення всіх складних взаємовідносин між учасниками інформаційного обміну.

Роз'яснюючи питання, які потребують спеціальних знань, спеціаліст із комп’ютерної криміналістики фактично займається перекладом з однієї мови на іншу. Для цього він повинен досконало володіти обома мовами. Спроби перекласти з технічної на юридичну часто наштовхуються на таку перешкоду: в іншій мові не існує відповідного терміна. Та що там терміна! Відповідного поняття не існує.

Аби правильно сформулювати запитання до експертизи, потрібно знати більшу частину відповіді. І розбиратися в термінології. А щоб знати спеціальні терміни, потрібно уявляти, що вони означають. Тобто, треба самому володіти спеціальними знаннями в галузі інформаційних технологій.

Коли сліди вчиненого злочину та можливі докази знаходяться в цифровій формі (у формі комп'ютерної інформації), їх одержання, фіксація та документування мають певну складність.

На відміну від багатьох інших видів доказів, комп'ютерна інформація не може сприйматися людиною безпосередньо - очима, вухами, пальцями. Сприймати її можна тільки через посередництво технічних, апаратних і

програмних засобів. Причому кількість і складність цих посередників настільки велика, що зв'язок між початковою інформацією і тим, що бачимо не екрані, далеко не завжди очевидний. А часом цей зв'язок і зовсім умовний і хисткий до неможливості.

Варто визнати, що огляд комп'ютерної інформації - це не огляд (від слова «дивитися»), а скоріше інструментальна перевірка, яка вимагає певних знань про використовувані технічні засоби, принцип дії яких не завжди очевидний. Ймовірність помилитися і побачити не те, що є насправді, при цьому підвищена, навіть за відсутності цілеспрямованого впливу противника.

Одне з найважливіших завдань на етапі розслідування злочинів полягає у вивченні такого елементу їх криміналістичної характеристики, як механізм слідоутворення, характерний для певного виду або групи злочинних посягань. Тут маються на увазі відомості про локалізацію слідів, їх ознаки, види, збереження та інші дані, які дозволяють більш ефективно вести пошук і працювати з ними.

Під слідом у комп'ютерних інформаційних системах розуміється результат взаємодії об'єктів інформаційного середовища (програм і елементів файлової системи), який вказує на зміну стану складових інформаційної системи в результаті функціонування в ній програмних продуктів.

Цілком певні об'єкти активного програмного забезпечення комп'ютерної системи при реалізації інформаційних процесів залишають цілком певні сліди, тобто конкретну інформацію в строго певних областях файлової системи.

Тому при встановленні і розслідуванні кіберзлочинів варто виявляти:

1) сліди, що залишаються штатними програмними засобами:

• системними програмами (компонентами і службами операційної системи (наприклад, для операційної системи Windows, служби управління об'єктами, журналювання, служби мережевого трафіку і маршрутизації, антивірусного захисту, файлова система, тощо); інсталяторами; драйверами

реальних пристроїв і їх емуляторами; серверами; утилітами обслуговування; мережевими сканерами; програмами шифрування тощо);

• прикладними програмами (редакторами; мережевими клієнтами; прикладними компонентами СУБД; конструкторами; програмами-перекладачами тощо);

• інструментальним програмним забезпеченням (трансляторами; конверторами, налагоджувачами і трасерами; дизасемблерами; шістнадцятирічними редакторами тощо);

2) сліди, що залишаються шкідливими програмами, об'єктами впливу яких є файлова система, оперативна пам'ять, конкретні файли, мережевий інтерфейс тощо.

При цьому важливим є розташування слідів на носіях у термінах структур файлової системи за їх ієрархією:

1) сліди у кластерах (розподілених під актуальні файли, розподілених під вилучені файли, зарезервованих, втрачених, у зазорах кластерів);

2) сліди в керуючих і описуючих структурах файлової системи (таблицях розділів, завантажувальних секторах, резервних областях, областях свопінгу, таблицях розміщення файлів, каталогах);

3) сліди у файлах:

• виконуваних модулях (компілятора; побудовника завдань (що використовує бібліотеки для конкретної операційної системи); програмного забезпечення, використовуваного для редагування вже створених виконуваних модулів (зміна кількості і змісту програмних секцій, зміна точок входу, додавання і модифікація коду));

• даних (ініціюючих початковий стан програми (налаштування); які є реєстраційними даними роботи програм (журнали); службових для організації призначеного для користувача інтерфейсу (файли-посилання); службових для організації програмного інтерфейсу (файли-канали, файли свопінгу і спулінгу); що містять документи користувачів; що містять системні таблиці тощо);

4) сліди під позакластерними структурами (на ділянках накопичувача, не розподілених під розділи і не описаних у поточній таблиці розділів).

Із вищесказаного випливає, що для успішної боротьби із кіберзлочинами недостатньо спеціалістів із відповідними юридичними знаннями, доповнених основами інформатики. Потрібні також спеціалісти, які мають глибокі знання з інформаційних і комунікаційних технологій, доповнених певними юридичними знаннями. Зрозуміло, що «ціна» такого інтегрованого спеціаліста на ринку праці (в тому числі міжнародному) зовсім «немаленька», особливо в організаціях, в яких заробітна платня сплачується у доларовому еквіваленті. І вона дуже (м'яко кажучі) відрізняється від заробітної платні, яку зараз можуть запропонувати бюджетні установи. Чи можна такого фахівця «з нуля» підготувати за 3, 6 або навіть 9 місяців? З нашої точки зору це неможливо. Який вихід у держави в сучасних умовах скрутного фінансування? Як можливий організаційно підготовлений варіант - таких спеціалістів можна готувати в рамках напрямку "Комп'ютерні науки" (в рамках відповідної спеціалізації), на який у 2011 році в ХНУВС призупинено набір, хоча ліцензія і акредитація за 4 рівнем чинні до 2019 року. Можливо у комбінованому варіанті – двох етапна підготовка – на першому етапі навчання за кошти кандидатів, а на другому – за кошти держави (або навпаки), залежно від кваліфікаційних вимог. Як підтверджено європейськими експертами (Любан Петрович) навчальні плани саме цієї спеціальності (з числа тих, на які ХНУВС має ліцензію) в найбільшій мірі відповідають вимогам до фахівців з боротьби з кіберзлочинами.

УДК 343.9
ДМИТРИЙ ЮРЬЕВИЧ УЗЛОВ
К.т.н., начальник Управления информационно-аналитического обеспечения ГУМВД Украины в Харьковской области, полковник милиции
АЛЕКСЕЙ ВЯЧЕСЛАВОВИЧ ВЛАСОВ
Заместитель начальника Управления информационно-аналитического обеспечения ГУМВД Украины в Харьковской области, подполковник милиции
АРТЕМ ИВАНОВИЧ ПЕТРУСЕНКО
Старший инженер программист управления информационно-аналитического обеспечения ГУ МВД Украины в Харьковской области, старший лейтенант милиции
СТАНИСЛАВ НИКОЛАЕВИЧ ДОСКАЛЕНКО
Инженер-программист Управления информационно-аналитического обеспечения ГУМВД Украины в Харьковской области, лейтенант милиции

КРИМИНОЛОГИЧЕСКИЙ АНАЛИЗ: РЕШЕНИЯ НА ОСНОВЕ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ

Любые данные, содержащие информацию о местоположении, могут быть отображены и проанализированы с помощью географической информационной системы (ГИС). Любая ГИС является неотъемлемой частью аналитического инструментария в работе по созданию необходимой информации для исполнителей. Объединив традиционные данные органов внутренних дел с иными значимыми информационными источниками (такими, как, например, данные о демографической или экономической ситуации в регионе), вы можете использовать ГИС для оперативного преобразования информации в своевременные управленческие решения. Тем самым, вы можете существенно улучшить реагирование подразделений на сообщения о событиях в быстро меняющемся окружении и, следовательно, повысить безопасность не только сотрудников, но и простых граждан.

Применение ГИС при анализе преступности.

Каждое преступление связано с какими-либо конкретными местами, такими, как дом, улица, почтовый индекс или целый район. ГИС может

помочь Вам усилить территориальный аспект ваших исходных данных, чтобы понять и решить проблему более эффективно.

Геоинформационные системы помогают в криминологическом анализе следующим образом:

• Выявление и маркировка подозрительных событий, содержащих признаки правонарушений, позволяет визуализировать латентную преступность;

• Поддержка принятия управленческих решений и анализ тенденций в смежных правоохранительных областях путем визуализации разнородных данных в едином пространстве;

• Уменьшение уровня преступности за счет реализации правоохранительных методов различных подразделений;

• Обратная связь с населением для более эффективного расследования преступлений и интеграция общества в правоохранительную деятельность за счет наглядности и мультиплатформенности приложений;

• Использование различных инструментов и методов для выявления серийности преступлений и прогнозирования развития ситуации.

Стратегический анализ преступности.

Правоохранительные органы, как правило, весьма ограничены в ресурсах. ГИС может помочь вам более эффективно управлять ими и повысить качество работы подразделений в целом. Выявляя скопления проблем, ГИС также обеспечивает визуализацию целых направлений или конкретных задач в борьбе с преступностью, а также эффективность обратной связи с населением, при реализации программы строительства безопасного общества.

ГИС может помочь Вам:

• В понимании картины событий, основанной на динамике в регионе в целом и по различным составляющим: лицам, событиям и иным криминогенным факторам;

• В определении факторов риска, состоящих из бизнес-схем, зданий и сооружений либо иных объектов, благоприятствующих преступлениям;

• В быстром управлении силами и средствами при перераспределении ресурсов, после анализа криминальных тенденций;

• В планировании специальных операций при отработке региона либо сезонных всплесках правонарушений;

• В обработке и фильтрации потока повторяющихся вызовов и запросов на использование сил и средств.

Сотрудники, работающие с населением, или следователи, работающие над событиями, как правило, сами прекрасно знают, где чаще всего происходят преступления. В дополнение к этим знаниям, визуализация ситуации на временных отрезках может помочь сотрудникам более эффективно анализировать происходящие в криминальной среде события, выявлять схемы и закономерности.

Использование ГИС также позволяет найти ответ на различные неочевидные вопросы. Например, могут ли определенные виды преступлений состоять в зависимости от времени суток или дня недели? Являются ли общедоступные, неконтролируемые места привлекательными для преступников? Как криминальный аналитик, вы можете оказать существенную помощь сотрудникам оперативных и следственных подразделений путем разработки более эффективных тактических подходов и методов расследования и, в конечном счете, предотвращения преступлений.

