МВС України
Харківський національний університет внутрішніх справ

ВИКОРИСТАННЯ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ У ПОПЕРЕДЖЕННІ ЗЛОЧИНІВ

Матеріали науково-практичного семінару
(м. Харків, 6 грудня 2012 року)

Харків 2012

УДК 343.85.001.76(477)
ББК 65.9(4УКР)61
В43

Друкується відповідно до розпорядження
Харківського національного університету внутрішніх справ
від 04.09.2012 № 144

В43 **Використання** інноваційних технологій у попередженні злочинів : матеріали наук.-практ. семінару (м. Харків, 6 груд. 2012 р.) / МВС України, Харк. нац. ун-т внутр. справ. – Х. : ХНУВС, 2012. – 196 с.

Збірка містить тези доповідей учасників науково-практичного семінару за напрямами: нормативно-правове та організаційне забезпечення використання інноваційних технологій у правоохоронній діяльності; міжнародний досвід використання інноваційних технологій у правоохоронній діяльності; інформаційно-аналітичне забезпечення боротьби зі злочинністю; інноваційні технології оперативно-розшукової діяльності; перспективні напрями застосування спеціальної техніки; особливості підготовки та підвищення кваліфікації фахівців для боротьби з високотехнологічними злочинами.

УДК 343.85.001.76(477)
ББК 65.9(4УКР)61

Матеріали викладені в авторській редакції з незначними коректорськими правками. Відповідальність за точність поданих фактів, цитат, цифр і прізвищ несуть автори.

ЗМІСТ

УДК 343.1:343.85-053.81(477)

Вадим Миколайович БАБАКІН
кандидат юридичних наук, доцент,
професор кафедри оперативно-розшукової діяльності
навчально-наукового інституту підготовки фахівців кримінальної міліції
Харківського національного університету внутрішніх справ

ОКРЕМІ АСПЕКТИ ПРАВОВОГО РЕГУЛЮВАННЯ ДІЯЛЬНОСТІ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ ОРГАНІВ ВНУТРІШНІХ СПРАВ ЩОДО ПРОТИДІЇ МОЛОДІЖНІЙ ЗЛОЧИННОСТІ

Робота присвячена вивченню сучасного стану правового регулювання діяльності оперативних підрозділів органів внутрішніх справ щодо протидії молодіжній злочинності.

За дослідженням протидія молодіжної злочинності це не лише ключ до розробки найбільш ефективних методів протидії з нею, але й засіб прогнозування взагалі злочинності у країні. У зв'язку із цим успішна протидія даному явищу дозволяє знизити кримінальну напруженість, а також слугує запобіганням зростання злочинності в цілому, у тому числі організованої. Саме цим і обґрунтовується актуальність дослідження особливостей суті та методів протидії із нею. Сучасні масштаби поширення молодіжної злочинності зумовлюють виникнення гострої необхідності у розвитку та вдосконаленні засобів такої протидії. Оскільки основою активної протидії є законодавче регулювання, то доцільно проаналізувати правове регулювання діяльності оперативних підрозділів органів внутрішніх справ, у тому числі із протидії молодіжній злочинності.

Традиційно проблема молодіжної злочинності розглядається або в контексті більш широкої проблеми дорослої злочинності, або в рамках злочинності неповнолітніх. У чинному законодавстві не існує розмежування проміжного між дитинством та дорослістю етапу розвитку особистості – молодості за якої відбувається формування та становлення дорослої особистості. Так, згідно із п. 1 ст. 22 Кримінального кодексу України, кримінальній відповідальності підлягають особи, яким на момент вчинення злочину виповнилося шістнадцять років; п. 2 цієї ж статті передбачено понижений вік кримінальної відповідальності та притягнення осіб віком від 14 років за вчинення вичерпного переліку тяжких і особливо тяжких злочинів [1].

Однією із вихідних точок для подальшого розвитку правового регулювання протидії молодіжній злочинності засобами оперативно-розшукової діяльності є дослідження діючих нормативно-правових актів, у яких відтворено пріоритети державних та національних

політики та запобігання злочинності. Як
та методи правового регулювання
діяльності оперативних підрозділів органів внутрішніх справ залежать також від завдань, цілеспрямованих інтересів держави в цій сфері, які об'єктивно обумовлені існуючими матеріальними умовами життя [2, с. 85], що ми підтримуємо.

За результатами проведеного аналізу чинного законодавства встановлено, що молодіжна політика держави відтворюється у тексті Конституції, Закону України «Про сприяння соціальному становленню та розвитку молоді в Україні». Зокрема, ст. 2 даного Закону встановлено, що одним із основних принципів соціального становлення та розвитку молоді є єдність зусиль держави, всіх верств суспільства, політичних і громадських організацій, підприємств, установ, організацій та громадян у справі соціального становлення та розвитку молоді [3]. Відповідно до цього положення участь оперативних підрозділів органів внутрішніх справ у реалізації державної молодіжної політики, на нашу думку, полягає у сприянні процесу декриміналізації молоді, що у межах їх повноважень зводитися до: виявлення, запобігання, припинення злочинів із участю молодіжного контингенту, зокрема, запобігання злочинної діяльності молодіжних угрупувань; виявлення причин та умов, що сприяють вчиненню молодіжним контингентом правопорушень та вживання заходів щодо їх усунення у межах своїх повноважень; проведення у процесі здійснення оперативно-розшукових заходів у такий спосіб, що сприяє формуванню авторитету закону, правоохоронних органів, конкретного працівника тощо.

Загалом, ефективність діяльності оперативних підрозділів органів внутрішніх справ у протидії молодіжній злочинності, багато в чому залежить від того, наскільки вдало вони вміють поєднувати свій професійний, життєвий та накопичений колективний досвід із здатністю творчо мислити при виявленні та розслідуванні конкретних злочинів. Також вона залежить і від наявності відповідних методик, їх адекватності тим проблемам, які постають при розслідуванні кожного конкретного злочину вчиненого молодіжним контингентом. Проте, головним критерієм оцінки оперативно-розшукової діяльності є дотримання законності. Тому неприпустимим у діяльності органів внутрішніх справ є будь-яке неправомірне, недосконале застосування

засобів оперативно-розшукової діяльності, спроможне причинити шкоду особистим інтересам громадян, що охороняються Конституцією України (ст. 3, 8, 17, 21, 28–32, 55) [3, с. 7].

Висновок. Зростання молодіжної злочинності, яке спостерігається в останні десятиліття, є безпосереднім наслідком ряду соціально-економічних та соціокультурних змін, а також свідченням глибокої кризи, яку переживає українське суспільство. Як свідчать результати дослідження на даний момент законодавство та нормативне регулювання діяльності оперативних підрозділів органів внутрішніх справ, у тому числі у протидії молодіжній злочинності, перебуває на етапі концептуального формування, у зв'язку із чим існує гостра потреба у проведенні подальших досліджень теорії і практики та удосконалення їх методологічного фундаменту.

Втім підняті питання не є остаточними і потребують додаткового дослідження чи наукового вивчення.

Список використаних джерел:

1. Кримінальний кодекс України [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2341-14. – Зі змін. та допов. на 07.06.2012.

2. Філіпенко Н. Є. Проблеми правового регулювання діяльності оперативних підрозділів органів внутрішніх справи України / Н. Є. Філіпенко // Форум права. – 2005. – № 1. – С. 78–95 [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/2005-1/05fnevsu.pdf.

3. Про сприяння соціальному становленню та розвитку молоді в Україні : закон України [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2998-12. – Зі змін. та допов. на 23.12.2010.

4. Сілюков В. О. Засоби оперативно-розшукової діяльності : навч.-метод. посіб. / Сілюков В. О., Черкова В. О. ; МВС України, Луган. держ. ун-т внутр. справ. – Луганськ : РВВ ЛДУВС, 2007. – 96 с.

Отримано 28.11.2012

УДК 351.746.2:007

Дмитро Олександрович БАБІЧЕВ
кандидат юридичних наук, доцент,
заступник начальника кафедри інформатики, спеціальної техніки
та інформаційних технологій у діяльності ОВС
Луганського державного університету внутрішніх справ
імені Е. О. Дідоренка
Анна Олександрівна МЕДВЕДЧУК
здобувач інформатики, спеціальної техніки
та інформаційних технологій у діяльності ОВС
Луганського державного університету внутрішніх справ
імені Е. О. Дідоренка

ІНФОРМАЦІЙНО-АНАЛІТИЧНІ СИСТЕМИ ГУМВС УКРАЇНИ В ЛУГАНСЬКІЙ ОБЛАСТІ: НАЯВНА ПРАКТИКА ТА ПРОБЛЕМИ ЗАСТОСУВАННЯ

Розглянуто практику застосування інформаційно-аналітичних систем в діяльності оперативних підрозділів органів внутрішніх справ, проаналізовано проблеми подальшого їх функціонування в умовах розвитку національної правової системи.

Попередження, виявлення та припинення злочинів є основним завданням діяльності оперативних підрозділів ОВС щодо захисту життя, здоров'я, прав і свобод громадян, власності, інтересів суспільства й держави. Ефективність його виконання в значній мірі залежить від своєчасного й системного інформаційного забезпечення, зорієнтованого на застосування іноваційних методів, новітніх програмних технологій і, зокрема, сучасних автоматизованих систем накопичення й обробки даних [1, с. 4].

У даному контексті таким, що заслуговує на увагу учасників семінару, є досвід Управління інформаційно-аналітичного забезпечення ГУМВС України в Луганській області (далі – УІАЗ) [2, с. 53–57]. Його працівниками впроваджено в оперативно-службову діяльність ОВС ряд унікальних інформаційно-аналітичних систем, що оперують алгоритмічно структурованими й постійно обновлюваними масивами даних. Всі системи розроблено з використанням найсучасніших інформаційних технологій, комп'ютерного та телекомунікаційного обладнання. Для зручності їх об'єднано в єдиний аналітичний комплекс – інтегровану інформаційну систему.

Одним з елементів створеного комплексу є АІС «СОВА+». Програмний комплекс характеризується повною автоматизацією

пошуку та виявлення логічних закономірностей зв'язків об'єктів оперативної зацікавленості у процесі багаторівневого опрацювання масивів вихідних даних з подальшим наданням результатів пошуку в наочному, інтуїтивно-зрозумілому операторові вигляді. Зокрема, результати аналізу можуть бути надані у формі максимально інформативного й логічно впорядкованого електронного «досьє», що показує повну графічну схему прямих і непрямих зв'язків об'єкта, картографічну інформацію (розташування певних об'єктів обліку на мапі чи схемі) тощо.

Прикладом застосування АІС «СОВА+» є розкриття злочину, вчиненого 13.09.2012 на території м. Лутугіно Луганської області. Так, до чергової частини звернулася с заявою гр. П. про те, що за місцем її проживання невідомий наніс ножове поранення її чоловіку, від якого останній помер. Отримана інформація після виїзду СОГ до місця пригоди була внесена через комп'ютерну мережу до ІІПС МВС України. Подальше її опрацювання співробітниками відділу оперативних обліків УІАЗ (у межах повідомлень негласного апарату, справ оперативних розробок тощо) дозволило визначити декілька осіб, які мешкають у селищах Лутугинського району, зловживають спиртними напоями, у відношенні яких є інформація про причетність до вчинення правопорушень, у тому числі насильницького характеру. Під час перевірки відповідної інформації працівниками карного розшуку був затриманий гр. Б., який зізнався у вчиненні вказаного вбивства.

Не менш ефективними ІАС є «Спіраль» – автоматизована габітоскопічна система ідентифікації особи за методом словесного портрета, в основі якої закладено спеціальний алгоритм нечіткого порівняння об'єктів, та «АРГУС» – автоматизована біометрична система ідентифікації людини за її фото- та відео зображенням, що реалізує програмні методи автоматичної ідентифікації, основані на фізіологічних та поведінкових характеристиках людини [5, с. 6].

Прикладом застосування АІС «Спіраль» є встановлення особи невпізнаного трупу, знайденого 09.06.2012 у лісосмузі біля кв. Мірний м. Луганська. Так, співробітниками УІАЗ в результаті ідентифікації визначено співпадіння указаного трупу з характерними прикметами та описом одягу декількох розшукуваних осіб: гр. Г., гр. М., гр. К. Подальшою перевіркою відповідної інформації силами працівників карного розшуку встановлено, що померлим є власне гр. М.

Вкрай актуальною в умовах застосування положень нового Кримінального процесуального кодексу України й відповідно створення «Єдиного реєстру досудових розслідувань» є АІС

«КРИСТАЛЛ». Дана система створена з метою вирішення завдань з формування, аналізу і контролю інформаційних масивів, що містять відомості про злочини та осіб, які їх вчинили [5, с. 37].

Ефективність і подальша доцільність застосування вищевказаних та інших ІАС в роботі оперативних підрозділів ОВС не викликає сумнівів, оскільки має міцне апробоване практикою й часом підґрунтя. З їх допомогою щорічно розкривається більш ніж 5 тисяч злочинів, що складає близько 70 % від загальної їх кількості [4, с. 70–81]; розшукується понад 100 злочинців; установлюються особистості десятків невпізнаних трупів тощо [3, с. 219–228].

Утім вимушені констатувати, що прийняття Закону України від 01.06.2010 «Про захист персональних даних», на фоні безумовної його значущості в контексті розвитку правової системи України, зумовило низку суттєвих проблем, пов'язаних як зі збереженням, так і з подальшою обробкою інформаційних масивів, що включають персональні дані осіб, які потрапляли або потрапляють в поле зору оперативних підрозділів ОВС. У чинній його редакції міститься ряд положень, які є сумнівними (на предмет універсальності щодо різних галузей діяльності) або не є конкретизованими. Зокрема, згідно до ст. 6 цього закону обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством. Не допускається обробка даних про фізичну особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

З одного боку, зрозуміло, що отримання згоди осіб, які становлять оперативний інтерес, або стосовно яких є одержана від конфіденційних джерел значуща інформація, щодо обробки їх персональних даних, або ж навіть їх повідомлення про наявності певного оперативного провадження по суті невілює саму ідею застосування ІАС в протидії злочинності.

З іншого, – сама нормативна основа для повноцінного використання ІАС є поки що недосконалою, такою, що не відповідає сучасним реаліям. На сьогодні одним з центральних нормативних актів, яким керуються підрозділи УІАЗ, є наказ МВС України від 12.10.2009 № 436 «Про затвердження Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України». Однак інформаційний ресурс, що мають сьогодні підрозділи УІАЗ, є значно ширшим, ніж передбачено п. 3 цього наказу. Тому з

урахуванням наявної позитивної практики застосування ІАС вкрай потрібне відповідне відомче або навіть законодавче підґрунтя.

Не менш актуальним є питання щодо відсутності в правовому полі вичерпного переліку відомостей, що відносяться до категорії персональних даних (Директива Європарламенту та Ради Європи 95/46/ЄС від 24.10.1995 «Про захист фізичних осіб при обробці персональних даних та про вільне переміщення таких даних», Закон України від 01.06.2010 «Про захист персональних даних», Рішення Конституційного Суду України від 30.10.1997 відносно офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та ін.). Його невизначеність для функціонування ІАС є певною «вибухівкою уповільненої дії», що в умовах однобічного розвитку національного законодавства в напряму захисту персональних даних не може не викликати занепокоєння.

Справа в тому, що підписання наказу Міністерства юстиції України від 22.06.2012 № 947/5 «Про затвердження Порядку здійснення Державною службою України з питань захисту персональних даних державного контролю за додержанням законодавства про захист персональних даних» запровадило послідовну організаційну основу відповідного контролю. У свою чергу, Законом України «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних», що набрав чинності 01.07.2012, внесено зміни до Кодексу України про адміністративні правопорушення та Кримінального кодексу України. Згідно цих змін за порушення законодавства про захист персональних даних передбачено адміністративну відповідальність. Відповідно доповнився перелік кримінальних дій щодо обігу конфіденційної інформації про особу. За вказаного підходу, яким буде «ставлення бюрократичної машини» до баз даних ІАС органів внутрішніх справ України, є питанням часу і «закулісних переговорів»!?

Сподіваємося, що вказана практика застосування ІАС ГУМВС України в Луганській області у протидії злочинності, а також викладені міркування щодо пов’язаних із цим проблем, викличуть інтерес у присутньої на семінарі наукової спільноти. Непрості питання щодо забезпечення конфіденційності використання баз даних ІАС, а також мови, на якій мають формуватися інформаційні масиви персональних даних, будуть обговорені в поточних бесідах за круглим столом.

Список літератури:

1. Бабічев Д. О. Інформаційно-аналітичне супроводження протидії злочинам загальнокримінальної спрямованості з використанням інтернет-мереж / Д. О. Бабічев // Співпраця поліції/міліції зі службами безпеки Інтернет-сайтів (аукціонів, соціальних мереж тощо) у боротьбі з інтернет-злочинністю на підставі національного законодавства та законодавства, яке діє у Європейському Союзі: тези доповідей міжнародної науково-практичної конференції (Хмельницький, 16–17 листоп. 2010 р.) / МВС України, УМВС України в Хмельницькій області. – Хмельницький : УМВС, 2010. – С. 2–6.

2. Гуславский В. С. Информационно-аналитическое обеспечение раскрытия и расследования пре ступлений : монография / В. С. Гуславский, Ю. А. Задорожний, Б. Г. Розовский. – Луганск : Изд-во «Элтон-2», 2008. – С. 53–57.

3. Задорожний Ю. А. Информационные технологии в ОРД: опыт и проблемы или проблемы и опыт? / Ю. А. Задорожний, Б. Г. Розовский // Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. – 2011. – № 4. – С. 219–228.

4. Задорожный А. Ю. Об информационных технологиях в ОРД с цифрами и доводами / А. Ю. Задорожный, Б. Г. Розовский // Додаток № 1 до Вісника Луганського державного університету внутрішніх справ імені Е. О. Дідоренка : у 2 ч. – 2012. – Ч. 2. – С. 70–81.

5. Современное оружие сотрудников органов внутренних дел: информационные технологии как ответ на вызовы времени : практ. пособие / Ю. А. Задорожный, А. Е. Трубкович, О. В. Калтырин и др. ; МВД Украины, Луган. гос. ун-т внутр. дел им. Э. А. Дидоренко. – Луганск : РИО ЛГУВД им. Э. А. Дидоренко, 2012. – 104 с.

Отримано 17.11.2012

УДК 343.85:343.3:343.341(477)

Володимир Олександрович БІЛЯЄВ
кандидат юридичних наук, доцент,
доцент кафедри оперативно-розшукової діяльності
Донецького юридичного інституту МВС України
Вадим Валерійович КЛЮС
кандидат юридичних наук, доцент,
старший викладач кафедри оперативно-розшукової діяльності
Донецького юридичного інституту МВС України

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ INTERNET-ТЕХНОЛОГІЙ ПІД ЧАС ПРОТИДІЇ ЕКСТРЕМІСТСЬКИМ ОРГАНІЗАЦІЯМ

Розглянуто сучасні можливості і загрози використання глобальних інформаційних технологій під час протидії діяльності організованих кримінальних структур екстремістської спрямованості.

Правоохоронними органами України протягом останніх десятиліть постійно фіксуються факти протиправної діяльності представників окремих етнічних груп та радикальних релігійних течій, які несуть загрозу для національної безпеки держави. Діяльність екстремістських організацій на території нашої держави може бути замаскована у формах легальної організації окремих спільнот: національно-культурні общини та діаспори, релігійні угруповання, що зовні не декларують радикальну ідеологічну спрямованість. Крім того, на території нашої держави поширилася діяльність тоталітарних сект, окремих деструктивних культів та вірувань, які несуть загрозу національній безпеці України.

Формуванню та функціонуванню в Україні організованих кримінальних структур екстремістської спрямованості сприяє низка чинників:

– активізація міграційних процесів, і передусім нелегальної міграції;

– соціальні, економічні та ментальні особливості організації життєдіяльності окремих етнічних громад (складні умови проживання, прагнення уникнути асиміляції, клановість, наявність кримінальних осередків прикриття тіньового бізнесу, тощо).

Останнім часом дедалі більш відчутним є вплив зовнішніх організованих структур на криміногенну ситуацію в державі. Нерідко під виглядом реалізації програм фінансової допомоги для будівництва

споруд релігійного призначення, духовних центрів, шкіл, просвітницьких закладів розгортається місіонерська діяльність екстремістських організацій. Занепокоєння викликають можлива політизація радикально-політичного руху, викликана останніми подіями у близькосхідному регіоні, який став ареною громадянських конфліктів, у тому числі й на релігійному ґрунті. Зовнішні події можуть впливати й на можливість поширення в Україні діяльності радикально налаштованих політичних та релігійних організацій.

Активність вищезазначених організацій виявляється у досить широкому спектрі протиправних діянь — від ритуальних вбивств на релігійному ґрунті до контрабанди стратегічно важливих сировинних товарів та вчинення злочинів у кредитно-фінансовій сфері.

Викликає занепокоєння загальна ситуація, що складається в державі. Зокрема, установлено факти проникнення до Криму представників радикальних мусульманських організацій «Сірі вовки», «Брати мусульмани», «Хизб ут тахрір» тощо. Зацікавленість мусульманським середовищем півострова виявляють і представники ваххабізму, який вважають релігійно-політичною базою ісламського фундаменталізму. До того через мережу Інтернет поширюється література радикальних релігійних та політичних організацій, у тому числі й українською мовою, у якій чітко простежується виправдання терористичних актів, вбивств, геноциду та інших особливо тяжких злочинів на релігійному ґрунті.

Потрібно погодитись з думкою, що ефективна діяльності оперативних підрозділів ОВС значною мірою залежить від інформаційного забезпечення та якісного користування ресурсами глобальної мережі Internet. Глобальна мережа Internet є публічним ресурсом глобального масштабу та елементом сучасного інформаційного суспільства. Використання її ресурсів в оперативно-розшуковій діяльності підвищує продуктивність праці, а також ефективність роботи оперативного працівника під час протидії злочинам [1].

Розглядаючи сучасні загрози в інформаційній сфері, К. О. Протасенко вважає, що стан забезпечення інформаційної безпеки України значною мірою залежить від моніторингу загроз в інформаційній сфері та використання при цьому сучасних інформаційних технологій, технічних і програмних засобів. Це дозволить значно зменшувати час, необхідний для пошуку та оброблення інформації, своєчасно виявляти реальні і потенційні загрози та аналізувати можливі напрями розвитку ситуації, з метою

прийняття обґрунтованих рішень щодо запобігання і нейтралізації загроз інформаційній безпеці Україні [2].

Необхідно також враховувати, що стрімкий розвиток інформаційної сфери є частиною не лише міжнародного співробітництва, але й суперництва. Адже не можна заперечувати того факту, що країни з високорозвиненою інформаційною інфраструктурою мають змогу формувати напрями діяльності інформаційних структур в інших країнах, впливають на їх подальший розвиток. Саме на етапі розвитку інформаційно-комунікаційних технологій, їх поширення на всіх ланках суспільної та економічної діяльності й виникають загрози національній безпеці країни [3]. Особливості протидії злочинам, що пов'язані з діяльністю екстремістських організацій полягають у необхідності врахування окремих факторів міжнародних відносин та впливу глобальних міжнародних інститутів. У ЗМІ нерідко поширюється інформація про причетність спеціальних служб окремих держав до створення та діяльності терористичних та екстремістських угруповань.

Враховуючи, що більшість сучасних універсальних операційних систем не виконують в повному обсязі вимоги до захисту автоматизованих систем для обробки конфіденційної інформації. Це значить, що, вони не можуть без використання додаткових засобів захисту застосовуватися для захисту конфіденційної інформації. При цьому слід зазначити, що основні проблеми захисту тут викликані не тим, що окремі вимоги до механізмів захисту не виконані в ОС, а принциповими причинами, які обумовлені реалізованою ОС концепцією захисту [4]. Фактично не вирішена проблема відповідальності учасників інформаційних відносин за правопорушення у сфері необґрунтованого використання конфіденційної інформації, за її якість та спричинення нею негативного інформаційного впливу.

Таким чином, використання Інтернет технологій під час протидії екстремістським організаціям є перспективним за умов вирішення низки проблем, які пов'язані з розглянутими вище сучасними інформаційними загрозами національній безпеці України.

Список використаних джерел

1. Сливенко В. Р. Використання ресурсів глобальної мережі Internet під час оперативного супроводження процесів державних закупівель підрозділами ДСБЕЗ / В. Р. Сливенко // Актуальні проблеми діяльності ДСБЕЗ та підготовка фахівців для її підрозділів : тези доп. та повід. – Л. : ЛьвДУВС, 2012.– С. 332–334.

2. Протасенко К. О. Моніторинг загроз інформаційній безпеці України / К. О. Протасенко // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-прак. конф., 22 берез. 2011 р. : у 2 ч. – К. : Наук.-вид. від. НА СБ України, 2011. – Ч. 1. – С. 132–135.

3. Чеховська М. М. Інформаційна безпека в умовах розбудови інформаційного суспільства в Україні / М. М. Чеховська // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-прак. конф., 22 берез. 2011 р. : у 2 ч. – К. : Наук.-вид. від. НА СБ України, 2011. – Ч. 1. – С. 165–166.

4. Блавацька Н. М. Проблема захищеності сучасних операційних систем класу автоматизованих систем, на яких обробляється інформація з обмеженим доступом / Н. М. Блавацька // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-прак. конф., 22 берез. 2011 р. : у 2 ч. – К. : Наук.-вид. від. НА СБ України, 2011. – Ч. 1. – С. 183–186.

Отримано 07.11.2012

УДК 681.3

Дмитро Сергійович БОНДАРЕНКО
курсант групи ФПТ-09-2 факультету психології, менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ
Костянтин Едуардович ПЕТРОВ
доктор технічних наук, професор,
начальник кафедри інформатики та інформаційних систем і технологій в діяльності ОВС факультету психології, менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ

РОЗРОБКА КОМПЛЕКСУ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ АКУСТИЧНИМ КАНАЛОМ

Представлено основні методи активного та пасивного захисту інформації. Розроблено комплекс захисту інформації від витоку акустичним каналом.

Інформація з обмеженим доступом, яка відтворюється та засіданнях, нарадах та інших подібних заходах, потребує захисту від

витоку акустичним каналом. Для цього застосовують як пасивні так і активні методи. Пасивні методи мають на меті послаблення акустичних сигналів на межі контрольованої зони до рівня, при якому неможливе їх виділення засобами розвідки на фоні природних шумів. При застосуванні активних методів створюються маскуючі акустичні, вібраційні завади для зменшення співвідношення сигнал/шум на границі контрольованої зони для унеможливлення їх виділення.

Одним з методів активного захисту інформації від витоку акустичним каналу є використання шумових сигналів. Найчастіше такий сигнал формують у вигляді «білого шуму» для перекриття усього частотного діапазону небезпечного сигналу, не враховуючи спектральну характеристику останнього. При цьому зрозуміло що потужність генератора використовується неефективно.

Ефективність значно зростає при використанні шумового сигналу з характеристиками подібними до характеристик небезпечного. Запропонований комплекс дозволяє значно спростити задачу формування маскуючих сигналів, так як в якості формувача мовоподібної завади використовується персональний комп'ютер. При цьому такий генератор може працювати у фоновому режимі і не заважатиме оператору виконувати основні штатні задачі.

В комплексі застосовується метод формування мовної завади, який полягає у формуванні випадкової послідовності імпульсів, в період слідування яких закладено характеристики спектральної щільності мовного сигналу.

В даному випадку комп'ютер, на якому встановлене необхідне програмне забезпечення, виконує роль формувача випадкової імпульсної послідовності. Ця послідовність через один з послідовних портів комп'ютера передається в лінію передачі. Така лінія протягується від до місця відтворення маскуючого сигналу.

Роль пристроїв відтворення маскуючого сигналу можуть виконувати малогабаритні акустичні колонки або п'єзовібратори, які встановлюються в місцях найбільш імовірного розміщення засобів акустичної розвідки.

Результати експериментальних досліджень дозволяють вважати, що застосування такого комплексу захисту інформації, що реалізує метод формування маскуючих сигналів на основі статистичних перетворень можна вважати перспективним, так як він дозволяє простими методами сформувати мовоподібний шумовий сигнал, та значно зменшити витрати на захист інформації.

Отримано 20.11.2012

УДК 35.078.3(075.8)

Лариса Володимирівна БОРИСОВА
кандидат юридичних наук, доцент,
доцент кафедри інформаційної безпеки факультету психології,
менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ
Юрій Миколайович ОНИЩЕНКО
викладач кафедри інформаційної безпеки факультету психології,
менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ
Роза Мартинівна БОЯДЖЯН
курсант групи ФПТ-09-3 факультету психології, менеджменту,
соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ

КРИПТОГРАФІЯ В УКРАЇНІ: ПРАВОВІ ОСНОВИ

Розглянуто правові основи криптографічного захисту інформації, шляхи його реалізації, типи засобів та вимоги до них.

Захист конфіденційної інформації, що циркулює (передається, приймається), обробляється та/або зберігається в спеціальних інформаційно-телекомунікаційних та інших системах, забезпечується застосуванням засобів криптографічного захисту інформації (КЗІ), а також виконанням відповідних організаційно-технічних та режимних заходів.

Основними нормативно-правовими актами, що регулюють використання криптографії в Україні, є закони «Про інформацію», «Про науково-технічну інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю», «Про Національну систему конфіденційного зв'язку» від 10 січня 2002 р. № 2919-ІІІ, «Про електронний цифровий підпис» [1–3].

Криптографічний захист інформації – вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Засоби КЗІ повинні розроблятися з урахуванням можливих загроз з боку середовища, у якому передбачається їх застосування. Розробник повинен передбачити організаційно-технічні заходи щодо захисту від несанкціонованого доступу, контролю цілісності програмного забезпечення засобу КЗІ, забезпечення надійного механізму тестування засобу КЗІ на правильність функціонування, а також обов'язкового блокування роботи засобу КЗІ у разі виявлення

користовуватися криптоалгоритми та
авними стандартами України або рекомендовані Департаментом. Для розробки засобів КЗІ використовується тільки ліцензійне програмне забезпечення. Залежно від способу реалізації розрізняють такі типи засобів КЗІ:

– апаратні засоби, алгоритм функціонування яких реалізовується в оптичних, механічних мікроелектронних або інших спеціалізованих пристроях та не може бути змінений під час експлуатації;

– апаратно-програмні засоби, алгоритм функціонування яких реалізується програмним забезпеченням, яке встановлюється під час виробництва засобу КЗІ у спеціальному запам'ятовуючому пристрої, виконується в ньому та може бути змінено лише під час виробництва;

– програмні засоби, алгоритм функціонування яких реалізується програмним забезпеченням, що функціонує під управлінням операційних систем електронно-обчислювальної техніки; окремі функції програмного засобу КЗІ можуть виконуватися апаратними або апаратно-програмними пристроями, що функціонують під управлінням програмного забезпечення засобу КЗІ [4].

Звичайно користувач апаратних засобів КЗІ не має доступу до змісту запам'ятовувальних елементів, що зберігають мікропрограми керування пристроєм, алгоритм функціонування пристрою змінюється тільки їх розробником або виробником.