Используя ГИС, вы также можете моделировать логику своего рабочего процесса и сохранять ваши лучшие наработки. Это позволяет оценивать работоспособность теорий, а также делиться опытом с другими сотрудниками. Вы можете получать знания и опыт из сотрудничества с

патрульными, следователями, оперативными работниками или другими аналитиками.

Картографирование – естественный способ организации информации в правоохранительных органах. Вы можете использовать отображение динамики различных видов правонарушений, чтобы наглядно демонстрировать результаты работы вашего подразделения. Временной и пространственный анализ с помощью ГИС может помочь вам визуализировать процесс реализации отдельных пунктов Стратегии деятельности госорганов в правоохранительной сфере, обеспечивать общую оперативную картину для руководства во время совещаний и реализовывать контакт с населением через интерактивные средства обмена информацией. Средства ГИС предоставляют преимущества во всех аспектах деятельности правоохранительных органов.

Оперативные возможности использования ГИС.

Каждый день оперативные подразделения, патрульные и следователи обращаются к аналитикам за результатами анализа криминогенной обстановки. Простые граждане постоянно обращаются в службу оперативного реагирования для принятия мер по предотвращению и предупреждению преступлений.

ГИС предоставляет возможность обрабатывать подобные запросы путем оперативного отображения преступности и предоставляет платформу для:

• анализа криминальной информации, который позволяет выявлять закономерности и серийность явлений;

• наглядно связать элементы состава преступления и конкретное место совершения;

• создания и отработки следственных версий путем объединения данных из нескольких источников;

• прогнозирования потенциальных мест концентрации преступности на основе пространственных инструменты и методов;

• аналитического сопровождения планов операций и уточнения идеальных мест развертывания;

• отсеивания ошибочных информаций путем привязывания подозреваемых к конкретным преступлениям, после их задержания;

• непрерывного мониторинга мест повышенного риска и профилактики ранее судимых.

Результаты аналитической работы ГИС:

• *выявление серийности и закономерностей*: используя ГИС, вы можете создать карту, которая отобразит не только места совершения преступлений, но и показать, на основе ваших исследований, все связанные с ними события. Это позволит усилиям более полно осведомленных следователей и патрульных не пропадать впустую, за счет оптимизации маршрутов, реагированию на местах и отработке наиболее вероятных версий событий;

• *наблюдение и оперативные планы*: преступники часто совершают преступления несколько раз. ГИС может помочь вам точно смоделировать шаблон и поведение нарушителя, определить вероятные маршруты и идеальные места для наблюдения;

• о*тработка версий*: вы можете визуально анализировать свои данные, чтобы отрабатывать алиби или уточнять, был ли подозреваемый в непосредственной близости от места преступления. ГИС обрабатывает связанные данные из различных источников, предоставляя сложную интегрированную платформу пространственно-временного анализа.

ГИС предоставляет методы и инструменты, работающие с информацией, поддерживающий все задачи и аспекты правоохранительных органов:

• *патрульный или следователь*: сотрудники правоохранительных органов в ходе своей работы могут оперативно получить доступ к текущему анализу преступности и иной криминально значимой информации. Возможность выполнять пространственные запросы, анализировать и визуализировать их результаты, предоставляет быстрый и интуитивно понятный интерфейс.

• *Руководящий состав*: руководство может использовать ГИС для понимания обобщенных тенденций, быстро принимать важные решения в периоды всплесков преступности и сотрудничать с другими государственными органами для эффективного распределения сил и средств в нужном месте и в нужное время.

• *Криминальный аналитик: к*риминальный аналитик может использовать более сложные инструменты и методы, чтобы обеспечить командно-штабные подразделения полным пакетом данных, для лучшей поддержки оперативных планов и решений тактического и стратегического характера.

УДК 343.9
АЛЕКСЕЙ ВЯЧЕСЛАВОВИЧ ВЛАСОВ
Заместитель начальника Управления информационно-аналитического обеспечения ГУМВД Украины в Харьковской области, подполковник милиции
АЛЕКСЕЙ БОРИСОВИЧ ГРИГОРОВИЧ
Начальник отдела Управления информационно-аналитического обеспечения ГУ МВД Украины в Харьковской области, капитан милиции
РУСЛАН ВАДИМОВИЧ БОРОВИК
Главный специалист Управления информационно-аналитического обеспечения ГУМВД Украины в Харьковской области, старший лейтенант милиции
АЛЕКСАНДР АЛЕКСАНДРОВИЧ ТАРАСЕНКО
Инспектор Управления информационно-аналитического обеспечения ГУМВД Украины в Харьковской области, лейтенант милиции

ДУБЛИРОВАНИЕ УСТАНОВОЧНЫХ ДАННЫХ И МЕТОДЫ ИХ ИНТЕГРАЦИИ В ЕДИНОЕ ИНФОРМАЦИОННОЕ ПРОСТРАНСТВО

В настоящее время нет единого принятого и стандартизованного способа идентификации лиц, документов, номерных вещей и других объектов криминологического учета, несмотря на то, что в последние годы введено в действие немалое число автоматизированных систем. Проблема идентификации становится особенно актуальной при использовании одной и той же информации в различных базах данных, когда необходимо проводить комплексную обработку данных с дальнейшей интеграцией полученных результатов. Необходимость единых идентификаторов за пределами одной системы является глобальным требованием. Различные инициативы построения идентификаторов и систем регулярно появляются в процессе нормативной и технической деятельности Министерства, однако, они пока так и не достигли необходимой степени интероперабельности.

Для упрощения обмена информацией в информационных системах и базах данных органов внутренних дел (БД) принято использовать уникальные числовые идентификаторы (ID) для различных информационных объектов внутри системы, позволяющие легко их отыскивать.

Внутрисистемные идентификаторы хорошо работают в рамках системы для определения и накопления информации об объектах. Поскольку криминологическая информация становится более открытой и доступной для сотрудников, релевантные информационные объекты повторяются во множестве систем, поддерживающих совместно используемые описания. Так, например, в каждой из этих систем один и тот же человек, наиболее вероятно, будет иметь свой внутрисистемный идентификатор, и в каждой системе описания имени могут иметь орфографические варианты записей в другом написании. Необходимы механизмы управления идентичностью для обеспечения эффективного управления различными идентификаторами немашинным способом.

К примеру, в момент внесения новой порции данных из подсистемы единого учета происшествий в центральную базу данных Интегрированной информационно-поисковой системы ОВД (ИИПС), в ней уже могут присутствовать записи, относящиеся к физическому лицу, запись о котором присутствует в загружаемом массиве данных. Это может быть запись с измененными данными о заявителе из того же района или новая запись, при подаче заявления в другой орган. При загрузке таких записей в центральной системе должен осуществляться анализ таких записей с целью принятия решения об их принадлежности одному и тому же лицу. Отсутствие в системе проверки общесистемных уникальных идентификаторов приводит к тому, что идентификацию записей приходится осуществлять путем сравнения значений определенного набора ключевых полей этих записей. В реальной ситуации задача выбора такого набора ключевых полей, и сама процедура принятия решений по сравнению значений этих полей о принадлежности или не принадлежности двух записей одному лицу оказывается очень непростой. Главные причины этого состоят в следующем:

1. Объективная неизбежность возникновения ошибок в значениях ключевых атрибутов записей о лице, возникающих при ручном вводе первичных данных операторами.

2. Недостаточная идентификационная способность традиционных идентификаторов личности. Например, результаты обработки данных о заявителях в ИИПС показали реальность существования у разных лиц одинаковых значений серии и номера паспорта (главного документа, удостоверяющего личность). Нельзя, также, исключать случаи предъявления заявителем при подаче документов в разные райотделы разных документов, удостоверяющих его личность.

3. Отсутствие в ИИПС возможности сверки электронных данных с их первичным документальным источником.

При принятии решения по результатам сравнения значений ключевых полей персональных записей возможны ошибки следующих двух видов.

• Ошибка первого рода - принятие решения о принадлежности записей разным личностям, не смотря на их фактическую принадлежность одному лицу.

• Ошибка второго рода - принятие решения о принадлежности записей одному лицу, в то время как на самом деле они представляют две разные личности.

Последствием этой ошибки будет то, что в базе ИИПС будут объединены данные записей, относящихся к разным личностям, или данные записи одной личности будут замещены данными записи, принадлежащей другой персоне. Результат - *невосстановимые* искажения или потеря данных, что делает цену такой ошибки очень высокой.

Снижение вероятности возникновения рассматриваемого вида ошибки возможно при соответствующем выборе набора ключевых полей. В связи с тем, что, как показала практика, в нашем распоряжении нет одного надежного общесистемного идентификатора личности, ключ для идентификации должен быть *составным*, т.е. представлять собой *набор* полей, например, помимо серии и номера паспорта, содержать поля ФИО, номер идентификацинного кода налоговой или какие-либо еще. Совершенно ясно, однако, что при возможном наличии в загружаемых

данных значений ключевых полей с ошибками, совершенными при их вводе, увеличение числа сравниваемых ключевых полей будет осложнять обнаружение записей, принадлежащих одной личности, увеличивая вероятность ошибок первого рода. Понятно, также, что увеличение числа ключевых полей и увеличение среди них доли вводимых вручную текстовых полей, будет приводить к увеличению вероятности несовпадения значений этих полей у записей, принадлежащих одной личности, из-за возможных ошибок при вводе этих значений.

Однако, меры по минимизации воздействия для одного типа ошибки, приводят к увеличению вероятности другого вида ошибок. Так, увеличение количества ключевых полей снижает вероятность ошибки второго рода, то есть *ложной идентификации*, но увеличивает вероятность ошибки первого рода - *отсутствия идентификации*.

Решение проблемы, можно получить при сочетании расширеного набора ключевых полей и использовании процедуры принятия решения, в которой, кроме принимаемых с необходимой степенью уверенности решений вида - "записи представляют *одну* личность" или "записи представляют *разные* личности", в случаях, когда степень этой уверенности оказывается недостаточной, принимается решение о проведении дополнительного, более детального анализа значений полей сравниваемых персональных записей.

Возможность уточнения принимаемого при идентификации записей решения путем дополнительного анализа значений сравниваемых ключевых полей основывается на том, что при искажении значений полей из-за ошибок ввода, хотя и нарушается точное совпадение значений этих полей, тем не менее, сохраняется определенная их близость ("похожесть"), позволяющая в ряде случаев даже при неполном совпадении значений ключевых полей делать вывод о принадлежности записей одной личности. Например, если у двух записей поля значения полей **серия_номер_паспорта, дата_рождения** и **фамилия** совпали, а значение поля **имя** не совпало, но отличается в одном символе, можно с очень большой степенью уверенности отнести эти записи к

одной личности, считая, что значения поля имя различаются в результате опечатки при вводе.