Засоби КЗІ без уведених ключових даних мають *гриф обмеження доступу*, який відповідає грифу обмеження доступу опису криптосхеми. Гриф обмеження доступу засобів КЗІ з уведеними ключовими даними визначається грифом обмеження доступу ключових документів, але не нижче грифа обмеження доступу опису криптосхеми. Гриф обмеження доступу ключових документів, що використовуються для КЗІ, повинен відповідати грифу обмеження доступу інформації, що захищається.

Відповідно до ст. 9 Закону України «Про ліцензування певних видів господарської діяльності» від 1 червня 2000 р. № 1775-III, суб'єкти, які здійснюють розроблення, виробництво та експлуатацію

засобів КЗІ, визначають режим доступу до інформації про ці засоби, установлюють і підтримують відповідний режим безпеки з урахуванням вимог замовника та відповідно до нормативно-правових актів у сфері КЗІ [5].

Застосування засобів КЗІ під час міжнародного обміну інформацією здійснюється відповідно до законодавства та міжнародних угод (договорів) України.

На теперішній час методи і засоби криптографії використовують для забезпечення інформаційної безпеки не тільки держави, а й приватних осіб та організацій, реалізуючи різноманітні механізми захисту конфіденційності, цілісності, доступності та повноти інформації.

Список використаних джерел:

1. Про Національну систему конфіденційного зв'язку : закон України від 10 січ. 2002 р. № 2919-III // Відомості Верховної Ради України. – 2002. – № 15. – Ст. 103. – Редакція від 4 лют. 2009 р.

2. Про затвердження Положення про державний контроль за станом технічного захисту інформації [Електронний ресурс]: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16 трав. 2007 р. № 87. – Режим доступу: http://zakon.rada.gov.ua/laws/show/z0785-07. – Редакція від 27 січ. 2009 р.

3. Про захист інформації в інформаційно-телекомунікаційних системах : закон України від 5 лип. 1994 р. № 80/94-ВР // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286. – Редакція від 30 квіт. 2009 р.

4. Богуш В. М. Інформаційна безпека держави : навч. посіб. / В. М. Богуш, О. К. Юдін. – К. : МК-Прес, 2005. – 432 с.

5. Про ліцензування певних видів господарської діяльності : закон України від 1 черв. 2000 р. № 1775-III // Відомості Верховної Ради України. – 2000. – № 36. – Ст. 299. – Редакція від 17 листоп. 2010 р.

Отримано 19.11.2012

УДК 341.215.43

Іван Олександрович БОРОЗЕННИЙ
слухач магістратури
Харківського національного університету внутрішніх справ

ОКРЕМІ АСПЕКТИ ПОШУКУ ІНФОРМАЦІЇ ПРО ОСІБ, СХИЛЬНИХ ДО ВЧИНЕННЯ ЗЛОЧИНУ, У СОЦІАЛЬНИХ МЕРЕЖАХ ІНТЕРНЕТУ

Розглянуто окремі аспекти пошуку інформації про осіб, схильних до вчинення злочину, у соціальних мережах Інтернету.

Уявити сучасний світ без мережі Інтернет та сучасних [illegible] просто не можливо. Через Інтернет [illegible]нь купують продукти харчування, промислові та інші товари, квитки на культурні і розважальні заходи та на усі види транспорту, сплачують податки та штрафи, роблять регулярні комунальні платежі та сплачують відсотки по кредитах. За дослідженням, не мільйони, а мільярди людей з різною регулярністю спілкуються шляхом електронного листування. Навіть важко уявити, скільки би йшов звичайний лист, наприклад з Австралії до України!

Починаючи з 2004 року широкого розповсюдження набули такі Інтернет – ресурси, як соціальні мережі. Кожен день сотні мільйонів людей спілкуються, знайомляться, обмінюються фотографіями та відеозаписами, та навіть займаються комерційною діяльністю через різноманітні соціальні мережі, що нерідко залишається поза контролем податкової адміністрації та інших правоохоронних органів. Взірцем сучасних соціальних мереж у звичному для нас вигляді є соціальна мережа, розроблена у 2004 року в США Марком Цукербергом, яка має відому та впізнаваєму у всьому світі назву «Facebook» [1]. Сам Марк Цукерберг за створення цієї соціальної мережі, у 2010 році був визнаний Американським журналом «Times» людиною року, та став за її використання наймолодшим мільярдером. На пострадянському просторі, найвідомішими соціальними мережами є «Одноклассники» [2] та «Вконтакте» [3]. Обидві соціальні мережі, як «Одноклассники», так і «Вконтакте», на даний момент по своїм функціональним можливостям та структурі істотно відрізняються від соціальної мережі США «Facebook». Однак якщо порівняти сучасний вигляд та структуру соціальної мережі «Вконтакте» з первинним виглядом та структурою соціальної мережі «Facebook», то великих розбіжностей ми не побачимо. Але соціальна мережа «Facebook» була створена раніше за «Вконтакте».

Головний принцип, на якому ґрунтуються та використовуються майже усі існуючи соціальні мережі це добровільне створення користувачами своїх профілів та добровільне заповнення цих профілів інформацією про свою особистість. Зокрема, це інформація про особу користувача: місце, дату та рік його народження, місце проживання, навчальні заклади, в яких навчався чи навчається користувач, відомості про його родичів, відомості про соціальний та сімейний стан; вподобання користувача: улюблені книги, кінофільми, пісні, цитати відомих людей та інше; контактні дані користувача: номера телефонів, адрес електронної пошти, ім'я користувача в сервісі Skype, номер сервісу ICQ, адрес персонального Інтернет – сайту; особисті графічні та аудіо матеріали: фотографії та відеозаписи, на яких є сам користувач, або його родичі чи знайомі, цифрові зображення картин чи інші цифрові зображення, аудіо композиції, відео кліпи та відео ролики, котрі відображають, у тому числі естетичні смаки користувача. Всі ці дані користувачі соціальних мереж розміщують у своїх профілях добровільно, а не малозначним є те, що чим більше інформації про себе користувач розмістить в своєму профілі соціальної мережі, тим більший соціальний статус своєму профілю користувач здобуде за рахунок спілкування в мережі Інтернет. Тобто соціальні мережі стимулюють розміщення користувачами їх особистої інформації всередині самих соціальних мереж.

Велика кількість людей, які мають створені в соціальних мережах, тим самим відкриває вільний шлях для отримання інформації про їхню особу. Можна навести низку ефективних способів, завдяки яким можливо отримати достатньо велику кількість інформацію про особу, яка цікавить правоохоронців.

Для найбільш швидкого та повного пошуку необхідної інформації, треба знати справжні прізвище, ім'я та по-батькові особи, яка представляє для працівників ОВС оперативний інтерес. В даному випадку необхідно ввести вказані данні про особу в пошукову систему, наприклад «Google» [4]. Переглядаючи отримані пошукові результати, необхідно перевіряти якомога більше результатів, та перш за все необхідно перейти на сторінки профілів даної особи в соціальних мережах, якщо такі є. Для цього зручно буде послідовно ввести в пошуковій системі прізвище, ім'я та по-батькові особи, та назву соціальної мережі, наприклад: «Іваненко Іван Іванович facebook», після перевірки результатів – «Іваненко Іван Іванович вконтакте», і так само далі з іншими соціальними мережами.

Якщо є відомості про особисті дані особи лише частково, в подальшому доцільно буде застосувати ще й інші два способи пошуку.

Зокрема: 1) необхідно ввести в пошукову систему спочатку всю відому інформацію про особу та назву соціальної мережі. Наприклад: «Іваненко Іван Іванович 23.03.1986 +380951882999 Харків Dorosh@mail.ru Facebook». Якщо це не принесло бажаних результатів, то в подальшому доцільно буде ввести по черзі частку інформації про особу, та назву соціальної мережі. Це пов'язано з тим, що особа, яка цікавить правоохоронців, може створювати в соціальних мережах профілі з іншими прізвищами та частково, або повністю зміненими особистими даними. Наприклад працівникам ОВС відомі дата народження та номер телефону особи, про яку необхідно отримати певну інформацію, отже для цього доцільно використати відомі дані, для чого необхідно ввести в пошуковій системі: «23.03.1986 +380951882999 одноклассники», потім «23.03.1986 одноклассники», потім «+380951882999 одноклассники», потім «23.03.1986 +380951882999 вконтакте», потім «23.03.1986 вконтакте», і так далі; 2) пошук може вестись всередині самих соціальних мереж, для чого необхідно створити власний профіль. Цей метод дуже доцільний завдяки тому, що у кожній соціальній мережі є дуже функціональна система пошуку з багатьма фільтрами. В системах пошуку всередині соціальних мереж можна шукати особу тільки по прізвищу, чи по віку, чи по даті народження, чи по місту народження, чи по ставленню, наприклад до вживання спиртних напоїв. Список фільтрів пошуку, які можна використати при пошуку певної особи є дуже великий.

Дуже корисним для правоохоронців може бути спосіб перевірки діяльності особи в мережі Інтернет, коли відомі справжні та заповнені відповідною інформацією профілі даної особи в соціальних мережах. Наприклад достатньо використовувати адрес електронної пошти, номер ICQ, ім'я в сервісі Skype та телефонний номер особи, яка цікавить правоохоронців, а також добавляючи у подальшому ключові слова при пошуку. Це пов'язано із тим, що левова частка користувачів Інтернету використовує різноманітні вузько направлені Інтернет – ресурси для спілкування, під час якого вони спілкуються під вигаданими прізвищами, наприклад: Scorpio, TNT, Master. В цій діяльності можна навести приклад пошукового запиту, якщо завданням є пошук особи по форумах, Інтернет – магазинах, та для вивчення її листування. Для прикладу, правоохоронцям відомі такі дані про особу: адрес електронної пошти – Bada@darts.ru, номер ICQ – 567652987, ім'я в сервісі Skype – Filat, телефонний номер – +380667772332. Тоді доцільним буде використання таких пошукових запитів: «Bada@ddt.ru 567652987 Filat +380667772332 форум», далі «Bada@ddt.ru 567652987 Filat +380667772332 інтернет магазин», далі

«Bada@ddt.ru 567652987 Filat +380667772332 купити», далі «Bada@ddt.ru 567652987 Filat +380667772332 продати», а ще далі інші слова, чи речення, які часто використовує при спілкуванні особа, чи вказуючи словосполучення, що цікавлять правоохоронців.

Можна зробити висновок, що для пошуку інформації про осіб схильних до вчинення злочину, є наявна можливість правоохоронцям розширити пошук необхідної інформації використовуючи соціальні комп'ютерні мережі. Втім підняті питання не є остаточними і підлягають додатковому дослідженню або науковому вивченню.

Список використаних джерел:

1. Соціальна мережа «Facebook» [Електронний ресурс]. – Режим доступу: http://www.facebook.com.

2. Соціальна мережа «Одноклассники» [Електронний ресурс]. – Режим доступу: http://www.odnoklassniki.ru.

3. Соціальна мережа «Вконтакте» [Електронний ресурс]. – Режим доступу: http://www.vk.com.

4. Пошукова система «Google» [Електронний ресурс]. – Режим доступу: http://www.google.com.

Отримано 20.11.2012

УДК 343.13

Максим Миколайович БУГАЙ
курсант групи ІКМ 09-5 навчально-наукового інституту
підготовки фахівців кримінальної міліції
Харківського національного університету внутрішніх справ

ЗАСТОСУВАННЯ ЕЛЕКТРОННИХ ЗАСОБІВ КОНТРОЛЮ ЗА НОВИМ КРИМІНАЛЬНО-ПРОЦЕСУАЛЬНИМ ЗАКОНОДАВСТВОМ

Проаналізовано порядок застосування електронних засобів контролю і нагляду за підозрюваними та обвинуваченими в зв'язку з набуттям чинності новим Кримінальним процесуальним кодексом України.

Головною подією 2012 року в сфері кримінального процесу і, мабуть, юриспруденції як такої стало прийняття Верховною Радою України нового Кримінального процесуального кодексу України (далі

– КПК України), який за словами розробників, створений з єдиною метою служити і захищати [1, с. 55].

Новим кроком на шляху гуманізації кримінального провадження в Україні стало право застосування уповноваженими органами державної влади електронних засобів контролю (далі – ЕЗК). Адже ввід ЕЗК допоможе не тільки розгрузити наші переповнені слідчі ізолятори, а й дозволить обвинуваченому або підозрюваному залишатись вдома, працювати, не залишати сім'ю.

Перший пристрій електронного моніторингу був розроблений в США в середині 1960-х років. Своє законодавче закріплення пристрій електронного моніторингу отримав в 1968 році, коли був прийнятий Федеральний Закон США «Про електронний нагляд», однак активно електронні браслети застосовуються в Західній Європі і США лише з 1995 року. Основне призначення цих пристроїв полягає в контролі умовно засуджених або осіб, які знаходяться під домашнім арештом, а

гермін за тяжкі злочини [2, с. 150].

України дано визначення поняття

засобів контролю» (застосування електронних засобів контролю полягає у закріпленні на тілі підозрюваного, обвинуваченого пристрою, який дає змогу відслідковувати та фіксувати його місцезнаходження [3, с. 102]), суб'єктів які мають право їх застосовувати та порядку застосування.

Зупинимось детальніше на порядку застосування ЕЗК, він регламентується наказом МВС України «Про затвердження Положення про порядок застосування електронних засобів контролю» від 09.08.2012 № 696.

Зокрема в даному відомчому нормативно-правовому акті дано визначення таким основним поняттям:

Електронні засоби контролю – електронний браслет, електронний моніторинг, мобільний контрольний пристрій, мобільний пульт моніторингу, персональний трекер, ретранслятор, сервер моніторингу, стаціонарний пульт моніторингу, стаціонарний контрольний пристрій.

Електронний браслет – електронний пристрій, виконаний у вигляді браслета, що закріплюється на тілі підозрюваного або обвинуваченого з метою його дистанційної ідентифікації та відстеження місцезнаходження, який призначений для носіння на тілі і захищений від самостійного знімання, пошкодження або іншого втручання в його роботу з метою ухилення від контролю та має сигналізувати про спробу особи здійснити такі дії.

Електронний моніторинг – система заходів контролю за місцезнаходженням осіб, які зобов'язані слідчим суддею, судом носити ЕЗК [4].

Отримавши ухвалу слідчого судді, суду про обрання запобіжного заходу, не пов'язаного з позбавленням волі, якою на підозрюваного (обвинуваченого) покладено зобов'язання носити ЕЗК, слідчий або співробітник оперативного підрозділу за його дорученням зобов'язаний негайно передати таку ухвалу для виконання до уповноваженого підрозділу за місцем реєстрації або проживання підозрюваного (обвинуваченого).

Уповноважений підрозділ органів внутрішніх справ, який здійснює забезпечення електронного контролю за місцезнаходженням підозрюваного (обвинуваченого) визначається Міністром внутрішніх справ України.

Ознайомлення з правилами користування пристроєм, технікою безпеки поводження з ним та наслідки його зняття або неправомірного втручання в його роботу з метою ухилення від контролю, оформлюються протоколом про оголошення підозрюваному (обвинуваченому) ухвали слідчого судді, суду щодо застосування запобіжного заходу та врученням її копії та протоколом про роз'яснення підозрюваному (обвинуваченому) правил користування електронними засобами контролю.

Отже справа залишилась за малим успішно реалізувати ці безумовно корисні та актуальні ідеї.

Список використаних джерел:

1. Демин Д. С. Избрание меры пресечения: правила игры по новому УПК / Д. С. Демин // «ЮРИСТ & ЗАКОН». – 2012. – № 73. – С. 54–56.