Для проверки предположения о том, что причиной несовпадения значений сравниваемых полей, представляющих одного и того же лица, являются ошибки ввода, производится сравнение значений "подозрительных" полей по более сложному алгоритму, учитывающему лингвистическую близость (похожесть) сравниваемых значений полей. Для определения лингвистической похожести зна-чений полей может быть использован так называемый алгоритм Левенштейна, в котором мерой разницы двух последовательностей символов (строк) является минимальное количество операций вставки, удаления и замены одиночных символов, необходимых для перевода одной строки в другую. Таким образом, если строки полностью совпадают, то дистанция Левенштейна равна нулю, если они отличаются одним символом, то единице, и т.д.

Все изложенное выше делает также исключительно важным рассмотрение мер, которые могли бы, хоть и не исключить совсем появление неоднозначно идентифицируемых записей, но, по крайней мере, минимизировать их количество. в частности, мер снижения ошибок при вводе первичных данных в автоматизированных системах.

УДК 65.012.8 + 004
ОЛЕКСАНДР ВОЛОДИМИРОВИЧ МАНЖАЙ
Кандидат юридичних наук, доцент, доцент кафедри захисту інформації факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ ЛЕГЕНДОВАНИХ ПРОФІЛІВ КОРИСТУВАЧІВ ПРАВООХОРОННИМИ ОРГАНАМИ ВЕЛИКОБРИТАНІЇ ТА США

Розвиток інформаційних технологій обумовлює удосконалення методів роботи правоохоронних органів. У цьому сенсі потрібно згадати таку новацію, як створення та застосування поліцейськими органами легендованих профілів в комп'ютерних мережах для виявлення, попередження та розслідування злочинів.

Так, у Великобританії створення легендованого профілю соціальної мережі не є спеціальним заходом, який потребує санкціонування. Для звичайних користувачів мережі Інтернет, створення вигаданих профілів утворює склад правопорушення, яке зазіхає на приватне життя, передбачене Законом «Про незаконне використання комп'ютера», оскільки особа отримує доступ до відомостей інших осіб та вводить в оману інших користувачів. «Ловля на живця» не є правопорушенням, якщо захід проводиться у зв'язку із санкціонованими слідчими діями (обшук, огляд, виїмка) (ст. 10 Закону «Про незаконне використання комп'ютера»). З метою недопущення використання відомостей, одержаних з використанням легендованого профілю в особистих цілях, Законом «Про захист особистих даних» встановлюється відповідальність за одержання інформації, яка виходить за рамки заходу [1, с. 131].

Як відмічають автори монографії «Оперативно-розшукова компаративістика» [2, с. 279-280] у США працівники ФБР можуть видавати себе в комп'ютерних мережах за неповнолітніх, спілкуючись з педофілами, як це було, наприклад, у справі Патріка Нотона 1999 року. Як потім

з’ясувалося, протягом кількох місяців Патрік Нотон спілкувався з буцімто 13-річною дівчинкою, якій він запропонував зустрітися з метою «ближчого знайомства». Наразі ж під час проведення операції ФБР у місці призначення зустрічі Нотона було заарештовано та засуджено до 5 років випробувального терміну та 9 місяців домашнього арешту.

Проведення таких оперативних комбінацій шляхом використання кіберпростору у США має назву «*онлайнові секретні операції*» (online undercover operations). Строк проведення таких операцій встановлюється не більше 30 діб, але за необхідності його можна подовжити. Санкцію на їх проведення видає спеціальний агент, а за наявності певних «делікатних обставин» ця санкція погоджується зі Штаб-квартирою ФБР. Результати проведення такої операції фіксуються у відповідному звіті.

Під час проведення онлайнової секретної операції секретний співробітник зобов’язаний:

- робити точні записи всіх онлайнових комунікацій;
- уникати будь-якої незаконної діяльності;
- підтримувати онлайновий профіль (параметри користувача) по змозі в обмеженому вигляді, достатньому для досягнення мети операції;
- уникати фізичного контакту з фігурантами;
- робити всі необхідні дії протягом періоду операції для захисту потенційних жертв та попередження серйозної кримінальної діяльності, якщо під час онлайнового контакту з’ясується, що існує реальна серйозна загроза третім особам, комерційним організаціям або урядовим об’єктам;
- припинити секретну діяльність, якщо протягом 30 діб буде ухвалено рішення про припинення секретної операції.

Підсумовуючи, потрібно відмітити, що поступово у світі з’являються не лише адаптовані, але й низка цілком нових оперативно-розшукових заходів, зокрема «зняття інформації з електронних інформаційних систем». Починаючи з 1999 року, цей захід поступово знаходить своє відображення у законодавствах країн світу, наприклад, США (1999), Німеччина (2008),

Україна (2012). Гадаємо, що із розвитком інформаційних технологій поява нових оперативно-розшукових заходів є неминучою, а, відтак, українським правоохоронним органам потрібно їх своєчасно відслідковувати та намагатися імплементувати корисні новації до українського законодавства.

Список використаних джерел: **1.** Ташмагамбетов А. М. Оперативно-розыскные мероприятия с использованием социальных сетей: опыт Великобритании и Республики Казахстан / А. М. Ташмагамбетов // Наука и бизнес: пути развития. – 2013. – № 11 (29). – С. 129-133. **2.** Бандурка О. М. Оперативно-розшукова компаративістика: монографія / О. М. Бандурка, М. М. Перепелиця, О. В. Манжай та ін. – Х. : Золота миля, 2013. – 352 с.: іл.

УДК 004.056: 004.942: 343.1

ВІТАЛІЙ ВІКТОРОВИЧ НОСОВ
Кандидат технічних наук, доцент, професор кафедри захисту інформації факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми Харківського національного університету внутрішніх справ

ЗАСТОСУВАННЯ ПОНЯТТЯ "СЦЕНАРІЇ РИЗИКІВ" ДЛЯ СЗІ ОВС УКРАЇНИ У КОНТЕКСТІ СИСТЕМНОГО ПІДХОДУ COBIT®5

У базових державних стандартах із захисту інформації [1, 2, 3] та інших вітчизняних нормативно-методичних документах регламентується визначати та оцінювати для інформації, що захищається, окремі складові інформаційних ризиків: загрози, джерела загроз, ймовірність прояви загроз та очікувану шкоду від їх реалізації, окрему модель загроз. Ці оцінки використовуються при розробленні адекватної системи захисту інформації.

Якщо постулювати необхідність застосування системного мислення та системного підходу при створенні життєздатної системи захисту інформації [4], то представляється доцільним взяти до уваги підходи, що реалізовані у проекті COBIT®5, які є сукупністю взаємопов’язаних методологій та

стандартів в галузі управління, аудиту і IT безпеки, розроблених світовою спільнотою фахівців під егідою міжнародної асоціації ISACA (Information System Audit and Control Association, Асоціація з управління і аудиту інформаційної системи).

У методиці [5] бази знань COBIT®5, на відміну від [1, 2, 3], пропонується інтегрований підхід до розгляду складових інформаційних ризиків, де використовується поняття "сценарії ризиків", яке поєднує в собі усі відповідні складові і дозволяє системно виходити на основну мету IT безпеки - надання можливості організації виконувати свої функції (створення цінностей для зацікавлених сторін) при мінімізації ресурсних затрат і виникаючих супутніх IT ризиків (певне поєднання імовірності небажаних подій в IT із їх наслідками).

ОВС України, згідно [6], утворено з метою формування та реалізації державної політики у сфері захисту прав і свобод людини та громадянина, власності, інтересів суспільства і держави від злочинних посягань. Зацікавленими сторонами (на різних рівнях системи), для яких ОВС створює цінності, є людина, суспільство і держава. На інформаційні технології (IT) спирається уся діяльність ОВС, а значить загальні ризики для ОВС у значній мірі визначаються IT ризиками. IT ризики для ОВС можна поділити на дві категорії: (а) зупинка зростання підтримки цільової діяльності ОВС і (б) втрата вже досягнутого рівня IT підтримки цієї діяльності (рис. 1).

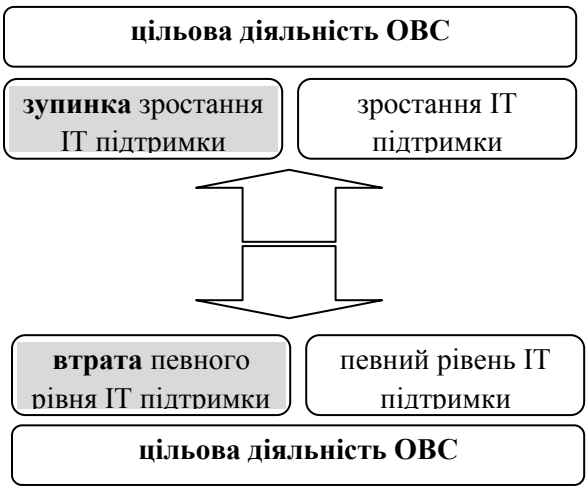


Рис. 1. Категорії IT ризиків ОВС

У рамках системи IT безпеки (системи захисту інформації) ОВС потрібні стратегічне керування (governance) та операційне управління (management) IT ризиками, які потребують створення відповідних структур