2. Шаталов Ю. М. Применение электронного мониторинга при исполнении домашнего ареста в Венгрии / Ю. М. Шаталов // Вестник Владимирского юридического института. – 2009. – № 1. – С. 218–221.

3. Кримінальний процесуальний кодекс України. Закон України «Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Кримінального процесуального кодексу України». – Х. : Одіссей, 2012. – 360 с.

4. Про затвердження Положення про порядок застосування електронних засобів контролю : наказ МВС України від 09.08.2012 № 696 : зареєстр. в М-ві юстиції України 05.09.2012 за № 1503/21815 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/z1503-12.

Отримано 30.11.2012

УДК 343.97

Богдан Анатолійович БУРБЕЛО
викладач кафедри криміналістики, судової медицини та психіатрії
факультету з підготовки слідчих
Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ ІННОВАЦІЙ В РОЗКРИТТІ І РОЗСЛІДУВАННІ ЗЛОЧИНІВ

Розглянуто використання інновацій в розкритті і розслідуванні злочинів.

сті боротьби зі злочинністю диктує
вих засобів і шляхів одержання і
нтуючої інформації. Вирішення цього завдання безпосередньо пов´язане з інтеграцією в криміналістику сучасних досягнень природничих і гуманітарних наук.

Виявляється, що будь-який запозичений і адаптований криміналістикою метод інших наук можна розглядати як нетрадиційний. Більш того, цей метод може тривалий час перебувати в так званому «пограничному просторі» до тих пір, поки криміналістична практика і теорія не виконають функції суворого «відділу технічного контролю» та не приймуть його в якості спеціального методу іншої науки, адаптованого для вирішення завдань криміналістики, або не відкинуть його як метод ненадійний і який не забезпечує належного вирішення криміналістичних завдань.

Одними із нетрадиційних засобів розкриття злочинів можуть бути застосування гіпнозу і поліграфа при отриманні інформації від потерпілих, свідків, підозрюваного, обвинуваченого. На нашу думку застосування гіпнозу доцільно, лише коли свідок або потерпілий хоче допомогти слідству у встановленні істини у справі, але з тих чи інших причин (наприклад, стресовий стан у результаті вибуху) не може пригадати і відтворити побачену подію або риси людини. Другою умовою використання допомоги спеціаліста – гіпнолога є наявність добровільної згоди потерпілого чи свідка дати свідчення. Застосування гіпнозу до підозрюваного чи обвинуваченого, на наш погляд,

неприпустимо. Сеанси гіпнозу можуть проводити тільки спеціально підготовлені особи - психіатри і психологи.

Певні успіхи в боротьбі зі злочинністю досягнуті в Росії, США з впровадженням в практику розслідування психофізіологічних досліджень на так званому детекторі брехні. Методика виявлення неправдивих свідчень за допомогою поліграфа є лише одним з напрямків можливого використання психофізіологічних досліджень у криміналістиці та слідчо-оперативній практиці. Поліграф являє собою комплекс приладів для синхронної реєстрації різних фізіологічних функцій людського організму: ритму і глибини дихання, ритму серцебиття, зміни тиску крові, електропровідності шкіри, величини м'язової напруги. Сутність методу опитування на поліграфі полягає в пред'явленні опитуваному ряду питань, на які він дає відповіді, при цьому прилад фіксує зміна фізіологічних показників, що відбивається на поліграф. На основі конкретних фізіологічних реакцій, відбитих на носії при реєстрації показників, відбувається побудова висновків щодо проведеного дослідження.

У науковій літературі неодноразово висловлювалася думка про необхідність застосування поліграфічного методу в рамках судово-психологічної експертизи, що дозволить використовувати отримані результати в якості доказів у кримінальному судочинстві [2, с. 46]. Ми підтримуємо цю точку зору, і вважаємо, що відомості, отримані в результаті застосування поліграфічного методу, можуть використовуватися не тільки в оперативно-розшукової діяльності, але і в тактиці слідчих дій, в процесі доказування у кримінальному провадженні.

Однак найсучасніші поліграфи, на думку деяких вчених і практиків, не гарантують достовірність висновку. Один з факторів, що впливають на можливі помилки, полягає в обов'язковому отриманні згоди особи на проведення перевірки на детекторі брехні. Тому досвідчений терорист чи інший професійно підготовлений злочинець може уникнути викриття, використавши законне право на відмову від тестової перевірки; крім того, багато підозрюваних, особливо з числа терористів, найманих убивць, а тим більше штатні співробітники розвідувальних служб проходять спеціальну антиполіграфічну підготовку і можуть обдурити детектор брехні і оператора. Але використання поліграфа в правоохоронній діяльності Росії, Польщі, США виправдовує себе. Співробітники Інституту криміналістики ФСБ Росії вважають, що «людина перед поліграфом беззахисна» [6, с. 117].

Останнім часом з'явилися принципово нові науково-технічні розробки поліграфічних комплексів. Так, в США вченим науково-

дослідних центрів Mayo Clinic і Honeywell Laboratories вдалося створити спеціальну високочутливу камеру, яка фіксує миттєвий приплив крові до очей суб'єкта. Це є рефлексною відповіддю на поставлені оператором незручні або викриваючи питання. Дуже важливою обставиною, що характеризує особливості використання цього поліграфа, є можливість безконтактної роботи апарату, що уловлює воістину мікроскопічні зміни температури шкіри. Відсутність безпосереднього контакту з тілом людини дозволить використовувати в оперативно-розшукових цілях високочутливий детектор брехні негласно, без повідомлення про це перевіряється і без отримання його згоди, що значно збільшить ефективність роботи та надійність результатів.

У зв'язку з введенням поліграфічних пристроїв в діяльність правоохоронних органів є безліч вимог та обмежень, супутніх використання поліграфа. Зокрема вони стосуються, що на сьогодні в Україні відсутня така відомча нормативна база, що регламентувала б застосування поліграфа органами внутрішніх справ, відсутність національної школи із підготовки поліграфологів. Тому інформація, отримана під гіпнозом, не має, так само як і в процесі опитування з використанням поліграфа, доказового значення. Разом з тим докладне опитування може дати важливі для розслідування злочинів орієнтуючі відомості, які можуть використовуватися для побудови та перевірки версій, прийняття рішення при виборі тактичних прийомів чи напрямку розслідування злочинів.

Список використаних джерел:

1. Варламов В. А. История возникновения детектора лжи [Електорнний ресурс] / В. А. Варламов // Труды Академика Варламова – 2007. – Режим доступу: http://www.omegaconsulting.ru/varlamov_01.htm.

2. Комиссаров В. И. Использование полиграфа в борьбе с преступностью / В. И. Комиссаров // Законность. – 1995. – № 11. – С. 43–47.

3. Корчагин М. Н. Применение инструментального (полиграфного) метода для познания идеальных следов преступления (психологические аспекты проблемы) / М. Н. Корчагин // Психопедагогика в правоохранительных органах. – 1997. – № 1 (5). – С. 73–74.

4. Скрыпников А. И. Нетрадиционные методы получения информации в раскрытии преступлений / А. И. Скрыпников, Л. П. Гримак // Психопедагогика в правоохранительных органах. – 1997. – № 1. – С. 75–77.

5. Филонов Л. Б. Психологические приемы допроса обвиняемого / Л. Б. Филонов, В. И. Давыдов // Вопросы психологи. – 1966. – № 6. – С. 111–122.

6. Холодный Ю. И. Применение полиграфа при профилактике, раскрытии и расследовании преступлений : пособие / Ю. И. Холодный. – М., 2000. – 160 с.

Отримано 15.11.2012

УДК 65.012.8+004

Андрій Вікторович ВІНАКОВ
начальник відділу нагляду за додержанням законів органами внутрішніх справ при провадженні оперативно-розшукової діяльності прокуратури Харківської області

ЗМІСТ ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ ПІДРОЗДІЛІВ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В СУЧАСНИХ УМОВАХ

Проаналізовано зміст підготовки фахівців, задіяних у боротьбі з кіберзлочинністю, розкрито важливість комплексної підготовки останніх в умовах запровадження у дію положень нового Кримінального процесуального кодексу України.

У Посланні Президента України до Верховної Ради України 2011 року було наголошено, що вияви кіберзлочинності у вигляді хакерських атак на комп'ютерні системи банківських та інших фінансових установ, крадіжок електронних коштів, широкого використання мережі Інтернет для наркоторгівлі, торгівлі людьми, інших протиправних дій стають реальною загрозою національній безпеці. Кібернетичний простір дедалі більше стає полем протистояння між окремими державами, джерелом небезпек для національної інфраструктури з боку військових і розвідувальних структур, організованих злочинних угруповань, що прагнуть використовувати Інтернет і новітні інформаційно-комп'ютерні технології для досягнення своїх підривних або кримінальних цілей [1].

У сучасних умовах запровадження в дію положень Кримінального процесуального кодексу України від 13.04.2012 [2]

набуває нового змісту підготовка фахівців для підрозділів боротьби з кіберзлочинністю.

У зв'язку з набуттям нових повноважень слідчими, а за їх дорученням оперативними працівниками, необхідно по новому підходити до підготовки відповідних фахівців. Значна частина нових повноважень, зокрема, у сфері проведення окремих слідчих та негласних слідчих (розшукових) дій, пов'язана із застосуванням технічних засобів. Особливо актуальним це стає для працівників ОВС, задіяних у боротьбі з кіберзлочинністю, які окрім володіння відповідними юридичними знаннями повинні мати навички роботи з комп'ютерною технікою та досконало розбиратися у механізмі вчинення кіберзлочинів.

Тому важливою є комплексна підготовка таких працівників, яка базуватиметься на принципі поєднання технічних та юридичних

у фахівців, задіяних у боротьбі з

ю у Харківському національному

Фахівці за спеціалізацією «Боротьба з кіберзлочинністю» готуватимуться за двома напрямами підготовки: «Правознавство» та «Системи технічного захисту інформації».

За першим напрямом підготовки варіативна частина плану підготовки включатиме курси спеціалізації з технічним нахилом або такі, що охоплюватимуть одночасно технічні та юридичні знання. Це такі дисципліни як: «Основи боротьби з кіберзлочинністю», «Попередження та розкриття кіберзлочинів», «Оперативно-технічні засоби», «Оперативно-технічні заходи та негласні слідчі (розшукові) дії», «Безпека інформаційних та комунікаційних систем», «Основи обробки та передачі інформації», «Основи програмування та алгоритмічні мови», «Застосування комп'ютерних технологій в ОВС», «Інформаційне забезпечення ОВС», «Основи web-технологій баз та банків даних» тощо.

За другим напрямом підготовки – технічним уведено додаткові варіативні курси: «Правознавство», «Основи криміналістики», «Кримінальне право», «Кримінальний процес», «Судова експертологія», «Адміністративна діяльність ОВС», «Криміналістична інформатика» тощо.

Така стратегія дозволить комплексно підійти до питання підготовки фахівців, задіяних у боротьбі з кіберзлочинністю, та створить передумови для якісного поповнення кадрового складу органів внутрішніх справ України в умовах збільшення кількості високоінтелектуальних злочинів.

Список використаних джерел:

1. Модернізація України – наш стратегічний вибір : Послання Президента України до Верховної Ради України : 2011 рік від 07.04.2011 [Електронний ресурс] / Ліга: Закон Еліт : Мережна версія.
2. Кримінальний процесуальний кодекс України : від 13.04.2012 // Голос України. – 19.05.2012. – № 90–91.

Отримано 10.11.2012

—

УДК 343.982.33

Аліна Едуардівна ВОЛКОВА
старший експерт Науково-дослідного експертно-криміналістичного центру УМВС України в Сумській області

ВИКОРИСТАННЯ КРИМІНАЛІСТИЧНИХ КОЛЕКЦІЙ В ЕКСПЕРТНІЙ ПРОФІЛАКТИЦІ ЗЛОЧИНІВ

Розглянуті основні напрямки використання криміналістичних обліків з метою профілактики злочинів. Проаналізовані можливості деяких видів колекцій для вироблення відповідних рекомендацій.

В даний час в підрозділах експертної служби МВС України ведуться різноманітні види оперативних та інформаційно-довідкових криміналістичних картотек і колекцій. Їх використання орієнтоване, перш за все, на розкриття злочинів, а також інформаційно-довідкове забезпечення, як експертних досліджень, так і процесу розслідування злочинів. Проведений аналіз існуючих видів криміналістичних колекцій дозволяє визначити ряд напрямків їх використання в цілях запобігання деяких видів злочинів, а також для виявлення та усунення обставин, що сприяють їх вчиненню.

У профілактичних цілях можуть використовуватися балістичні колекції, наприклад кулегільзотека зброї, що перебуває у власності громадян і організацій. В експертних підрозділах МВС організований відстріл такої зброї, так як воно може бути застосоване у кримінальних цілях, що є потужним засобом профілактичного впливу на власників зброї, інформованих про цілі і завдання постановки на криміналістичний облік зразків стріляних куль і гільз.

Іншим напрямком використання балістичного обліку є виявлення технічних недоробок в конструкції реєстрованих об'єктів, що створюють сприятливі умови для вчинення злочинів. Так, в інформаційних масивах акумулюються відомості про різні моделі зброї заводського виготовлення, в основному газового і сигнального, з якого шляхом переробки виготовляється зброя для стрільби бойовими патронами. Такий криміналістичний облік дозволяє виявити найбільш часто використовувані для цих цілей моделі, встановити ті їх конструктивні особливості, які сприяють переробці і виробляти відповідні профілактичні пропозиції.

Колекції саморобної та переробленої вогнепальної зброї сприяють також ефективному встановленню джерел походження (виготовлення) зразків зброї, що надходять. Експертні дослідження дозволяють виявити ознаки, характерні для одного і того ж промислового устаткування і зробити висновок про єдине джерело виготовлення з прийняттям відповідних превентивних заходів.

ожуть бути реалізовані можливості
ді ведення довідкових обліків зразків
саморобного виготовлення, а також колекції саморобних вибухових пристроїв. Криміналістичні обліки пломб та інших контрольних пристроїв дають можливість розробляти нові їх види, підвищувати ступінь захищеності від несанкціонованого доступу, вносити зміни в правила пломбування та виробляти інші профілактичні заходи. Аналогічним чином використовується трасологічна колекція замків для вироблення рекомендацій щодо їх надійності, підвищенню таємності. Висока ефективність експертної профілактики в цьому випадку досягається шляхом поміщення в засобах масової інформації матеріалів з аналізом надійності замків, що надходять у торговельну мережу, з рекомендаціями по їх установці і підвищенню технічної укріпленості дверей.

У профілактичних цілях використовуються і такі криміналістичні картотеки та колекції, як колекції зразків почерків і підписів, відтисків штампів і печаток нотаріусів, лікарів, співробітників підрозділів ДАІ, тобто тих працівників та установ, підписи та печатки яких найчастіше підробляються. Систематичне ведення зразків бланків поліграфічної продукції дозволяє запобігати витоку бланків та їх підробку. Ведення картотеки підроблених документів дозволяє виявляти найбільш поширені види підробок і на основі відповідного аналізу виробляти профілактичні пропозиції, спрямовані на посилення захисних властивостей документів суворої звітності, а також поліпшення якості матеріалів документів: паперу,

барвників, чорнил. Довідкові колекції зразків лікеро-горілчаної продукції, зразків спирту заводів-виробників можуть працювати на усунення причин і умов фальсифікації горілки. Цим же цілям можуть служити зразки етикеток вино-горілчаної продукції, зразки ковпачків і способів закупорювання пляшок. Аналіз показує, що з метою попередження злочинів пов'язаних з фальсифікацією нафтопродуктів дуже ефективно можуть використовуватися колекції зразків бензинів. Сам факт їх наявності в експертних підрозділах МВС та можливість проведення регулярних перевірок якості палива на заправках є стримуючим чинником зловживань у цій сфері. Попередження злочинів може здійснюватися активним використанням криміналістичних обліків зразків наркотичних засобів і прекурсорів, об'єктів інтелектуальної власності, колекцій харчових продуктів, рецептур, ДСТУ, технологічних карт на виробництво продовольчих товарів, картотек маркувальних позначень, торгових марок, етикеток підприємств-виробників харчових продуктів, баз даних правовласників на аудіовізуальні твори та іншу ліцензійну продукцію.