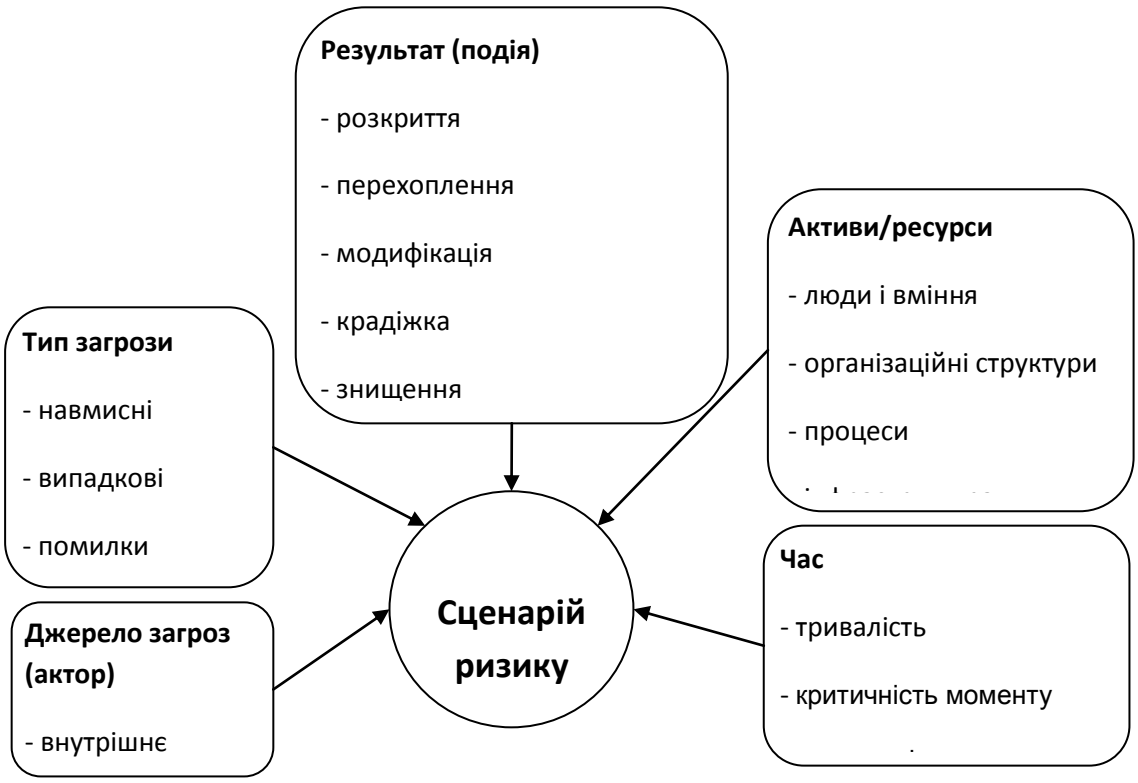


Рис. 2. Структура сценарію ризику

та процесів за методиками [7, 8].

Сценарії ризиків для ОВС повинні представляти собою опис імовірних подій, що можуть вплинути на процес захисту прав і свобод людини та громадянина, власності, інтересів суспільства і держави від злочинних посягань. Вплив імовірних подій може бути як позитивним, так і негативним. Структуру сценарію ризику можна представити як на рис. 2.

Сценарії ризиків можуть бути отримані двома різними шляхами (рис. 3).

- *зверху-вниз*, аналізувати задачі основної діяльності ОВС і визначати сценарії найбільш релевантних і імовірних ІТ ризиків, які впливають на виконання цих задач;
- *знизу-уверх,* виходити із відомого переліку типових сценаріїв ІТ ризиків, з якого вибирати найбільш релевантні та уточнювати їх у відповідності із особливостями конкретних ІТ різних підрозділів ОВС. Методика [5] містить потрібний перелік типових сценаріїв ІТ ризиків.

Таким чином, використання нового поняття "сценарії ризиків" у контексті системного підходу COBIT®5 при створенні життєздатної системи захисту інформації ОВС дозволить поставити процеси захисту інформації у залежність від процесів основної цільової діяльності ОВС.

Рис. 3. Шляхи отримання сценаріїв ризику

Список використаних джерел: **1**. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.96 р. № 423 - Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=38883&cat_id=38838. – Назва з екрана. **2.** ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Затверджено наказом Держстандарту України від 19.12.96 р. № 511. - Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=38911&cat_id=38836. – Назва з екрана. **3.** ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р. №200. - Режим доступу: http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?art_id=38934&cat_id=38836. – Назва з екрана. **4.** Носов В.В. Системний підхід у забезпеченні інформаційної безпеки / В.В. Носов // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2010. – № 1 (20). – С. 92-97. **5.** Risk Scenarios Using COBIT® 5 for Risk. ISACA. 2014. - Режим доступу: http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/risk-scenarios-using-cobit-5-for-

risk.aspx. – Назва з екрана. **6.** Указ Президента України "Про затвердження Положення про Міністерство внутрішніх справ України" від 6 квітня 2011 р. № 383/2011. - Режим доступу: http://zakon2.rada.gov.ua/laws/show/383/2011. – Назва з екрана. **7.** The Risk IT Framework. ISACA. 2009. - Режим доступу: http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework_fmk_Eng_0610.pdf. – Назва з екрана. **8.** The Risk IT Practitioner Guide. ISACA. 2009. - Режим доступу: http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Practitioner-Guide_res_Eng_0610.pdf. – Назва з екрана.

УДК 004.75

ІГОР ВОЛОДИМИРОВИЧ КОБЗЕВ
Кандидат технічних наук, доцент, доцент кафедри інформаційної та економічної безпеки Харківського національного університету внутрішніх справ
ОЛЕКСАНДР ЮРІЙОВИЧ ГОРЕЛОВ
Студент Харківського національного університету радіоелектроніки

ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ В НАВЧАЛЬНОМУ ПРОЦЕСІ

Хмарні обчислення - одна з провідних тенденцій світових інформаційних технологій. Концепція хмарних технологій полягає в розподіленій обробці даних, в якій додатки, комп'ютерні ресурси і потужності надаються користувачеві як Internet-сервіс. Під хмарою розуміють центр обробки даних із складною інфраструктурою.

Ідеї подібних технологій існували ще в 60-і роки минулого століття. Появу терміну «хмарні обчислення» (англ. cloud computing) відносять до 2006 року. В цей же час компанією Amazon був запущений один з перших проектів на базі хмарних технологій. Менш ніж за десять років після своєї появи хмарні обчислення знайшли застосування в самих різних галузях.

Користувачі багатьох Internet -сервісів можуть і не знать, що ці сервіси реалізовані на основі хмарних технологій (наприклад, пошта Gmail, пошукова система Google, банківські послуги, деякі ігри).

Застосування хмарних технологій в учбовому процесі стає усе більш популярним і відкриває багато можливостей як для освітніх установ, так і для викладачів і студентів.

Зараз реалізована безліч хмарних сервісів, які можуть бути використані в учбовому процесі. Хмарні сервіси Google Apps for Education і Microsoft Office 365 for education дозволяють використовувати електронну пошту, календарі для спільного планування і загальні адресні книги. Кожен користувач хмарних систем отримує значний дисковий простір для зберігання будь-якої інформації, яка була отримана в результаті роботи з хмарою.

Також існує можливість використовувати в хмарі функції стандартного офісного пакету для спільної роботи з електронними документами, таблицями і для створення презентацій.

Навчальні заклади, що підключилися до освітніх програм Microsoft Office 365, можуть на умовах підписки надавати безкоштовний доступ до сервісів для співробітників і студентів. Google Apps для викладачів, школярів і студентів надає сервіси безкоштовно у рамках вибраного освітньою установою домена. По даним на 2014 рік, Google Apps для навчальних закладів використовують більше 30 мільйонів студентів і викладачів [1]. За технологіями Microsoft Office 365 for education вчаться понад 110 мільйонів викладачів і студентів.

Хмарні сховища даних призначені для розміщення призначених для користувача даних будь-яких типів. Існує безліч платних і безкоштовних сховищ, що відрізняються об'ємом простору, що надається, і додатковими послугами (Dropbox, Google Drive, Mega, Яндекс.Диск, Copy.com та ін.). Практично скрізь доступні автоматична синхронізація даних, що зберігаються, між усіма підключеними до хмарного сервісу пристроями,

шифрування передаваних даних, можливість налаштування доступу до файлів, що зберігаються в хмарі, для інших осіб, забезпечення надійності зберігання.

Існують сервіси, що дозволяють створювати і налаштовувати програми безпосередньо на хмарі, використовуючи середовища багатьох мов програмування, що може бути використано при навчанні програмуванню.

Широко використовуються хмарні технології при побудові середовищ дистанційного навчання, створенні електронних бібліотек. Існує досить багато сервісів, за допомогою яких можна створювати електронні журнали, особисті кабінети для учнів і викладачів, інтерактивні приймальні, організовувати тематичні форуми, відеоконференції, проводити вебінари. Популярні хмарні системи для створення тестів, електронних підручників, повчальних програм і тренажерів.

Використання хмарних обчислень в області освіти має позитивні і негативні сторони. Дані, розміщені на хмарі, доступні з будь-якого місця, де є Internet, і з будь-якого пристрою. До того ж хмарна інфраструктура гарантує збереження даних.

Розміщення інформації і програмного забезпечення на хмарах дозволяє значно скоротити витрати на створення і обслуговування власних центрів обробки даних, закупівлю серверного і мережевого устаткування для створення власної IT-інфраструктури, що особливо актуально для навчальних закладів.

Хмарні сервіси, як правило, використовують новітні версії програмного забезпечення, що дозволяє йти в ногу з часом і готувати фахівців сучасного рівня. Підготовка студентів по деяких спеціальностях припускає використання програмного забезпечення, що вимагає значних обчислювальних ресурсів або дорогого устаткування, придбання якого не усі учбові заклади можуть собі дозволити. Хмарні сервіси дозволяють розмістити або узяти в оренду необхідне програмне забезпечення. Проте слід

врахувати, що для роботи з хмарними сервісами потрібний постійний і надійний широкосмуговий доступ в Internet.

Таким чином, в сучасній системі освіти хмарні обчислення можуть бути використані для забезпечення учбового процесу і при створенні ефективних інструментів організації науково-дослідної діяльності.

В рамках надання освітніх послуг в Харківському національному університетів хмарні технології доцільно використовувати в процессі проведення лабораторних робіт та практичних занять по дисциплінам блоку інформаційних та телекомунікаційних технологій.

Список використаних джерел

1. Protecting Students with Google Apps for Education. [Електронний ресурс]. Режим доступу URL: http://googleforwork.blogspot.com/2014/04/protecting-students-with-google-apps.html

2. By the Numbers: Microsoft's Impact on Education/ [Електронний ресурс]. Режим доступу URL: http://blogs.technet.com/b/microsoft_in_education/archive/2015/04/06/by-the-numbers-microsoft-39-s-impact-on-education.aspx

УДК 343.346.8
ВОЛОДИМИР ВОЛОДИМИРОВИЧ ТОРЯНИК
Кандидат фізико-математичних наук, доцент,
доцент кафедри інформаційних технологій та захисту інформації факультету права та масових комунікацій Харківського національного університету внутрішніх справ
АНТОН ЮРІЙОВИЧ ЧМИРЬ
Студент факультету права та масових комунікацій Харківського національного університету внутрішніх справ

УРАЗЛИВІСТЬ СУЧАСНИХ ТЕХНОЛОГІЙ РАДІОЧАСТОТНОЇ ІДЕНТИФІКАЦІЇ

Технічний аспект. Фізичним принципом функціонування систем радіочастотної ідентифікації (Radio Frequency IDentification - RFID) є явище відбиття і модуляції об'єктом- радіоміткою високочастотних електромагнітних хвиль, згенерованих джерелом-рідером. Перша радіочастотна ідентифікація здійснена британцями в 1939 р. у військових цілях. Основою комерційного вжитку технологій RFID є роботи Г.Стокмана «Комунікації за допомогою відбитого сигналу» (IRE, 1948 р.) та М.Кардулло «Пасивний радіопередавач з пам'яттю» (патент США, 1973 р.). Перша демонстрація RFID-чипів була проведена в Los Alamos Scientific Laboratory (США, 1973 р.) [1,2].