Як приклад позитивного використання колекцій для попередження злочинів відзначимо, що в ДНДЕКЦ МВС створена довідкова база даних по іменним маркерам, які є у підривників країни. Створення такої довідкової колекції призвело до значного скорочення кількості розкрадань засобів підривання.

Таким чином, за допомогою інформаційно-довідкових обліків можна отримувати важливу інформацію про причини і умови, що сприяють вчиненню злочинів, допомагають слідчим органам приймати необхідні профілактичні заходи.

Отримано 08.11.2012

УДК 343.97

Іван Андрійович ГРАБАЗІЙ
викладач кафедри оперативно-розшукової діяльності
навчально-наукового інституту підготовки фахівців кримінальної міліції
Харківський національний університет внутрішніх справ

ІНФОРМАЦІЙНА ВЗАЄМОДІЯ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ ОВС З ІНШИМИ ПРАВООХОРОННИМИ ОРГАНАМИ УКРАЇНИ ПІД ЧАС ВИЯВЛЕННЯ ОРГАНІЗОВАНИХ ГРУП, ЯКІ ЗАЙМАЮТЬСЯ ТОРГІВЛЕЮ ЛЮДЬМИ

Представлено напрямки інформаційної взаємодії оперативних підрозділів ОВС з іншими правоохоронними органами України під час виявлення організованих груп, які займаються торгівлею людьми.

Розподіл процесу документування злочинної діяльності організованих груп, які займаються торгівлею людьми на етапи, дає можливість визначити основні ефективні форми взаємодії та напрямки її удосконалення залежно від кола завдань, що вирішуються.

Так, на початковому етапі, під час виявлення організованих груп, які займаються торгівлею людьми основними є такі завдання:

– виявлення можливих об'єктів торгівлі людьми та осіб, які потерпіли від злочинної діяльності організованих груп;

підготовки та здійснення злочинної

нної діяльності організованих груп та їхніх конкретних членів, що займаються торгівлею людьми, та конкретизація форм і видів торгівлі людьми;

– конкретизація виду злочинної діяльності: експлуатація (сексуальна, рабство, примусова «потогінна» або «інтелектуальна» праця (наукова, творча тощо); використання у порнобізнесі; проведення дослідів над людиною без її згоди; злочинна діяльність; використання у збройних конфліктах та етноконфесійних протистояннях тощо; вилучення органів та іншого матеріалу.

Забезпечувальними завданнями є:

– вивчення потерпілих та можливих джерел інформації ы свідків злочинної діяльності ОЗУ з їх оточення;

– встановлення кола та напрямку пошуку інформації про злочинну діяльність розроблюваних;

– встановлення психологічного контакту з можливими об'єктами торгівлі людьми та потерпілими.

Основною формою взаємодії на цьому етапі є інформаційна. Як показало дослідження, обмін оперативною інформацією в ході документування злочинної діяльності злочинних груп, які займаються торгівлею людьми у 32,1 % випадків з оперативними підрозділами СБУ, у 58,9 % – з оперативними підрозділами ДПСУ. Наведені дані свідчать про недооцінку використання оперативними працівниками цієї форми взаємодії, тому необхідно вдосконалити механізм обміну інформації у режимі «on-line», що дозволить більш повно вирішувати завдання оперативної розробки організованих угруповань, які займаються торгівлею людьми.

Так, відповідно до ст. 24 Закону України «Про Службу безпеки України», обов'язками СБУ є: надання допомоги органам МВС та іншим правоохоронним органам у боротьбі з торгівлею людьми; неодмінний обмін оперативною інформацією про злочинну діяльність, пов'язану з торгівлею людьми; розробка та проведення спільних заходів з протидії злочинним об'єднанням, що займаються торгівлею людьми, з використанням оперативних та інших можливостей, а також участь у розробці заходів та у вирішенні питань, що стосуються в'їзду осіб в Україну й виїзду їх за кордон, перебування іноземців на території України, дотримання прикордонного режиму та митних правил.

З метою виявлення ознак злочинної діяльності та встановлення об'єктів – осіб торгівлі людьми отримується інформація про перетин кордону об'єктами-особами та трафікерами від компетентних оперативних підрозділів Державної прикордонної служби України. Шляхом удосконалення цієї форми взаємодії є запровадження каналу доступу до інформаційних масивів ДПС України у режимі «on-line».

Інформаційна взаємодія з Державною митною службою (банки даних: всеукраїнський класифікатор митних ліцензійних складів; реєстр суб'єктів, які здійснюють брокерську діяльність; реєстр суб'єктів зовнішньоекономічної діяльності, які користуються особливим режимом сприяння; перелік та місце розташування установ, що здійснюють безмитну торгівлю товарами; інформаційні масиви переміщення вантажів і фізичних осіб через митний кордон) дозволяє встановити юридичних осіб, транспортні засоби яких використовувалися або можуть використовуватися для нелегального перевезення людей.

Державна податкова адміністрація та податкова міліція за рахунок своїх інформаційних масивів (база даних суб'єкта

підприємницької діяльності: назва та юридична адреса СПД, дата реєстрації, код єдиного державного реєстру підприємства; дані про засновників та інвесторів, директора та бухгалтера СПД; розрахункові рахунки, дати їх відкриття, МФО банківської установи; щоквартальна та щорічна звітність, дата ліквідації СПД; база даних 1-ДР – індивідуальні номери платників податків – фізичних осіб: установча інформація на кожного жителя, який одержав індивідуальний номер; база даних 8-ДР – відомості про платників прибуткового податку, що надається щомісяця до ДПА бухгалтерією кожного підприємства та організації: місце роботи конкретної фізичної особи та сума утриманого з неї прибуткового податку) під час обміну інформацією дозволяє встановити фірми, які займаються торгівлею людьми та можуть забезпечувати відмивання коштів від торгівлі людьми та входять до інфраструктури злочинної групи. Означена інформація може бути підтверджена узагальненими матеріалами центрального органу виконавчої влади із спеціальним статусом з питань фінансового моніторингу, отриманих в установленому законом порядку.

Узагальнюючи викладене, можемо констатувати, що на попередньому етапі одним із напрямків удосконалення взаємодії є запровадження каналу доступу до інформаційних масивів СБУ, ДПСУ, ДПАУ, Інтерполу у режимі «on-line» та формування відповідно аналітичних банків у державі та регіоні.

Список використаних джерел:

1. Про затвердження Положення про органи досудового розслідування Міністерства внутрішніх справ України : наказ МВС України від 09.08.2012 № 686. – К. : РВВ МВС України, 2012. – 14 с.

2. Бандурка О. М. Оперативно-розшукова діяльність. Ч. І : підручник / О. М. Бандурка. – Х. : Вид-во Нац. ун-ту внутр. справ, 2002. – 336 с.

3. Будко Т. В. Теорія та практика дослідження мовленнєвих текстуальних джерел інформації у діяльності СБ України : автореф. дис. на здоб. наук. ступеня д-ра юрид. наук : спец. 21.07.01 «Оперативно-розшукова діяльність»/ Будко Т. В. – К., 2004. – 34 с.

4. Грабазій І. А. Шляхи удосконалення взаємодії у попередженні та розкритті торгівлі людьми / І. А. Грабазій // Теорія та практика кримінального судочинства : матеріали наук-практ. конф. (Харків, 20 трав. 2011 р.). – Х., 2010. – С. 164–166.

Отримано 29.11.2012

УДК 343.97

Михайло Васильович ГРУБИЙ
ад'юнкт кафедри оперативно-розшукової діяльності
Національна академія внутрішніх справ

ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ СФЕРИ ВИСОКИХ ТЕХНОЛОГІЙ У РОЗСЛІДУВАННІ СЕРІЙНИХ КВАРТИРНИХ КРАДІЖОК

Присвячено використанню можливостей сфери високих технологій у розслідуванні серійних квартирних крадіжок під час створення єдиної інформаційно-телекомунікаційної системи правоохоронних органів.

Особливості розслідування серійних квартирних крадіжок з використанням можливостей сфери високих технологій привертає увагу дослідників [1]. Утім вітчизняне кримінально-процесуальне законодавство не враховує потенційні можливості використання телекомунікаційних технологій при їх розслідуванні.

Застосування інформаційних технологій у кримінальному

рішено при виконанні будь-яких
ичайному, так і в інтерактивному
ночасним веденням документообігу і
діловодства на паперових та електронних носіях, з яких для учасників процесу у випадках, передбачених процесуальним законодавством, виготовляються автентичні копії процесуальних документів.

Специфіка виявлення та проведення слідчих дій в Інтернет-просторі вимагає розробки спеціальних криміналістичних методик, глибоких знань сучасних інформаційних технологій, наявності відповідного апаратного та програмного забезпечення, налагодження міжнародного співробітництва для розслідування серійних квартирних крадіжок та ліквідації злочинних угруповань.

Для виявлення схеми вчинення злочину є потреба у застосуванні певних технологій та програмно-апаратних засобів, для чого доцільно залучати сертифікованих спеціалістів. Консультації спеціалістів допоможуть визначити: 1) місця, в яких можуть залишитися сліди вчинення злочину, вигляд останніх; 2) необхідні

програмно-технічні засоби для виявлення цих слідів та їх фіксації у вигляді, зручному для безпосереднього сприйняття; 3) технічні та програмні засоби, якими, можливо, користувався правопорушник, його фаховий рівень; 4) найбільш оптимальні схеми виявлення, моніторингу та фіксації злочинної діяльності правопорушника, необхідність залучення фахівців.

У сучасних умовах комп'ютерна техніка може фіксувати докази злочинів не тільки в Інтернет-мережі. Доцільність та ефективність одержання доказів із застосуванням телекомунікаційних технологій очевидна. У кримінальному судочинстві пропонують за необхідне як найшвидше введення в кримінально-процесуальне законодавство норм, що визначають специфіку доказів, одержаних з використанням телекомунікаційних засобів, детально регламентувавши особливості такого способу отримання доказів.

Отже, одним з напрямів щодо вирішення проблеми криміналістичної модернізації є створення інтегрованої інформаційно-аналітичної системи правоохоронних органів, яка передбачена Концепцією національної програми інформатизації України [2] та впроваджується в ОВС України.

Технічний аспект пов'язаний, перш за все, з вивченням проблем надійності, швидкості та точності передачі інформації, з методами, технічними засобами побудови каналів передачі сигналів тощо.

Потрібно розробити науково обґрунтовані методики програмного забезпечення аналізу оперативної інформації, отриманої оперативно-технічними засобами для моделювання ситуацій, які складаються при проведенні оперативно-розшукових заходів [3].

Отже, пріоритетним напрямком криміналістичної модернізації є науково-технічна розробка та впровадження в досудовий кримінальний процес інноваційних проектів експертно-пошукових систем. Особливу актуальність це набуває у сфері розслідування серійних квартирних крадіжок. Тому викладені пропозиції пропонується використати під час створення єдиної інформаційно-телекомунікаційної системи правоохоронних органів, що сприятиме реалізації державної політики з питань боротьби із злочинністю в цілому, а з серійними квартирними крадіжками зокрема, забезпечить створення умов для поліпшення координації організаційних, профілактичних, оперативно-розшукових заходів, а також підвищить ефективність інформаційно-аналітичного забезпечення правоохоронної діяльності за рахунок удосконалення інформаційної взаємодії шляхом використання сучасних захищених інформаційно-

телекомунікаційних систем і проведення стандартизованих (уніфікованих) процедур обміну інформацією.

Список використаних джерел:

1. Синєокий О. В. Інформаційне право України та електронне право високих технологій / О. В. Синєокий. – Запоріжжя : ЗНУ, 2010. – 215 ел. с. [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua.

2. Про Концепцію Національної програми інформатизації : закон України від 4 лют. 1998 р. // Юридичний вісник України. – 1998. – №18.– С. 8–16.

3. Про схвалення Концепції Державної програми інформаційно-телекомунікаційного забезпечення правоохоронних органів, діяльність яких пов'язана з боротьбою із злочинністю : розпорядження Кабінету Міністрів України від 19 верес. 2007 р. № 754-р. – Режим доступу: http://zakon.rada.gov.ua/laws/show/754-2007-р.

Отримано 26.11.2012

УДК 621.373.54

Георгій Геннадійович ГУБАРЄВ
кандидат технічних наук, старший науковий співробітник,
доцент кафедри інформаційної безпеки факультету психології,
менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ

ПРО СТАНДАРТИЗАЦІЮ ЕЛЕКТРОШОКОВИХ ПРИСТРОЇВ В УКРАЇНІ

У зв'язку з неконтрольованим обігом електрошокерів в Україні, необхідно законодавчо врегулювати їх використання та створити національний стандарт «Електрошокові пристрої». На основі розробленої методики вимірювання вихідних параметрів електрошокерів та обґрунтованого критерію безпечності їх розрядів, ця проблема може бути вирішена за участю ХНУВС.

Постановка проблеми. Електрошокові пристрої відносяться до спеціальних засобів забезпечення громадського порядку і використовуються в розвинутих країнах правоохоронними

структурами і населенням більше 40 років. В таких країнах використання електрошокерів врегульовано національними законами про зброю та відповідними державними стандартами.

В Україні, на відміну від інших західних країн, Росії та Білорусії, електрошокові пристрої дозволено застосовувати лише в правоохоронних підрозділах. Однак в Проекті закону «Про зброю», який знаходиться на розгляді у Верховній Раді, використання електрошокових пристроїв не регламентовано. В той же час електрошокери для населення заборонено, оскільки, згідно з Постановою Верховної Ради від 17.06.1992 № 2471-XII, вони не можуть бути у власності громадян, громадських об'єднань, міжнародних організацій та юридичних осіб інших держав на території України.

Незважаючи на це, в Україні безконтрольно реалізуються на ринках та через інтернет-магазини десятки моделей електрошокерів зарубіжного виробництва, часто сумнівної якості та з невстановленими параметрами. В результаті значна кількість наших громадян піддаються небезпеці нанесення шкоди здоров'ю від використання таких електрошокерів, а злочинці отримують сучасні засоби спеціальної техніки для скоєння злочинів.

Харківський національний університет внутрішніх справ має значний досвід в галузі розробки і впровадження електрошокових пристроїв та методик вимірювання їхніх вихідних параметрів. Це підтверджується науковими публікаціями наших учених,

знаходи (№ 60071, № 79487, № 82374) організації виробника вітчизняних електрошокерів ТТ і методикою вимірювання вихідних параметрів електрошокерів [1], затвердженою Харківським центром метрології і стандартизації. Для обґрунтованого вибору допустимих значень вихідних параметрів електрошокерів, автором розроблено критерій безпечності розрядів електрошокових пристроїв [2].

Можливі підходи до розв'язання проблеми. Враховуючи ситуацію що склалася, для врегулювання в Україні обігу специфічного виду зброї – електрошокових пристроїв та для захисту внутрішнього ринку від неякісної і несертифікованої зарубіжної продукції, край необхідно запровадити національний закон «Про зброю» та державний стандарт «Електрошокові пристрої». Для цього необхідно невідкладно розпочати спільно з державним науково-дослідним інститутом МВС України роботу над розробкою та запровадженням національного стандарту України «Електрошокові пристрої». При цьому ХНУВС міг би взяти на себе зобов'язання

провести розробку такого державного стандарту і в короткий термін надати його першу редакцію. В свою чергу Державний науково-дослідний інститут МВС України може виступити в ролі замовника такої науково-дослідної роботи і, згідно з ДСТУ 1.2:2003, в ролі організації, яка вносить стандарт до прийняття Держспоживстандартом України.

На другому етапі розв'язання проблеми в Україні необхідно створити спеціалізовану вимірювальну лабораторію для визначення вихідних параметрів електрошокових пристроїв, оснащену цілим рядом спеціальних вимірювальних засобів. Така лабораторія після відповідної акредитації могла б проводити судово-технічну експертизу електрошокових засобів, використаних як знаряддя злочинів, та надавати висновок на відповідність електрошокових пристроїв вітчизняних і іноземних виробників національному стандарту «Електрошкові пристрої», який, ми сподіваємось, з часом буде прийнято.

Список використаних джерел:

1. Губарев Г. Г. Методика вимірювання експлуатаційних електричних параметрів електрошокерів / Г. Г. Губарев, С. И. Трубаев // Сучасна спеціальна техніка. – 2005. – № 2(7). – С. 72–88.

2. Губарев Г. Г. Енергетичний критерій безпечності електричних розрядів, вибір допустимих вихідних параметрів електрошокових пристроїв / Г. Г. Губарев // Право і Безпека. – 2011. – № 2 (39). – С. 212–218.

Отримано 02.11.2012

УДК 342.536:343

Антоніна Валеріївна ГУБСЬКА
оперуповноважений УДСБЕЗ УМВС України в Сумській області,
здобувач кафедри оперативно-розшукової діяльності
навчально-наукового інституту підготовки фахівців кримінальної міліції
Харківського національного університету внутрішніх справ

ОСОБЛИВОСТІ ПІДГОТОВКИ ТА ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ ПРАЦІВНИКІВ ДСБЕЗ В ОРГАНІЗАЦІЇ РОБОТИ ПІД ЧАС ПРОТИДІЇ ЗЛОЧИНАМ У СФЕРІ ЖИТЛОВО-КОМУНАЛЬНОГО ГОСПОДАРСТВА

У даній роботі досліджені особливості підготовки та підвищення кваліфікації працівників ДСБЕЗ у організації роботи під час протидії злочинам у сфері житлово-комунального господарства.

Із часу проголошення незалежності України першочерговим завданням стало питання боротьби з економічною злочинністю, яка виявилася одним із суттєвих чинників руйнування економіки держави [1, с. 9].

Згідно зі статистичними даними ДДСБЕЗ МВС України, кількість виявлених злочинів у сфері ЖКГ зростає. Так, у 2008 році викрито 538 злочинів, у 2009 – 557, що на 3,5 % більше ніж у 2008 р., у 2010 – 930, що на 6,9 % більше ніж у 2009 р., у 2011 – 1015, що на 9,1 % більше ніж у 2010 р.

На підставі викладеного ми дійшли висновку, що якісний процес організації протидії підрозділами ДСБЕЗ злочинам, що вчиняються у сфері ЖКГ залежить від особливості підготовки та підвищення кваліфікації працівників ДСБЕЗ, який, нажаль, не відповідає вимогам сьогодення.

Нами розроблена типова схема організації протидії підрозділами ДСБЕЗ злочинам, що вчиняються у сфері ЖКГ, яка повинна складатися з наступних елементів: збір і аналіз інформації про

і житлово-комунального господарства,
нання запланованих дій з організації
ЖКГ, постійна взаємодія з різними суб’єктами протидії злочинам у сфері ЖКГ, контроль за організацією протидії працівниками ДСБЕЗ злочинам, що вчиняються у сфері ЖКГ.

По-перше, для ефективної організації збору інформації про оперативну обстановку у сфері житлово-комунального господарства необхідно дотримуватись наступної схеми: 1) визначити назву,

кількість та місцезнаходження підприємств, організацій, установ державної та комунальної форм власності, які функціонують у сфері ЖКГ, таким чином окреслити коло об'єктів оперативного обслуговування сфери ЖКГ; 2) підібрати осіб з об'єктів сфери ЖКГ для залучення до негласного співробітництва та раціонально розставити їх з метою охоплення найбільш криміногенних об'єктів вказаної сфери; 3) зібрати інформацію про всі можливі схеми скоєння злочинів у сфері ЖКГ, а також про осіб, які становлять оперативний інтерес; 4) зібрати інформацію стосовно анкетних даних керівників об'єктів ЖКГ та вивчити їхні повноваження; 5) завести відповідні справи контрольно-спостережного провадження для оперативного обслуговування сфери ЖКГ.

По-друге, необхідно визначити найважливіші умови планування, зокрема це: висока компетентність керівництва підрозділів ДСБЕЗ у питанні вибору найбільш оптимальних шляхів протидії злочинам у сфері ЖКГ на всіх рівнях управління; високий рівень володіння спеціальними знаннями працівників ДСБЕЗ, що обслуговують об'єкти сфери ЖКГ; високий рівень поінформованості працівників ДСБЕЗ про оперативну обстановку у сфері ЖКГ.

Важливо відмітити, що працівники ДСБЕЗ планують роботу на певний період, а саме: складають щоденний план, план на місяць та півріччя. Особливістю плану як виду управлінського рішення є складний характер його змісту, що включає в себе взаємозалежну сукупність окремих рішень, особливу форму їх викладу, а також сувору визначеність процедури його вироблення і прийняття, застосування специфічних методів його обробки. У плані обов'язково знаходять відображення цілі і завдання підрозділу ДСБЕЗ на майбутній період, заходи, що підлягають виконанню для реалізації поставлених цілей і завдань, послідовність їх виконання, строки реалізації, виконавці, а також способи контролю за виконанням запланованих заходів. Таким чином, правильно спланована робота це запорука швидкій та якісній протидії злочинам у сфері ЖКГ.

Підрозділи ДСБЕЗ під час проведення оперативно-розшукових заходів, з метою протидії злочинам у сфері ЖКГ і відшукання джерел інформації, мають застосовувати наявні сили, засоби, методи і тактичні прийоми [2, с. 185].

По-третє, необхідною умовою в удосконаленні підготовки працівників ДСБЕЗ є налагодження взаємодії підрозділів ДСБЕЗ з контролюючими, координуючими, правоохоронними органами та ЗМІ. Молодому працівнику ДСБЕЗ необхідно володіти інформацією про коло суб'єктів з якими потрібна взаємодія у досягненні цілі щодо

протидії злочинам у сфері ЖКГ, якими нормативними актами передбачені дані відносини та позитивна сторона цієї взаємодії.

Останнім елементом організаційної структури протидії злочинам у сфері ЖКГ є контроль за організацією протидії працівниками ДСБЕЗ злочинам у названій сфері. Робота підлеглих певним чином сполучена зі стилем управлінської діяльності керівника. Офіційні відносини створюють певні гарантії дотримання норм службової поведінки, що призводить до стабільності, впевненості та цілеспрямованості діяльності. Негативно впливають на стан організаційних відносин бюрократичні прояви в управлінні, заорганізованість, незбалансованість задач, конформізм керівника [3, с. 27]. Тільки керівник, який має високі інтелектуальні здібності; досвід роботи в оперативних підрозділах; відповідні морально-психологічні риси; знання людської психології; вміння організувати колектив, розподілити роботу; авторитет та повагу серед підлеглих, зможе ефективно контролювати діяльність своїх підлеглих, що дозволить успішно вирішити такі завдання, як: виконання раніше затверджених планів, підвищення загального рівня оперативної готовності підрозділу; своєчасне виявлення наявних упущень та недоліків, а також вжиття оперативних заходів для їх усунення; правильний підбір і розстановка кадрів; підвищення виконавчої дисципліни; створення умов для надання практичної допомоги оперативному підрозділу і його окремим працівникам [4].

Виходячи із викладеного, можна стверджувати, що при значній увазі щодо особливостей підготовки та підвищення кваліфікації працівників ДСБЕЗ, а також при жорсткому підборі керівного складу підрозділів ДСБЕЗ, розумному формуванні організаційних відносин у цих підрозділах та правильному контролю за діяльністю підлеглих можуть бути досягнуті значні результати під час організації протидії працівниками ДСБЕЗ злочинам, які вчиняються у сфері житлово-комунального господарства, що приведе до зменшення кількості злочинів у даній сфері економіки.

Список використаних джерел:

1. Василинчук В. І. Правові й організаційно-тактичні основи попередження та розкриття шахрайств з фінансовими ресурсами оперативними підрозділами ДСБЕЗ: монографія / В. І. Василинчук, В. О. Глушков. – Луганськ : РВВ ЛАВС, 2004. – 232 с.

2. Бахин В. П. Использование средст массовой информации в борьбе с преступностью / В. П. Бахин, Н. С. Карпов, М. А. Михайлов //

Вісник ЛАВС ім. 10-річчя незалежності України. – 2002. – № 2. – С. 181–200.

3. Використання психологічних знань в оперативно-розшуковій діяльності / О. Ф. Долженков, Г. Є. Запорожцева, А. П. Кіцул, В. Е. Рижков. – О. : НДРВВ ОІВС, 2001. – 231 с.

4. Завгородній В. А. Форми взаємодії органів внутрішніх справ та громадських організацій у протидії корупції [Електронний ресурс]. – Режим доступу: http://radnuk.info/statti/565-pranoohor/14778-2011-01-19-02-34-03.html.

Отримано 20.11.2012

УДК 349.97

Олена Олександрівна ДЕНИСЯКА
курсант групи ФСД-09-3 факультету з підготовки слідчих
Харківського національного університету внутрішніх справ

КІБЕРТЕРОРИЗМ: ВІРТУАЛЬНЕ ЯВИЩЕ ЧИ РЕАЛЬНА ЗАГРОЗА

Досліджено принципово новий вид тероризму – кібертероризм. Визначено основні загрози з боку даного явища. Запропоновано ряд заходів щодо удосконалення боротьби з кібертероризмом.

На сучасному етапі розвитку суспільства все більше відчувається значимість інноваційних процесів, що відбуваються у зв'язку з інформатизацією. Але поряд із позитивними здобутками, інформатизація супроводжується побічними, негативними явищами криміногенного характеру, до яких відносять «кіберзлочинність». Глобальна всесвітня мережа Internet, що об'єднала мільйони комп'ютерів, розташованих в різних країнах, і відкрила широкі

та обміну інформації, все частіше
х цілях. А це, безумовно, потребує
протидії даному різновиду злочинності
на державному рівні. Для сучасного суспільства (в період його переходу від індустріального етапу розвитку до нового – постіндустріального, інформаційного) актуальність цієї проблеми не викликає сумнівів.

Деякі аспектиданого питання неодноразово висвітлювали у своїх працях А. А. Васильєв, О. Г. Волеводз, В. О. Мещеряков, В. О. Голубєв, Т. Л. Тропіна та інші науковці. Але з розвитком суспільства зростають масштаби й способи учинення нових видів злочинів , що здійснюються з використанням ЕОМ.

Зокрема, все більше уваги з боку керманичів як нашої так і інших країн привертає принципово новий вид тероризму – кібертероризм. Під кібертероризмом слід розуміти вид терористичної діяльності, який полягає в навмисній комплексній атаці на комп`ютерну інформацію, включаючи захоплення, виведення з ладу й руйнування об'єктів, що створює загрозу виникнення надзвичайної ситуації в телекомунікаційних мережах, заподіяння значної майнової шкоди чи настання інших суспільно небезпечних наслідків. Такі дії вчиняють із метою порушення громадської безпеки, залякування населення, провокацій військового конфлікту, ускладнення міжнародних відносин, здійснення впливу на органи влади або привернення уваги громадськості до певних політичних, релігійних чи інших організацій. Характерною відмінністю кібертероризму від кіберзлочинності є його відкритість, коли вимоги терориста широко сповіщаються [1]. Варто відзначити, що дане поняття свого закріплення на законодавчому рівні ще не знайшло.

Оцінюючи загрозу кібертероризму Україні слід ураховувати деякі особливості нашої країни. Це, по-перше, високий потенціал і професійний рівень програмістів, послугами яких охоче користуються навіть такі флагмани програмної індустрії, як Майкрософт. По-друге, здатність молоді швидко опановувати технічні новинки, про які ще вчора вони не мали жодної уяви. Ураховуючи той факт, що обчислювальна техніка постійно дешевшає, можна очікувати, що буде зростати й кількість користувачів Інтернет у нашій країні. По-третє, хоча ще слабкий, але вже помітний підйом економіки неодмінно викличе зростання комп'ютеризації і ще на один-два кроки наблизить нас до країн з розвиненою інфраструктурою, що зробить загрозу кібертероризму цілком реальною [2]. Кібертерористи можуть блокувати роботу метрополітену; паралізувати роботу залізничного і повітряного транспорту з метою спричинення економічних збитків державі; проникати в локальні мережі державних структур (МВС, фінансові заклади) з метою зміни чи знищення інформації, блокувати роботу комп'ютерів, викрадати кошти тощо. Такі терористичні угруповання, як Hizbollah, HAMAS, theAbuNidalorganization і BinLaden'salQa'ida використовують комп'ютерні файли, електронну пошту та шифрування (криптографію й комп'ютерну стеганографію)

для підтримки своєї протиправної діяльності, що в декілька разів ускладнює боротьбу з ними [3].

Рішуча кібератака приречена на успіх. Тому дуже важливим є правове обмеження цієї діяльності і міжнародна співпраця. На нашу думку, самі заходи технічного захисту не зупинять кібератаку, якщо вони не будуть доповнені інтенсивною політичною і правовою співпрацею. Це пояснюється тим, що завдяки широкому розповсюдженню глобальних телекомунікаційних мереж, для того, хто вчиняє кіберзлочин, не існує політичних кордонів. Правопорушник може знаходитися в одній країні (в якій не розвинена система протидії кіберзлочинності), а предмет його посягання – в іншій.

З огляду на зазначене, вважаємо за доречне частину державного апарату Управління боротьби з кіберзлочинністю переорієнтувати на створення системи боротьби з кіберзлочинами, підвищити рівень підготовки кадрів для підрозділів боротьби з кіберзлочинністю, удосконалити вже існуючі нормативно-правові акти, що регулюють дану сферу відносин, враховуючи досвід провідних іноземних країн та розробити нові, які чітко б регулювали процедуру розслідування кіберзлочинів та взаємодію вітчизняних й іноземних підрозділів по боротьбі з кіберзлочинами, визначали основні напрямки протидії таким злочинам та методи їх попередження. Також схиляємося до думки, що державні правоохоронні органи повинні підтримувати тісний зв'язок з такими міжнародними організаціями як з Міжнародна організація з доказів комп'ютерних злочинів – IOCE (International Organisationon Computer Evidence) або з Форум команд з безпеки та реагування на інциденти – FIRST (Forumof Incident Responseand Security Teams) [4]. Це зможе забезпечити більш швидке та ефективне проведення розслідування та розкриття кіберзлочинів.

Список використаних джерел:

1. Голубєв В. О. Україні загрожує... кібертероризм [Електронний ресурс] / В. О. Голубєв. – Режим доступу: http://www.viche.info/journal/3018/.

2. Голубєв В. Кібертероризм – загроза національній безпеці та інтересам України [Електронний ресурс] / В. Голубєв // Юридичний журнал. – 2004. – № 1. – Режим доступу: http://www.justinian.com.ua/article.php?id=1002.

3. Погребняк А. В. Технології комп'ютерної безпеки : монографія / А. В. Погребняк. – Рівне : МЕГУ, 2011. – 117 с.