Переваги RFID-технологій полягають у тому, що ідентифікація відбувається на значній відстані та поза межами прямої видимості поміж антенами рідера та радіомітки. Таким чином, мітка може бути прихованою усередині об'єкту ідентифікації. Суттєво, що радіомітка може бути пасивною, тобто використовувати випромінювану рідером електромагнітну енергію для живлення власної мікросхеми-модулятора. За рахунок індукційного зв'язку антен рідер-мітка-рідер відповідна модуляція з'являється в антені рідера та ідентифікується.

Застосування RFID-технологій. Основними галузями застосування радіочастотної ідентифікації є системи управління та контролю доступом,

транспорт та логістика, системи інвентаризації, бібліотеки, медицина, електронні документи, системи лояльності. Зокрема, станом на 2008 р., як повідомляє Міністерство громадської безпеки Китаю, там функціонує близько одного мільярда RFID [3]. В Україні загальнозастосованими RFID зараз є безконтактні картки оплати метрополітену та біометричні паспорти [4].

Типові загрози. Зворотнім боком переваг та зручностей RFID-технологій є можливість дистанційного несанкціонованого зчитування радіоміток. Про такі загрози було повідомлено ще у 2006 р. [4].

Основна небезпека полягає у можливості зловмисного впливу на систему ідентифікації через радіомітку, що підмінена або модифікована спеціальним вірусом [5]. Атаки можуть проводитися у вигляді SQL-ін'єкції або шляхом переповнення буфера, попри те, що мітки містять невеликі фрагменти даних. Типовий сценарій дії зловмисника може бути наступний [6-8]. Варіант 1 - клонування: виконується несанкціоноване зчитування оригінальної мітки нештатним портативним зчитувачем та запис RFID-клону з метою зловмисної ідентифікації, інакше кажучі – крадіжка ключа. Варіант 2 - атака на систему ідентифікації: викрадена RFID інформація (варіант 1) модифікується за допомогою спеціального програмного забезпечення з метою створення RFID- вірусу. Таким чином створюється інфікований RFID, вірусний код якого при санкціонованому зчитуванні потрапляє в систему ідентифікації та ушкоджує її базу даних. Також інфікована система може переносити вірус на інші оригінальні мітки, що нею використовуються.

Принципи та засоби захисту.

Уразливість систем радіочастотної ідентифікації можливо знизити діями у наступних напрямах:

- організайіцному – через розробку та впровадження загальної політики безпеки RFID-системи в цілому, зокрема мінімізувати несанкціонований доступ до міток та документації до них, що містить конфіденційну інформацію;

- фізичному – використовувати метод екранування радіоміток при їх переміщенні або зберіганні застосовуючи спеціальні екрануючі чохли або контейнери (за принципом клітки Фарадея);
- логічному – використовувати оптимізоване програмне забезпечення RFID-системи для уникнення загроз SQL-ін'єкції, переповнення буфера, виконання інших несанкціонованих клієнтських сценаріїв.

Висновки. Зростаюча популярність RFID- міток, карток, документів та засобів безконтактної оплати привертає увагу хакерів. З іншого боку ведеться моніторинг безпеки RFID [9]. Підсумовуючі аналіз уразливості радіочастотної ідентифікації, означимо, що підвищити інформаційну безпеку можна вимагаючи від розробників та власників даної технології більшої пильності та делікатності при обробці персональних даних, а від клієнтів - дотримання адекватної політики безпеки.

Список використаних джерел:

1. The History of RFID Technology [Ел.рес.]. – Режим доступу: http://www.rfidjournal.com/articles/view?1338
2. Радіочастотна ідентифікація [Ел.рес.]. – Режим доступу: http://uk.wikipedia.org/wiki/ Радіочастотна ідентифікація
3. «Может ли ваша кошка заразиться компьютерным вирусом?» [Ел.рес.]. – Режим доступу: http://www.svoboda.org/content/article/134700.html
4. Введення біометричних паспортів в Україні: про переваги та небезпеку [Ел.рес.]. – Режим доступу: http://eastbook.eu/ua/2012/12/country-ua/ukraine-ua/vvedennia-biometrychnych-pasportiv-v-ukrainy-pro-perevagy-ta-nebezpeku
5. Study Says Chips in ID Tags Are Vulnerable to Viruses [Ел.рес.]. – Режим доступу: http://www.nytimes.com/2006/03/15/technology/15tag.html?_r=0
6. RFID Viruses and Worms [Ел.рес.]. – Режим доступу: http://www.rfidvirus.org
7. Rieback M., Crispo B., Tanenbaum A. Is Your Cat Infected with a Computer Virus? // PERCOM '06 Proceedings of the Fourth Annual IEEE

International Conference on Pervasive omputing and Communications / IEEE Computer Society Washington, DC, USA, 2006.- P. 169-179
8. First human 'infected with computer virus' [Ел.рес.]. – Режим доступу: http://www.bbc.com/news/10158517
9. The RFID Guardian Project [Ел.рес.]. – Режим доступу: http://www.rfidguardian.org

УДК 372.862+004.94
ВОЛОДИМИР ВОЛОДИМИРОВИЧ ТУЛУПОВ
Кандидат технічних наук, доцент кафедри інформаційних технологій та захисту інформації факультету права та масових комунікацій Харківського національного університету внутрішніх справ
ОЛЕКСІЙ МИХАЙЛОВИЧ РВАЧОВ
Викладач кафедри захисту інформації факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми Харківського національного університету внутрішніх справ

ДЕЯКІ ПИТАННЯ РОЗРОБКИ ТА ВПРОВАДЖЕННЯ КОМПОНЕНТІВ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ПІДГОТОВКИ ФАХІВЦІВ З ОРГАНІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ

Постановка проблеми. Розробка та впровадження компонентів інформаційних технологій для підготовки фахівців з організації захисту інформації має суттєву прикладну компоненту наближення до проблематики діяльності підрозділів технічного захисту інформації органів внутрішніх справ. Тому, комп'ютеризація і тренажерізация навчання відносяться до числа найбільш наукомістких областей, що вимагають величезних витрат інтелектуальної праці, у тому числі праці методистів вищої кваліфікації.

Щоб представити масштаб проблем, досить звернути увагу на такі фактори.

По-перше, найбільш ефективна комплексна комп'ютеризація і тренажерізація професійної підготовки фахівців, що забезпечують усі стадії

життєвого циклу виробу: проектування, розробку, випробування, виробництво, експлуатацію і технічне обслуговування, ремонт, або успішного виконання учбового завдання [1, с. 237].

По-друге, розробка однієї години високоефективної навчальної комп'ютерної програми, як показує вже наявний досвід, вимагає витрат багатьох людино-годин праці кваліфікованих методистів і програмістів. При цьому контроль якості навчаючих програм, ефективності тренажерної підготовки є справою складною, що потребує спеціальних тестів, участі експертів тощо. Без такого контролю і сертифікації можливі негативні результати, виникнення помилкових навичок, втрати природного інтелекту у особи, що навчається та ін. До цього варто додати констатацію неухильного зросту вартості апаратних і програмних засобів тренажерів.

По-третє, високий темп розвитку інформаційних технологій зумовлює:

– оновлення засобів матеріально-технічного забезпечення навчального процесу новими зразками техніки та інформаційними технологіями;

– оновлення кадрового потенціалу спеціальних кафедр та взаємопроникнення інформаційних технологій та спеціальних знань в суміжні дисципліни, що викладаються;

– впровадження нових методик і прийомів навчання, комп’ютеризація навчального процесу;

– тісний зв’язок з передовими науково-технічними розробками в сфері інформаційних технологій і спеціальної техніки [1, с. 238].

Метою даної роботи є виділення кола існуючих проблем щодо програмно-технічного забезпечення викладання спеціальних навчальних дисциплін профілюючої кафедри та шляхи їх подальшої реалізації на прикладі створення електронних навчаючих систем та впровадження їх у навчальний процес.

Ефективна організація захисту інформації, у тому числі, що становить державну таємницю, не можлива без виявлення та блокування технічних

каналів витоку інформації. Для цього фахівець із захисту інформації повинен мати навики роботи з вимірювальною апаратурою.

Навик керування складними електронними приладами доцільно, у тому числі, отримувати з використанням різноманітних спеціалізованих комп’ютерних тренажерів та навчаючих програм.

Використовуючи можливості сучасних інформаційних систем можливо провадження в навчальний процес наступних **електронних навчаючих систем**:

– *комп'ютерна навчаюча програма* – єдиний комплекс програмних, текстових та мультимедійних засобів, що за єдиним сценарієм розкриває задану тему;

– *електронний тренажер* – це комплекс програмних, мультимедійних, текстових і графічних комп'ютерних засобів, що покликаний допомоги особи, яка навчаються, відпрацьовувати навички прийняття рішення;

– *електронний підручник* – найбільш статичний за характером спосіб видачі в автоматизованому режимі з використанням комп'ютера матеріалу особі, яка навчається [2].

Також в навчальному процесі можуть бути використані *інтерактивні навчальні відеофільми* (підготовлені із використанням сервісів відеохостінгу «Youtube» або меню оптичних дисків, що були записані у форматі «DVD-Video»), які допомагають отримати та перевірити навички прийняття рішень особою шляхом проходження ним певних квестів (різні наслідки розвитку подій в сюжеті квесту в залежності від варіанту дій, що обрала особа, яка навчається) [3].

Говорячи про електронні тренажери в сфері технічного захисту інформації, необхідно відмітити, що на теперішній час вже пропонуються різні **тренажерні комплекси** для практичного навчання фахівців, професійна діяльність яких пов’язана з технічним захистом інформації, наприклад:

– *програмно-апаратний комплекс «Салют»*, що призначений для пошуку і локалізації відеокамер та акустичних розвідувальних засобів, включаючи тренажер для підготовки операторів;

– *навчаючий тренажерний комплекс «Заря»*, що призначений для підготовки фахівців в галузі атестації об’єктів;

– *навчаючий тренажерний комплекс «Спектр»*, що призначений для підготовки фахівців в галузі пошуку і виявлення радіозакладних пристроїв);

– *автономний імітатор радіозавад «Кобра»*, що призначений для імітації постановки завад радіоелектронним засобам різного призначення і типу з метою навчання операторів рішенню задач в умовах дії навмисних завад, а також відпрацювання дій груп пошуку і знищення передавачів завад, що були занесені та/або встановлені;

– *навчальний тренажерний комплекс з підготовки фахівців у галузі атестації об'єктів інформатизації «Звезда»*, що призначений для практичного навчання фахівців і придбання ними первинних навичок з експлуатації типових програмно-апаратних комплексів для проведення акустичних і віброакустичних вимірювань і контролю ефективності захисту мовної інформації [4].

Вищезазначені тренажерні комплекси, у тому числі розробки кафедр, дозволять у деякій мірі замінити тренування на штатних існуючих або відсутніх на кафедрах приладах засобами сучасних інформаційно-комунікаційних технологій, шляхом виконання учбово-тренувальних задач за допомогою інтерактивного середовища на персональному комп’ютері.

Можливі підходи до розв’язання проблем. У сучасних тренажерах та програмах підготовки і навчання, на них заснованих, закладаються принципи розвитку практичних навичок з одночасною теоретичною підготовкою [5].

Впровадження нових методик навчання здійснюється і в системі відомчої освіти, зокрема в Харківському національному університеті внутрішніх справ, де, вже не перший рік, здійснюється підготовка фахівців за напрямом 6.170102 – «Системи технічного захисту інформації.

Розв’язання деяких вищезазначених проблем знайшли своє відображення в розробках кафедри захисту інформації, а саме: *комп’ютерний тренажер «Селективний мікровольтметр та вимірювач напруги завад SMV 8.5»* призначений для отримання курсантами первинних практичних навичок роботи з селективним мікровольтметром та вимірювачем напруги завад SMV 8.5. Тренажер являє собою спрощений аналог пристрою SMV 8.5 та має наступні можливості:

– ознайомлення користувача з призначенням пристрою;

– ознайомлення з технічними характеристиками SMV 8.5;

– ознайомлення з комплектацією пристрою;

– ознайомлення з органами управління пристроєм;

– демонстрація використання пристрою при виконанні учбово-тренувальних задач;

– безпосереднє виконання учбово-тренувальних задач для оволодіння навичками роботи з пристроєм;

– тестування користувача.

Для забезпечення проведення лабораторних робіт з дисципліни «Методи та засоби технічного захисту інформації» з використанням мультимедійної платформи Adobe Flash (раніше мала назву Macromedia Flash) та інших технологій також було розроблено **комп’ютерні тренажери**: *«Виміри за допомогою селективного мікровольтметру SMV 11»*, *«Виміри за допомогою селективного нановольтметру Unipan-233»* та *«Вимірювач шуму та вібрацій ВШВ-003-М2».* У рамках дипломного проектування розробляються комп’ютерні тренажери для інших пристроїв з подальшим впровадженням їх у навчальний процес.

Висновки. Впровадження таких розробок у навчальний процес дозволить у деякій мірі замінити традиційний науковий інструментарій засобами сучасних інформаційно-комунікаційних технологій, шляхом виконання учбово-тренувальних задач на тренажері, у зв’язку обмеженістю таких приладів на кафедрах.

Список використаних джерел:

1. Тулупов, В. В. Актуальні аспекти побудови комп'ютерних тренажерів для професійної підготовки кадрів органів внутрішніх справ [Текст] / В. В. Тулупов, О. М. Рвачов // Матеріали науково-практичної конференції «Спеціальна техніка у правоохоронній діяльності» (Київ, 25 листоп. 2011 р.). – К. : НАВС, 2012. – С. 236-239.

2. Электронные обучающие системы и тренажёры [Електронний ресурс] // NELSY: научные электронные системы. – Режим доступу: http://xn--h1affr2d.xn--p1ai/spisok-uslug/folder/elektronnye-obuchayuschie-sistemy-i-trenazhyory.

3. Програмні тренажери // Центр інформаційних технологій Національного університету цивільного захисту України. – Режим доступу: http://nuczu.edu.ua/ukr/departments/cit/trenager.

4. Обучающие тренажерные комплексы // ЗАО научно-производственный центр «НЕЛК» [Електронний ресурс]. – Режим доступу: http://www.nelk.ru/catalogue/s7.

5. Андрощук О. С. Розробка комп'ютерних тренажерів щодо навчання персоналу Державної прикордонної служби України [Електронний ресурс] / О. С. Андрощук // Вісник Національної академії Державної прикордонної служби України. – 2014. – Вип. 1. – Режим доступу: http://nbuv.gov.ua/j-pdf/Vnadps_2014_1_3.pdf.

УДК 657.004
ІРИНА КОСТЯНТИНІВНА СЕЗОНОВА
Кандидат технічних наук, доцент, професор кафедри інформаційної та економічної безпеки Харківського національного університету внутрішніх справ
ТЕТЯНА ПЕТРІВНА КОЛІСНИК
Кандидат педагогічних наук, доцент, доцент кафедри інформаційної та економічної безпеки Харківського національного університету внутрішніх справ

ІНФОРМАЦІЙНА БЕЗПЕКА ПРАВООХОРОННИХ ОРГАНІВ

Інформаційна безпека є невід’ємною складовою національної безпеки. Саме тому різні органи державної влади мають приділяти особливу увагу гарантуванню цієї безпеки, особливо в контексті неухильного руху розвинених суспільств (до яких активно, в силу нещодавніх політичних змін, намагається долучитися і наше суспільство) до всеохопної інформатизації всіх сфер їх життєдіяльності. Особливо це стосується правоохоронних органів та органів безпеки, які мають не лише забезпечити накопичення, а й збереження інформації державно-управлінського характеру.

Створення або модернізація інформаційних ресурсів державного підпорядкування неможливо без комплексу засобів і заходів по захисту інформації. Для успішного виконання поставленої задачі проектувальник та замовник повинні діяти по визначеному алгоритму, починаючи від передпроектної стадії та закінчуючі актами прийому системи в експлуатацію після відповідних випробувань. Одним з найважливіших організаціних моментів проектування та впровадження інформаційно-реєстраційних та довідкових комп'ютерних систем є необхідність розмежування виконавців різних етапів, тобто проведення робіт потрібно доручати різним організаціям. Етап передпроектного обстеження та його аналітичного обгрунтування виконується замовником або його представником. Для виконання робіт по створенню системи захисту необхідно залучати спеціалізовані організацій,

що мають необхідні ліцензії на право проведення робіт із захисту інформації та ін.

Сучасні інформаційно-реєстраційні та довідкові комп'ютерні системи (КС) державного підпорядкування, в яких фіксується та зберігається інформація, яка може бути об'єктом несанкціонованого доступу (НСД) з метою зміни обо вилучення, проектуються та запроваджуються сьогодні у всі сфери державного управління.

На передпроектній стадії система захисту інформації визначається на найзагальнішому, концептуальному рівні з тим, щоб правильно визначити основні пріоритети її побудови і взаємозв'язок між її окремими компонентами.

Передпроектна стадія включає: 1) визначення переліку відомостей, які підлягають захисту від НСД і від витоку інформації по технічних каналах; 2) проведення аналізу територіального розташування і режиму функціонування об'єкта захисту; 3) проведення аналізу організації фізичної охорони, пропускного і внутрішнього режимів роботи об'єкта захисту; 4) визначення переліку приміщень, що підлягають захисту; 5) визначення умов розташування об'єктів інформатизації щодо меж критичних загроз; 6) проведення аналізу організаційної структури об'єкта захисту; 7) проведення аналізу відповідальності персоналу за забезпечення безпеки комерційної таємниці; 8) визначення режимів обробки інформації, характеристик і класу захищеності комп'ютерних систем; 9)визначення заходів щодо забезпечення конфіденційності інформації в процесі проектування об'єкта інформатизації.

Передпроектне обстеження об'єкта, що захищається проводиться комісією, призначеною керівником підприємства (організації, фірми) або спеціалізованої сторонньою організацією, яка має відповідну ліцензію з укладанням відповідних договорів на проведення робіт з обстеження об'єктів, що захищаються.

Результатом передпроектного обстеження має бути аналітичне обгрунтування вимог до системи захисту інформації, яке оформлюється у

вигляді пояснювальної записки з наступними відомостями: інформаційною характеристикою та організаційною структурою КС; матрицею доступу до критичних даних; матрицею моделей ймовірного порушника системи захисту; матрицею моделей ймовірних загроз НСД до критичних даних; переліком технічних каналів витоку інформації, які підлягають закриттю при виявленні НСД; вимогами та можливостями щодо контролю ефективності захисту інформації та ін.

На підставі передпроектного обстеження оформлюється технічне завдання на проектування системи захисту, яке узгоджується з проектною організацією, службою безпеки організації - замовника та затверджується керівником організації - замовника.

Технічний проект включає розробку організаційних і технічних заходів за рівнями деталізації політики інформаційної безпеки.

Рівень «Організаційна безпека» включає: управління політикою інформаційної безпеки; розподіл обов'язків щодо забезпечення інформаційної безпеки; регламентацію процесу обробки критичних даних; аудит інформаційної безпеки; регламентацію роботи зі сторонніми організаціями.

Рівень «Управління персоналом» включає: підбір персоналу; включення питань інформаційної безпеки в посадові обов'язки; навчання персоналу; адміністративне реагування на інциденти порушення інформаційної безпеки.

Рівень «Фізичний захист і захист від впливів навколишнього середовища» включає: забезпечення безпеки та контроль доступу в зони, які охороняються; розташування і захист технічного устаткування; забезпечення захисту електроживлення та безпеки кабельної мережі від пошкодження і перехоплення інформації; організація технічного обслуговування обладнання.

Рівень «Безпечне адміністрування систем і мереж» включає: процедури рівня операційної системи щодо контролю дій системних адміністраторів;

захист від шкідливого програмного забезпечення; резервування інформації; управління безпекою мережі та її моніторінг.

Рівень «Управління контролем доступу користувача» включає: управління контролем доступу користувача; контроль мережного доступу; контроль доступу до операційної системи; контроль доступу до додатків; моніторинг доступу та використання системи.

Введення в експлуатацію системи захисту КС включає етапи: дослідної експлуатації системи захисту інформації в комплексі з іншими технічними та програмними засобами з метою перевірки її працездатності у складі об'єкта інформатизації та відпрацювання технологічного процесу обробки (передачі) інформації; випробувань системи захисту за результатами дослідної експлуатації; оцінки захищеності об'єктів інформатизації за вимогами інформаційної безпеки.