4. Глушков В. О. Про Проект Концепції стратегії реалізації державної політики щодо боротьби з кіберзлочинністю в Україні

[Електронний ресурс] / В. О. Глушков, К. І. Бєляков, С. О. Орлов. – Режим доступу: http://www.crime-research.ru/library/Glushkov.htm.

Отримано 29.11.2012

УДК 343.97

Олексій Олександрович ДЕРЕВЯГІН
кандидат юридичних наук,
старший викладач кафедри оперативно-розшукової діяльності
навчально-наукового інституту підготовки фахівців кримінальної міліції,
Харківського національного університету внутрішніх справ

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ ЯК ОСНОВА ЕФЕКТИВНОЇ ПРОТИДІЇ ЗЛОЧИННОСТІ

Представлено комплекс інноваційних спеціалізованих програмних засобів, що складають досягнення в сфері інформаційно-аналітичного забезпечення службово-бойової діяльності ОВС.

Оперативно-розшукова діяльність здійснюється заради отримання інформації, її накопичення, обробки, аналізу і висновків та вжиття відповідних заходів. Робота кожного оперативного підрозділу пов'язана, в першу чергу, з виявленням, попередженням і розслідуванням злочинів [1]. Неможливо навіть уявити, що оперативні підрозділи можуть виконати своє завдання, не маючи ніяких відомостей про злочинця. Повне і всебічне висвітлення діяльності суб'єкта правопорушення являється запорукою успішного припинення його протиправної поведінки. Наявність попередньої інформації про злочин і особу, яка його вчинила є основою у його протидії.

Соціально-економічний і науково-технічний розвиток України на сучасному етапі пов'язані з вирішенням проблем інформатизації держави, суспільства, правопорядку. Інформаційне забезпечення

ьності є складовою частиною их органів, в якій запровадження одна з першочергових задач за для ефективної протидії злочинності.

Міністерство внутрішніх справ України, зокрема, в своїх нормативно-правових актах, зосереджує увагу на якісно новому рівні

діяльності по вдосконаленню тактики і методики розкриття та розслідування злочинів, запровадженні в практику діяльності передових вітчизняних та зарубіжних форм і методів роботи.

Згідно з відомчою інформаційною політикою це завдання нерозривно пов'язано з формуванням інформаційного середовища органів, які здійснюють оперативно-розшукову діяльність, що складається з відомчих інформаційних ресурсів та інформаційної інфраструктури правоохоронних органів.

Ефективність інформаційного середовища правоохоронних органів України забезпечується за рахунок комплексного, системного підходу до вирішення проблем техніко-технологічного та соціально-політичного характеру [2, с. 116].

В цьому аспекті не аби яку роль відіграють новітні досягнення в сфері інформаційно-аналітичного забезпечення службово-бойової діяльності ОВС, висвітлення яких має стати запорукою ефективної протидії злочинності.

Так, співробітниками інформаційної служби ГУМВС України в Луганській області розроблено і введено в експлуатацію комплекс спеціалізованих програмних засобів. Його можливості і особливості вживання розглядаються в практичному посібнику «Сучасна зброя співробітників органів внутрішніх справ: інформаційні технології як відповідь на виклики часу» [3]. Зокрема у його розділах надано опис комп'ютерних підсистем:

– автоматизована інформаційно-аналітична система «СОВА». Основні функції – комплексне рішення завдань обробки і аналізу даних з метою надання інформації, сприяючої запобіганню і розкриттю злочинів. Система оперує єдиним інтегрованим масивом даних, що формується в результаті явної і негласної роботи підрозділів міліції, а також інших джерел інформації. В рамках системи реалізовано комплекс передових інформаційних технологій, у тому числі технології візуального аналізу даних, геоінформаційні технології, Data Mining і т. ін. Система є надбудовою над вже функціонуючими інформаційними застосуваннями, не роблячи впливу на їх функціонування і не вимагаючи їх заміни;

– автоматизована інформаційно-аналітична система «Кристал» – розроблена для вирішення завдань, по формуванню, аналізу і контролю інформаційного масиву, що містить відомості про злочини і осіб, що їх вчинили;

– автоматизована інформаційно-аналітична система «Аргус» – це автоматизована біометрична система ідентифікації громадян по їх фото- і відео зображенням. Вона реалізує програмні методи

автоматичної ідентифікації, засновані на фізіологічних або поведінкових характеристиках людини;

– автоматизована інформаційно-аналітична система «Спіраль» – це автоматизована габітоскопічна система ідентифікації особи за методом словесного портрету. Основою розробки є спеціальний алгоритм нечіткого порівняння об'єктів;

– автоматизована інформаційно-аналітична система «Парус» – призначена для автоматизації збору, накопичення, аналізу і узагальнення різних статистичних показників з метою своєчасної всебічної оцінки службової діяльності підрозділів ОВС області. Основною особливістю даної системи є можливість автоматизації процесу отримання даних, які не можна почерпнути з існуючих інформаційних сховищ;

– автоматизована інформаційно-аналітична система «Fastreport» – це програмний комплекс, що призначений для формування звітів і друкарських форм, він є розширеним інструментом для аналітичної і статистичної обробки інформації що зберігається в різних автоматизованих системах, маніпулювання і відображення різнорідних даних в найбільш зручному для сприйняття вигляді. Він виконує функції базового інструменту для ухвалення ефективних управлінських рішень.

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

Список використаних джерел:

1. Про затвердження Положення про органи досудового розслідування Міністерства внутрішніх справ України : наказ МВС України від 09.08.2012 № 686. – К. : РВВ МВС України, 2012. – 14 с.

2. Бандурка О. М. Оперативно-розшукова діяльність. Ч. І : підручник / О. М. Бандурка. – Х. : Вид-во Нац. ун-ту внутр. справ, 2002. – 336 с.

3. Современное оружие сотрудников органов внутренних дел: информационные технологии как ответ на вызовы времени : практ. посіб. / Ю. А. Задорожний, А. Е. Трубкович, О. В. Калтырин и др. ; МВД Украины, Луган. гос. ун-т внутр. дел им. Э. А. Дидоренко. – Луганск : РИО ЛГУВД им. Э. А. Дидоренко, 2012. – 104 с.

Отримано 26.11.2012

УДК 621.322

Станіслав Миколайович ДОСКАЛЕНКО
курсант групи ФПТ-09-2 факультету психології, менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ
Денис Сергійович КУЧЕРЕНКО
студент групи ОТ-320 Харківського радіотехнічного технікуму

РОЗПОДІЛЕНИЙ КОНТРОЛЬ ПОТОКІВ ДАНИХ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Представлені основні терміни розподіленого контролю даних в потоках ІТС. Розглянуто основні завдання розподіленого контролю потоків даних в ІТС, механізми моніторингу та управління інформацією. Застосування та побудова системи розподіленого контролю потоків даних в ІТС.

Ідея реалізації функцій контролю та управління доступом на рівні інфраструктури мережі є аналогією мереж шифрованого зв'язку. Створення технічних засобів, що дозволяють будувати мережі зв'язку з контрольованим і керованим доступом, забезпечить в інформаційно-телекомунікаційних системах (ІТКС) надійний захист від внутрішнього порушника подібно до того, як мережі шифрованого зв'язку забезпечують захист від зовнішнього порушника.

Завдання розподіленого контролю потоків даних в ІТКС полягає у моніторингу та управлінні передачею інформації між територіально розподіленими вузлами системи, об'єднаними мережею зв'язку. Під потоком даних розуміється одно-або двонаправлений обмін даними між двома вузлами мережі обмежений за часом. У загальному випадку

си можуть вимагати обміну даними між схемами – безпосередньо, або через йсь іншій схемі. Таким чином, безліч вузлів ІТКС, здиснюючи оомін даними за допомогою передачі потоків даних за певною схемою, утворюють сеанси зв'язку. Інформація, що циркулює в межах сеансів зв'язку, розглядається як об'єкт доступу.

Завдання розподіленого контролю потоків даних в ІТКС може бути вирішена різними методами. Ідентифікація вузлів зв'язку може бути виконана на основі мережевої адреси, або із залученням засобів ідентифікації і аутентифікації користувачів. Віднесення потоків даних до сеансів зв'язку може бути виконане на основі аналізу даних, що пересилаються, маркування даних перед відправленням додатками, або за вказівкою від користувача вузла зв'язку. Механізми моніторингу та управління передачею інформації можуть бути реалізовані на вузлах зв'язку, або в мережі на основі шлюзових технологій; у випадку, якщо всі сеанси зв'язку організовуються через єдиний сервер зв'язку, механізми управління передачею потоків даних можуть розташовуватися на цьому сервері.

Застосування концепції мереж зв'язку з розмежуванням доступу (МЗРД) дозволяє вирішити завдання розподіленого контролю потоків даних без необхідності модифікації додатків і сервісів ІТКС. Іншою істотною перевагою запропонованого підходу є істотне зниження складності сертифікаційних досліджень ІТКС на основі МЗРД. Точно також, як застосування сертифікованих потокових шифраторів знімає необхідність реалізації і подальшої сертифікації підсистем криптографічного захисту каналів зв'язку, застосування МЗРД зніме необхідність розробки і подальшої сертифікації підсистем контролю та управління доступом, реєстрації та обліку подій.

Побудова МЗРД на практиці пов'язано з безліччю труднощів. Так в одній ІТКС, як правило, функціонує безліч додатків, кожне з яких використовує свої протоколи зв'язку. Існує також службовий трафік, такий як ARP, ICMP, DHCP, DNS і тп. Великий обсяг протоколів зв'язку ускладнює детектуючі механізми мережі зв'язку. Також необхідно визначити чи буде застосовувана політика безпеки єдиною для всіх додатків, або для кожного додатка буде окрема політика. Одним з найсерйозніших питань розробки мереж зв'язку з розмежуванням доступу є механізм інтеграції з цільовою ІТКС. Від цього залежать підсистеми ідентифікації, аутентифікації, детектування та ін.

Питання розробки мереж зв'язку з розмежуванням доступу досить актуальні. І по мірі того, як будуть ускладнюватися ІТКС, актуальність цих питань буде зростати, оскільки на сьогоднішній день не існує інших способів зниження трудомісткості процесу сертифікації, крім використання готових сертифікованих компонентів при побудові ІТКС.

Отримано 12.11.2012

УДК 343.98

Євгеній Вікторович ЗОЗУЛЯ
викладач кафедри криміналістики, судової медицини та психіатрії
факультету з підготовки слідчих
Харківського національного університету внутрішніх справ

ЗАСТОСУВАННЯ ДОСЯГНЕНЬ НАУКИ І ТЕХНІКИ В ПРОЦЕСІ РОЗКРИТТЯ І РОЗСЛІДУВАННЯ ЗЛОЧИНІВ

Розглянуті питання щодо застосування в кримінальному процесі сучасних досягнень науки і техніки.

Одним із найважливіших завдань сучасної Української держави і суспільства в цілому є забезпечення суворого додержання законності, викорінення будь-яких порушень громадського порядку, ліквідація злочинності, усунення причин та умов, що породжують та сприяють її розвитку.

Необхідність застосування у кримінальному процесі наукових, технічних та інших знань пов'язана з тим, що розслідування злочину є складним процесом пізнання об'єктивної дійсності. Тому пізнання події злочину та порушника, який його вчинив, вимагає від особи, що проводить дізнання, слідчого та інших учасників кримінального процесу застосування різних спеціальних знань та навичок у певних видах діяльності. Науково-технічний прогрес дає більш широке застосування його надбань у правоохоронній діяльності.

Науково-методичним забезпеченням є система науково визначених напрямів діяльності, в кожному з яких цілеспрямоване здійснення певних заходів сприяє оптимізації кримінально-процесуальної діяльності. До його структури доцільно віднести: законодавчий, інформаційний, науково-технічний, організаційний, кадровий і матеріально-технічний напрями [1].

Діяльність [illegible] завжди пов'язана з розслідуванням [illegible]я як фахівці-юристи, так і особи, які [illegible]ями в інших галузях науки, техніки, мистецтва та ремесла. Така діяльність спрямована, в першу чергу, на забезпечення об'єктивності досудового слідства, встановлення істини у кримінальному провадженні, що є основною метою розслідування.

Тому виникнення і розвиток інституту застосування спеціальних знань у кримінальному судочинстві тісно пов'язані з процесом розвитку та удосконалення теорії і практики кримінально-процесуальної форми досудового слідства та судового розгляду кримінальних справ.

Найчастіше для застосування науково-технічних засобів слідчими залучаються як спеціалісти експерти-криміналісти, судово-медичні експерти науково-дослідних (криміналістичних) установ (бюро) системи МВС, МОЗ, Міністерства юстиції України та ін.

Вагома технічна допомога слідчому надається спеціалістами-криміналістами при огляді місця події, проведенні слідчого експерименту, обшуку тощо. Важливо й те, що при проведенні цих та інших слідчих дій спеціаліст іноді може застосувати той чи інший технічний засіб, який є новинкою.

При проведенні огляду місця події та деяких інших слідчих дій важливо виявити, зафіксувати та вилучити непошкодженими невидимі неозброєним оком сліди злочину. Участь спеціаліста з метою застосування новітніх і найскладніших науково-технічних засобів підвищує надійність гарантії виявлення, фіксації та вилучення таких речових доказів і об'єктивність їх оцінки й використання у кримінальній справі [2].

Слід зауважити, що всі досягнення криміналістики можуть застосовуватись тільки в рамках кримінально-процесуального законодавства, з дотриманням процесуальної форми. Здобуті фактичні дані можуть бути використані в судовому доказуванні тільки, якщо вони відповідають встановленим процесуальним законом правилам допустимості доказів.

Протягом тривалого часу у спеціальній літературі висловлені спірні міркування з питань застосування у розкритті й розслідуванні злочинів поліграфу як технічного засобу виявлення, фіксації, вилучення і дослідження внутрішнього емоційного стану людини. Не викликає сумніву, що сучасний поліграф – це високоточний прилад, який відображає психофізіологічний стан організму досліджуваної особи [3]. Нині використання поліграфу в КПК України не врегульоване і до процесуальних дій не відноситься. Щоправда, у 2001–2002 роках в Україні проводився експеримент щодо використання комп'ютерних поліграфів у діяльності органів внутрішніх справ України. Відповідно до наказу МВС України № 743 від 28 серпня 2001 року, поліграфна перевірка здійснювалася при опитуванні кандидатів на службу в органи внутрішніх справ чи навчання в учбових закладах МВС України, осіб, які включалися до складу миротворчих місій, висувалися на керівні посади.

Експеримент по використанню комп'ютерних поліграфів у кадровій роботі продовжувався до 1 вересня 2002 року. Однак у подальшому ні Концепція використання поліграфу в діяльності органів внутрішніх справ України, у тому числі по розкриттю й розслідуванню злочинів, ні інший відомчий документ, який регламентував би питання використання поліграфу, не прийнятий. За умов відсутності правового регулювання поліграф не може застосовуватися у кримінально-процесуальній діяльності органів внутрішніх справ України.

Підвищення якості слідчої і судової діяльності залежить від умілого використання новітніх науково-технічних засобів, інформаційних технологій, сучасних прийомів, способів та методів. Важливою умовою ефективного розслідування злочинів та судового розгляду справ є використання спеціальних знань, призначення і проведення судових експертиз, впровадження передових досягнень науки і техніки у практику боротьби зі злочинністю, що сприяє надійності системи доказування по справі.

Список використаних джерел:

1. Бахін В. П. Удосконалення форм використання науково-технічних досягнень у розслідуванні / В. П. Бахін, П. В. Цимбал // Проблеми удосконалення кримінального та кримінально-процесуального законодавства : міжвуз. зб. наук. пр. – К. : Укр. акад. внутр. справ, 1993. – С. 112–121.