Одним з найважливіших організаціних моментів проектування та впровадження інформаційно-реєстраційних та довідкових КС є необхідність розмежування виконавців різних етапів, тобто проведення робіт потрібно доручати різним організаціям. Етап передпроектного обстеження та його аналітичного обгрунтування виконується замовником або його представником. Для виконання робіт по створенню системи захисту необхідно залучати спеціалізовані організацій, що мають необхідні ліцензії на право проведення робіт із захисту інформації та ін.

Інформаційна безпека є комплексною та багатозадачною проблемою, рішення якої потрібно починати на етапі проектування КС з дотриманням визначеного алгоритма.

УДК 378.147
ВОЛОДИМИР ПЕТРОВИЧ КУБРАК
Старший викладач кафедри інформаційної
та економічної безпеки ХНУВС

ЗНАЧЕННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ РОБОТИ В ДІЯЛЬНОСТІ ОРГАНІВ ВНУТРІШНІХ СПРАВ

Невід'ємною та важливою складовою частиною будь якої управлінської діяльності є інформаційно-аналітична робота, яка уявляє собою збір, обробку, вивчення та оцінку інформації з метою прийняття необхідних управлінських рішень. Інформаційно-аналітична робота в органах внутрішніх справ направлена на вивчення та оцінку інформації про стан злочинності та громадського порядку, результати роботи органів щодо виконання поставлених перед ними завдань. Наявність об'єктивного та достатнього обсягу інформації є головними умовами прийняття вірних управлінських рішень щодо попередження негативних тенденцій, ефективного керування силами та засобами, своєчасного надання підлеглим органам необхідної допомоги та розповсюдження передового досвіду.

Основне завдання, що стоїть сьогодні перед інформаційно-аналітичними підрозділами, це забезпечення надання на всіх рівнях управління інформації про реальний стан оперативної обстановки, можливих напрямках її розвитку, і на цій основі розробка конкретних пропозицій по попередженню правопорушень та оперативному реагуванню на зміну криміногенної ситуації, об'єктивна оцінка результатів оперативно-службової діяльності служб і підрозділів органів внутрішніх справ.

Основне місце в інформаційно-аналітичній роботі займає вивчення та оцінка оперативної обстановки, яка уявляє собою сукупність об'єктивно існуючих умов, в яких діє орган внутрішніх справ, а також його сили і засоби та результати діяльності.

Основним прийомом аналітичної роботи є порівняння статистичних показників, які характеризують оперативну обстановку, в просторі та часі.

Порівняння в часі – це порівняння показників досліджуваного регіону за поточний період з показниками попередніх періодів. Порівняння в просторі – це порівняння показників досліджуваного регіону з аналогічними показниками іншого однорідного регіону (або регіонів) або показниками регіону більш високого рівня (порівняння показників району з показниками області, держави).

Порівняльна оцінка показників оперативної обстановки дає можливість прослідкувати її зміну в негативний або позитивний бік і як слідство – прийняти заходи усунення недоліків або розповсюдження передового досвіду.

За своїм складом аналіз оперативної обстановки повинна включати в себе характеристику злочинності, аналіз середовища, вивчення осіб, які вчинили злочини, оцінку результатів оперативно-службової діяльності.

Характеристика злочинності полягає в вивченні її загального розміру, складу, інтенсивності, структури, динаміки, суспільної небезпеки, територіальної поширеності (“географії”).

Аналіз стану злочинності починається з вивчення її абсолютних показників – загального розміру та складу злочинності. Знання цих показників дозволяє співставити їх з попередніми (наприклад, за минулий рік) значеннями, зробити відповідні висновки щодо характеру їх зміни.

Але вивчення загального розміру та складу злочинності є тільки першим кроком в статистичному аналізі злочинності. На жаль ці показники не мають необхідних аналітичних можливостей та не дозволяють порівняти стан криміногенної обстановки в різних регіонах, встановити територіальну та часову розповсюдженість злочинів за їх видами, засобами вчинення, об’єктом посягання та іншими характеристиками.

Для аналізу територіальної розповсюдженості злочинності визначається інтенсивність злочинності, яка характеризується коефіцієнтом злочинної інтенсивності або кількістю злочинів, що припадає на певну кількість населення.

Слідуючим кроком в аналізі злочинності є визначення її структури, яка характеризується таким показником, як питома вага окремих груп злочинів в їх загальній кількості, що дозволяє охарактеризувати поширеність тих чи інших видів злочинів на певній території та визначити стратегію боротьби з ними.

Структуру злочинності можна визначати також і за ступенем тяжкості злочинів, статтями Кримінального кодексу, віком (неповнолітні, дорослі), наявністю чи відсутністю особи, що вчинила злочин, (очевидні, неочевидні) і т.д.

При дослідженні складу та структури злочинності цілим може бути як загальна кількість зареєстрованих злочинів, так і їх окремі види. Так, якщо за ціле взяти злочини певного розділу Кримінального кодексу, можна визначити склад та структуру цих злочинів за статтями Кримінального кодексу.

Крім вивчення загального розміру, складу, інтенсивності, структури злочинності увага повинна приділятися також дослідженню динаміки злочинності – зміни в часі вказаних показників, що дозволяє встановити тенденції, закономірності цих змін, здійснити прогнозування стану злочинності.

Важливою характеристикою злочинності є її суспільна небезпека. Найбільшу суспільну небезпеку являють тяжкі та особливо тяжкі злочини. Тому при оцінці оперативної обстановки необхідно окремо вивчати ці злочини: визначати їх кількість, питому вагу в загальній кількості зареєстрованих злочинів, коефіцієнт злочинної інтенсивності (рівень на певну кількість населення), склад, структуру та динаміку. За такими ж показниками необхідно вивчати неочевидні тяжкі та особливо тяжкі злочини.

Ще однією характеристикою злочинності є її територіальна поширеність (“географія”). Це розподіл злочинів по районах міста, адміністративних ділянках, мікрорайонах, сільських радах. Аналіз

здійснюється шляхом вивчення стану та динаміки злочинів. Важливе значення має визначення впливу на криміногенну ситуацію в межах району осіб, які мешкають в інших районах (так званий “коефіцієнт впливу”). Цей показник розраховується шляхом ділення кількості злочинів, вчинених на території даного району мешканцями інших районів на кількість злочинів, скоєних мешканцями даного району в інших районах. Чим вище цей показник, тим більше вчинюється злочинів “не місцевими” особами, і чим нижче – тим більше злочинів вчинюють місцеві особи в інших районах.

Однією з найважливіших завдань інформаційно-аналітичної роботи є виявлення статистичного зв'язку, залежності, співвідношення між злочинністю, діяльністю органів внутрішніх справ та факторами, які їх обумовлюють.

Знання характеру цих залежностей дозволяє пояснити причини зміни стану злочинності та правоохоронної діяльності в просторі та часі, а значить забезпечити прийняття необхідних заходів соціального реагування.

Значне місце в інформаційно - аналітичній роботі посідає вивчення осіб, які вчинили злочини. При цьому визначається як загальна кількість зареєстрованих осіб, які вчинили злочини, так і їх склад, злочинна активність, структура, динаміка.

При аналізі осіб, що вчинили злочини, необхідно визначати і міру ураження злочинами окремих груп населення: за віком, статтю, соціальним станом, родом занять, належністю до окремих галузей народного господарства і т.д. Ці дані одержуються шляхом обчислення спеціальних коефіцієнтів злочинної активності (розділити число осіб будь-якої категорії, що вчинили злочини, на чисельність населення цієї категорії). Порівнюючи отримані коефіцієнти між собою, визначається, наскільки вражена злочинністю та чи інша група.

Оцінка результатів оперативно-службової діяльності здійснюється на базі критеріїв та показників, встановлених нормативними актами МВС

України, за основними напрямками діяльності та лініями служб в порівнянні з аналогічним періодом минулого року.

Таким чином, інформаційно-аналітична робота є невід'ємною частиною діяльності ОВС щодо боротьби зі злочинністю.

УДК 621.324
МИХАЙЛО ВІТАЛІЙОВИЧ ЦУРАНОВ
Викладач кафедри інформаційних технологій та захисту інформації факультету права та масових комунікацій ХНУВС
ОЛЕКСАНДР ВОЛОДИМИРОВИЧ БЕЗРУК
Студент факультету права та масових комунікацій Харківського національного університету внутрішніх справ

ПОКАЗНИКИ ЕФЕКТИВНОСТІ ПЕРЕДАЧІ ІНФОРМАЦІЇ В БАНКІВСЬКИХ СИСТЕМАХ

За останні роки правоохоронні органи почали реєструвати все більшу кількість спроб кіберзлочинців отримати доступ до особистих або фінансових даних громадян. Так, наприклад в 2011 році було здійснено 7600 несанкціонованих операцій, в результаті чого банками та їх клієнтами було втрачено 9,1 млн. гривень [1]. Слід зазначити, що з кожним роком втрати від карткових кіберзлочинців збільшуються не третину [1]. Також слід зазначити, що українці публікують свої персональні данні у відкритому вигляді у соціальних мережах і з легкістю повідомляють незнайомим особам свої паспортні данні по телефону[2].

Управління боротьби з кіберзлочинністю МВС України зазначило, що збитки від дії кіберзлочинців за 2012 рік сягнули 100 мільйонів грн. [2].

За останні 5 років кількість платежів з використанням платіжних карток зростає на 7% щорічно, на теперішній час в країнах СНД кількість безготівкових платежів з використанням платіжних карток збільшилась до 38%[2]. Тому слід приділяти більшу увагу надійності банківських мереж та програмно-апаратних які в них використовуються.

В спеціальній літературі можна зустріти наступне визначення показника ефективності – кількісна характеристика властивості ефективності системи чи цілеспрямованого процесу, яка є результатом вимірювання чи підрахунку[3]. Для того щоб більш повно оцінити ефективність систем потрібно вирішувати багатокритеріальні задачі.

Під критерієм ефективності слід розуміти – правило чи спосіб прийняття рішення з врахуванням ефективності системи.

Для підключення банкоматів до банківської мережі фінансові установи використовують декілька видів технологій. Найбільш поширеним серед яких є підключення за допомогою стільникових мереж чи каналів радіозв'язку.

На ці канали значною мірою впливають різні завади, як штучного так і природного походження. Це значною мірою зменшує швидкість обміну інформації між банкоматом та процесінговим центром, що призводить до збільшення часу очікування клієнта відповіді банкомату.

Для вирішення вищезгаданої проблеми банківськими установами використовуються різні види завадостійкого кодування. Найбільш поширеним серед яких є коди коди Боуза - Чоудхурі - Хоквингхема (БЧХ-коди) [4]. Ці коди відрізняються можливістю побудови з попередньо визначеними корегуючими властивостями, а саме, мінімальною кодовою відстанню, яке визначається кількістю знайдених і виправлених помилок.

Для визначення найбільш оптимальних характеристик завадостійких кодів автори рекомендують використовувати завадостійке кодування з використанням наступного комплексного показника ефективності:

$$K_к = K_{в1}\frac{K_1}{K_1 + K_2} + K_{в2}\frac{F_{сри}}{t_\Sigma к} + K_{в3}\frac{F_{сри}}{t_\Sigma дк} + K_{в4}\frac{Ко_{одн}}{Ко_{общ}} + K_{в5}\frac{K_{ош}}{K_{ош} + K_{нош}} + K_{в6}\frac{K_{мах}}{K_{общ}}$$

де $К_{в1}$, $К_{в2}$, $К_{в3}$, $К_{в4}$, $К_{в5}$, $К_{в5}$ - вагові коефіцієнти, які визначають експерти;

К1 - кількість інформаційних символів;

К2 - кількість перевірочних символів;

$F_{сри}$ - Тактова частота процесора, вимірюється в тактах;

$t_{\Sigma}к$ - Сумарний час, в тактах процесора, необхідний для виконання операцій кодування алгоритму завадостійкого коду, при однакових пакетах даних;

$t_{\Sigma}дк$ - Сумарний час, в тактах процесора, необхідний для виконання операцій декодування алгоритму завадостійкого коду, при однаковому каналі зв'язку та пакеті даних;

$Ко_{одн}$ - кількість одночасно виконуваних операцій в алгоритмі;

$Ко_{общ}$ - загальна кількість операцій в алгоритмі;

Кош - кількість помилок які виникли в результаті передачі даних КЗ;

Кнош – Кількість, теоретично обґрунтованих, виправлених помилок;

$К_{общ}$ - загальна кількість біт для передачі з використанням алгоритму;

$К_{мах}$ - максимально можлива кількість помилкових біт в алгоритмі, які можливо виправити.

Література:

1. Банки готовятся к всплеску карточного мошенничества во время Евро-2012 [Електронний ресурс]. – Режим доступу до ресурсу: http://www.banki.ua/news/bankpress/?id=158120&sphrase_id=145250
2. Довірливі українці легко стають жертвами інтернет-шахраїв [Електронний ресурс]. – Режим доступу до ресурсу:http://tsn.ua/ukrayina/nayivni-ukrayinci-legko-stayut-zhertvami-internet-shahrayiv-279012.html
3. Надежность и эффективность в технике: Справочник: В10 т. / Ред. совет: В.С. Авдуевский (пред.) и др. – М.: Машиностроение, 1986. Т. 1: Методология. Организация. Терминология/Под ред. А.И. Рембезы. – 224 с.: ил.
4. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. – М. : Мир, 1986.

УДК 65.012.8 + 004
ЄВГЕН ОЛЕКСАНДРОВИЧ ЖИЦЬКИЙ
Здобувач Харківського національного університету внутрішніх справ

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНОГО ОБСЛУГОВУВАННЯ В ОКРЕМИХ КРАЇНАХ

Одним з найважливіших факторів, який визначає ефективність оперативного обслуговування, є його якісне інформаційно-аналітичне забезпечення, яке не можна розглядати окремо, безвідносно до системи оперативного обслуговування, адже воно безпосередньо є його елементом. Як видно із самого терміну його можна розкласти на дві складових частини: інформаційну та аналітичну.

Інформаційне забезпечення є тісно пов’язаним із поняттям інформаційна потреба, якою визначається характер інформації, її обсяг, джерела та носії, канали одержання, порядок накопичення, аналізу та використання, тобто якісні та кількісні характеристики інформаційних потоків. Так, недостатність інформації призводить до поверхневої, неглибокої оцінки фактів та подій, а надлишковість – до засмічення інформаційного масиву, надмірній затраті сил на її обробку. У цьому сенсі окремі дослідники сфери оперативно-розшукової діяльності справедливо відмічають інформаційну перенасиченість працівників кримінальної міліції. При цьому наголошується, що нерідко значний масив оперативно-розшукової інформації, якою володіють оперативні працівники, залишається невикористаною. Вказане твердження наштовхує на думку про те, яким чином можна таку інформацію зберегти, проаналізувати та використати у рамках оперативного обслуговування? Відповідей на це запитання може бути декілька. Разом з тим, на нашу думку, найбільш прийнятним вирішенням цього завдання, яке не обтяжуватиме оперативних працівників зайвою звітністю, є поточне занесення відповідної інформації до спеціалізованої бази даних.

Російські науковці звертають увагу, що банки даних не будуть відповідати цілям їх створення, якщо надавані ними відомості хоча б у незначній мірі відрізнятимуться від дійсності. У цьому випадку, одного разу стикнувшись із викривленою або неповною інформацією, працівники оперативних підрозділів у кращому випадку будуть із обережністю ставитись до даних оперативних обліків, або взагалі відмовляться від їх використання.

У країнах світу інформаційному забезпеченню оперативного обслуговування приділяють значну увагу. У цьому сенсі корисним вбачається до застосування в Україні російський досвід залучення до оперативного обслуговування в частині його відповідного інформаційно-аналітичного забезпечення підрозділів оперативно-розшукової інформації, яким з цією метою надається право проведення окремих оперативно-розшукових заходів: опитування, наведення довідок, збирання зразків для порівняльного дослідження, ототожнення особистості, використання конфіденційного співробітництва. Вказані підрозділи беруть активну участь в аналізі оперативної обстановки за напрямами, що безпосередньо корелюється із завданнями оперативного обслуговування об’єктів і ліній роботи.

На теперішній час у країнах Заходу створено та інтегровано потужні інформаційні масиви за різними напрямками діяльності, що дозволяє ефективно здійснювати правоохоронну діяльність. Як правило ці тенденції стосуються лише провідних країн світу.

Наприклад, у Німеччині основними інформаційними базами, які можуть бути застосовані у негласній роботі є:

- INPOL (Informationssystem der Polizei) – інформаційна система поліцій федерації і земель ФРН в цілях розшуку людей/предметів в інтересах кримінального переслідування і запобігання небезпеки;

- SIS (Schengener Informationssystem) – Шенгенська інформаційна система – поліцейська комп’ютерна система розшуку, що забезпечує

працівникам європейських поліцій держав-учасниць Шенгенського договору прямий доступ до баз даних по розшуку осіб і предметів;

- VERMI / UTOT – поліцейська база даних безвісти зниклих / невпізнаних трупів;

- AFIS – поліцейська автоматизована система ідентифікації відбитків пальців;

- DAD – поліцейська база даних ДНК;

- SPUDOK – поліцейська база даних документації слідів злочинів;

- INTRANET/EXTRANET – закриті поліцейські розшукові бази даних;

- AZR – центральний реєстр іноземців;

- ZEVIS – Центральна інформаційна транспортна система федерального автотранспортного відомства ФРН тощо.

У правоохоронних органах США та низки країн Європи значна увага приділяється візуалізації, під час провадження кримінальної розвідки, зокрема під час розбудови зв'язків між особами, які становлять оперативний інтерес. З цією метою застосовується матричний або графовий підхід (рис. 1). Як показує практика, візуалізована інформація набагато краще сприймається правоохоронцями, а це у свою чергу підвищує ефективність їхньої діяльності.

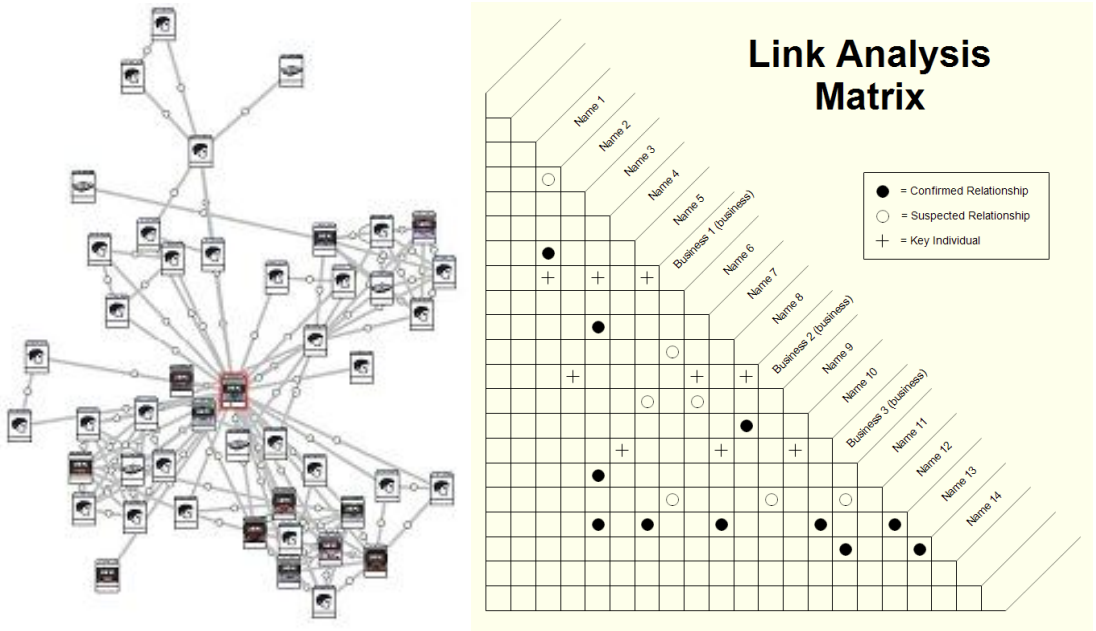


Рис. 1. – Форми візуалізації аналізу зв'язків осіб, які становлять оперативний інтерес

Попри наведені досягнення слід наголосити, що в окремих країнах, які розвиваються, спостерігається відставання у сфері інформаційного забезпечення. Наприклад, у Нігерії на теперішній час лише розробляється система накопичення оперативно-розшукової інформації, подібна до вітчизняної.

Підбиваючи підсумки, зазначимо, що враховуючи сучасні світові тенденції збільшення ролі інформаційного забезпечення в оперативному обслуговуванні, на нашу думку, варто розширити функції аналітичних підрозділів у рамках здійснення оперативно-розшукової діяльності.