2. Гончаренко В. Г. Використання положень природничих і технічних наук в кримінальному судочинстві / В. Г. Гончаренко. – К. : Вища школа, 1999. – 260 с.

3. Барко В. І. Перспективи застосування поліграфів «Axciton» в органах внутрішніх справ України / В. І. Барко // Актуальні проблеми юридичної психології : матеріали міжнар. наук.-практ. конф., 18–20 трав. 1999 р. / за ред. С. І. Яковенка. – К. : РВВ КІВС, 1999. – С. 8–10.

Отримано 14.11.2012

УДК 343.915

Алла Олексіївна ЙОСИПІВ
кандидат юридичних наук,
доцент кафедри кримінального права та кримінології
Львівського державного університету внутрішніх справ

ЗАПОБІГАННЯ ЗЛОЧИННОСТІ ПІДЛІТКІВ З МАРГІНАЛЬНОГО СЕРЕДОВИЩА

Розглянуто злочинність підлітків-маргіналів як особливої категорії злочинців, причини їх маргіналізації, особливості їх злочинності, досліджено необхідність вжиття запобіжних заходів для боротьби зі злочинністю даної категорії злочинців.

Злочинність підлітків з маргінального середовища як різновид підліткової і маргінальної злочинності має свої особливості і є самостійним об'єктом кримінологічного вивчення. В умовах соціальних, економічних і політичних перетворень, що відбуваються в суспільстві злочинність серед підлітків-маргіналів характеризується в останні роки негативними якісними і кількісними змінами, що актуалізує проблеми комплексного вивчення процесів, що відбуваються в маргінальному середовищі.

Злочинність зазначеної категорії осіб має не тільки загальні риси, що відносяться як до злочинності неповнолітніх, так і до злочинності в цілому, а й свої особливості, внаслідок чого підлітки-маргінали потребують особливих заходів профілактичного впливу. Як показує практика, заходи, що приймаються в галузі адміністративних, силових і репресивних методів боротьби з цим асоціальним, криміногенним явищем зазвичай виявляються безрезультатними. Системи освіти та охорони здоров'я, наукові установи у зв'язку з украй мізерним фінансуванням, відсутністю спеціальних кадрів, нерозвиненою мережею і матеріально-технічною базою закладів не змогли швидко розробити і впровадити методи та засоби профілактики, діагностики лікування та реабілітації дітей і підлітків з маргінальною середовища.

За даними Держкомстату, у 2010р. в підрозділах кримінальної міліції у справах дітей перебувало на обліку: 4133 неповнолітніх, які не працювали і не навчались; 5756 – мали одного з батьків; 785 – не мали батьків; 1117 – проживали в школах інтернатах та дитячих будинках; 7669 – проживали в неблагополучних сім'ях; 1839 – систематично залишали сімї, школи – інтернати, дитячі будинки;

6435 – схильні до вчинення правопорушень, бродяжництва, жебрацтва; 2168 – схильні до вживання алкогольних напоїв, наркотичних речовин.

Особливості злочинності підлітків-маргіналів, її причинного комплексу, а також особливості особистості неповнолітніх маргіналів обумовлюють і специфіку системи заходів попередження їх злочинної поведінки. Профілактика криміналізації підлітків з маргінальною середовища повинна бути спрямована на нейтралізацію субкультурної соціалізації. Для цього необхідний пошук нових організаційних форм роботи та поліпшення вже наявних. Основними напрямками профілактики асоціальної поведінки підлітків-маргіналів повинні стати психолого-педагогічні та організаційно-правові.

Труднощі у попередженні втягнення неповнолітніх до організованої злочинної діяльності, у виправленні, зміні життєвих орієнтирів підлітків, відомі світовій практиці, погіршуються в наших умовах практично повною відсутністю досвіду спеціальної профілактичної діяльності даного напрямку.

Найбільш пріоритетним напрямом діяльності суб'єктів профілактики щодо попередження злочинності серед зазначеної категорії осіб є профілактичний вплив на негативні фактори маргінального середовища на основі комплексної, безперервної програми, оскільки саме ці фактори є найбільш важливими в причинно-наслідковому комплексі вчинення ними злочинів. При цьому основне місце в попередженні злочинності підлітків-маргіналів повинна займати профілактична діяльність з оздоровлення соціально-правової обстановки в суспільстві, так як соціальне неблагополуччя є однією з основних причин, визначаючих стан і динаміку асоціальної поведінки та злочинності підлітків з маргінальною середовища.

Однією з причин потрапляння підлітків в маргінальне середовище, є їх безпритульність.

Ставши безпритульним, неповнолітній потрапляє ніби в соціальний вакуум, він пориває практично будь-який зв'язок з нормальним середовищем. Для нього не існують закони, призначені для звичайних громадян. Багато безпритульних підлітків зневажають прийняті усіма норми і правила, живуть за неписаними законами того суспільства, куди вони потрапляють, де заохочується, визнається те, що чуже людському суспільству, де своя мораль, своя правда, свої авторитети, наділені часом безмежною владою. Таким чином, маргінальне середовище саме по собі асоціальне (позасоціальне). До підлітків з маргінального середовища ми відносимо безпритульних, тобто бездоглядних, що не мають місця проживання і (або) місця перебування [1].

Ще в 20-ті роки XX ст. П. І. Люблінський, говорячи про безпритульність, зауважив, що це тривала хвороба, що проходить кілька стадій або фаз свого розвитку [2].

Дитяча безпритульність – наслідок сучасної соціально-економічної та духовно-моральної ситуації в Україні, яка характеризується наростанням соціального неблагополуччя сімей, падінням їх життєвого рівня, дистанціюванням школи від дітей з важкою долею, криміналізацією середовища. Дитяча безпритульність росте на фоні глибокої економічної, що триває не один рік, кризи, матеріального становища всіх верств населення, що постійно погіршується, росту алкоголізації дорослого та дитячого населення, краху традиційних загальнолюдських моральних цінностей. Повна безконтрольність з боку батьків, їх байдужість, педагогічна безграмотність сприяють тому, що неповнолітні до пізнього часу безцільно тиняються по вулиці, призвичаюються до спиртного, вчиняють різні правопорушення [3].

Запобігання злочинності підлітків-маргіналів повинно будуватися на врахування специфіки даної частина суспільства, беручи до уваги як загальні так спеціальні заходи.

Список використаних джерел:

1. Голодняк А. Ю. Криминологические особенности антиобщественного поведения подростков из маргинальной среды и предупреждение совершаемых ими пре ступлений : дис. … канд. юрид. наук : 12.00.08 / Голодняк А. Ю. – М., 2003. – С. 134.

2. Люблинский П. И. Борьба с преступностью в детском и юношеском возрасте (Социально-правовые очерки) / П. И. Люблинский. – М., 1923. – С. 45.

3. Станиславова И. Л. Современная семья и внутренний мир ребенка. Психология и педагогика детства / И. Л. Станиславова, Л. К. Скачкова // Тезисы докладов и сообщений III международной конференции «Ребенок в современном мире» – СПб., 1996. – С. 27.

Отримано 05.11.2012

УДК 621.322

Сергій Володимирович КАЛЯКІН
викладач кафедри інформатики та інформаційних систем і технологій в діяльності ОВС факультету психології, менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ
Костянтин Едуардович ПЕТРОВ
доктор технічних наук, доцент,
начальник кафедри інформатика та інформаційних систем і технологій в діяльності ОВС факультету психології, менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ
Андрій Анатолійович КОНДРАТЕНКО
курсант групи ФПТ-09-2 факультету психології, менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ

ОСНОВНІ НАПРЯМИ ТЕСТУВАННЯ БЕЗПЕКИ У ВЕБ-ДОДАТКАХ

Представлені основні терміни безпеки. Розглянуто прийоми тестування веб-додатків і надані рекомендації, щодо запобігання несанкціонованого доступу до програмних продуктів.

Розвиток сучасного світу неможливий без використання новітніх комп'ютерних та мережевих технологій. З усіх комп'ютерно-орієнтованих систем варто відмітити Internet та Web-базовані технології, в яких найкраще поєднуються універсальність, відкритість і надійність.

Тестування безпеки, це вид тестування, який дозволяє нам бути упевненими що персональна і конфіденційна інформація, що зберігається на наших серверах, такою і залишиться. Безпека включає і тестування того, що користувачі з різними правами доступу залишаються в рамках цих прав.

Основні термінів в області безпеки веб-додатків наступні.

Уразливості (*Vulnerabilities*) – це слабкі місця в додатках, які зловмисники використовують для проникнення в програму. Причиною таких вразливостей може стати недостатньо добре написаний код, SQL-скрипт, або просто наявність вірусів на сервері; міжсайтовий скриптінг (*Cross Site Scripting-XSS*) – тип вразливості інтерактивних інформаційних систем. Міжсайтовий скриптінг виникає, коли на сторінки, які були згенеровані сервером, з якоїсь причини

потрапляють скрипти користувачів; маніпуляції з посиланнями (URL *manipulation*) – Web додатки взаємодіють з сервером у формі клієнт-серверного обміну даними. Зміна або додавання інформації в URL може привести до непередбачених наслідків; SQL ін'єкції (SQL-injection) – це проникнення і виконання шкідливих дій шляхом виконання SQL запитів введених в поля призначеного для користувача інтерфейсу додатка; Спуфинг (Spoofing) – створення клона сайту або e-mail сервера з подальшим його використанням для нанесення шкоди власникові і користувачам додатка.

З'ясувавши основні зовнішні погрози для нашого застосування розглянемо прийоми тестування, які дозволять нам попередити доступ до нашого додатка зловмисників. Насамперед вимоги до тестувальників безпеки, вище, ніж до звичайних тестувальників. Вони повинні розуміти основні принципи роботи протоколів, як саме те або інше клієнтське застосування взаємодіє з сервером, знати прийому SQL і XSS ін'єкцій і т. д.

Практичні рекомендації по тестуванню розділимо так само – по видах вразливостей.

Першим в списку для тестування можна виділити тестування паролів. Чим більш ваш продукт вимогливий до формату пароля, тим краще. У мережі достатні багато додатків для зломупаролів, списків найбільш поширених паролів і імен користувачів. Неочевидним при тестуванні, але важливим елементом перевірки безпеки паролів є тестування cookies браузера. Загальна рекомендація – використовувати шифрування паролів cookies браузера. Та ж рекомендація стосується зберігання пароля в базі і при передачі пароля від клієнта до сервера. Навіть якщо за допомогою ін'єкції зловмисник дістане доступ до бази, існує можливість, що пароль він не розшифрує. Тестування паролів проводиться за допомогою перевірки тестувальником бази даних, шляхом складання запитів у відповідні таблиці, проглядання cookies браузера, і source коду сторінки. Це можна робити як простим пошуком, так і за допомогою спеціальних програм.

URL маніпуляції найчастіше можливі там, де використовується метод GET HTTP-протоколу для передачі інформації між клієнтом і сервером. Інформація передається в URL з елементами запиту в базу даних (це може бути user ID, група користувачів і ін.). Тестувальник, в такому разі, міняє ті дані в URL запиті, які відповідають запиту в базу.

SQL ін'єкції досить поширений спосіб проникнення в додаток. Простим способом захисту від SQL ін'єкцій є заборона на спеціальні символи в полях введення даних, такі як ' =; * тобто всі ті символи, без яких неможливе виконання запиту. Разом з розробниками необхідно

знайти місця в додатку, де є запити в базу з використанням призначених для користувача даних. Якщо призначені для користувача дані містять SQL запит для бази, навіть за наявності повідомлення про помилку, запит може бути виконаний, тому в цьому випадку необхідно не лише протестувати випадки SQL ін'єкцій, але і на рівні коду правильно на них реагувати.

Для того щоб протестувати захист від XSS атак, необхідно переконатися що будь-які <script> елементи не приймаються додатком і не обробляються при відправленні запиту. Зловмисники мають можливість скористатися спроможністю виконувати такого роду запити в полях додатка або в URL, шляхом впровадження в них скриптів. За допомогою таких скриптів існує можливість отримати доступ до інформації що зберігається в cookies.

Тестування безпеки – це завжди тестування на злом. Метою тестування безпеки є виявлення всіх можливих вразливостей, і в цьому випадку документування є важливим моментом.

Отримано 05.11.2012

УДК 342.536:343

Марія Віталіївна КАРА
старший оперуповноважений СБТЛ УКР УМВС України
в м. Севастополі,
здобувач кафедри оперативно-розшукової діяльності
навчально-наукового інституту підготовки фахівців кримінальної міліції
Харківського національного університету внутрішніх справ

СУЧАСНА ОПЕРАТИВНО-РОЗШУКОВА ХАРАКТЕРИСТИКА ОСОБИ ШАХРАЯ

Досліджено особливості оперативно-розшукової характеристики особи шахрая, наведено кваліфікацію та проаналізовано важливість її врахування під час організації протидії та розслідування шахрайств.

На усіх етапах історичного розвитку суспільства питання боротьби із злочинністю не втрачають своєї актуальності, набуваючи особливого значення в періоди політичних і соціально-економічних

перетворень. А прийдешні в Україні серйозні суспільно-політичні і соціально-економічні зміни (вступ нового УПК, нові реформи нещодавно обраної гілки влади – парламенту) не виключено, що можуть як супроводжуватися, так і спровокувати загострення криміногенної ситуації, зростання злочинності [1, с. 15]. При цьому характерною рисою сучасної злочинності є значне зростання тих видів злочинів, які мають корисливу мотивацію і носять яскраво виражений інтелектуальний характер. До цієї групи злочинів відноситься, в першу чергу, шахрайство.

Проблема особи шахрая актуальна передусім тим, що без вивчення її властивостей складно ефективно боротися з шахрайством як при проведенні оперативно-розшукові заходи (ОРЗ), так і при здійсненні слідчих дій. Оперативно-розшукова характеристика дає можливість правильно вирішувати питання про індивідуальну відповідальність і покарання, розкривати причини і умови, що сприяють вчиненню злочину [2, с. 39]. Тривале зростання шахрайських посягань на майно фізичних і юридичних осіб, підвищення рівня організованості шахраїв і масштабів заподіюваного збитку, високий рівень їх латентності і протидії розслідуванню вимагають віднести боротьбу з цим видом злочину до пріоритетних напрямів діяльності правоохоронних органів. У зв'язку з цим, МВС України за допомогою ЗМІ регулярно здійснює інформаційно-роз'яснювальну роботу щодо злочинів відносно соціально незахищених громадян. Ведеться активна робота працівниками карного розшуку ОВС України.

Зважаючи на це, вивчення особи злочинців дає можливість розділити їх на певні групи, які характеризуються переважанням одного або декількох найбільш важливих ознак (властивостей), покладених в основу такого ділення. Виділення таких груп потрібне для вивчення і попередження як злочинності в цілому, так і для вивчення окремих видів злочинів, диференціації вживаних заходів попередження [3, с. 83].

Рядом авторів були запропоновані типології осіб, що здійснюють шахрайські посягання. Так, А. А. Герцензон і І. Н. Даньшин за результатами узагальнення судової практики виділили наступні типи шахраїв: 1) випадкові шахраї, що здійснюють шахрайство уперше по легковажності, під впливом обставин або інших осіб; 2) шахраї-рецидивісти, що здійснюють головним чином дрібні шахрайські витівки; 3) шахраї – багатократні рецидивісти; 4) шахраї-гастролери; 5) шахраї, що здійснюють шахрайство, що продовжується. Окремо був виділений тип шахрая-аферіста.

О. В. Рудзитис, ґрунтуючись на результатах свого дослідження кримінології, розрізняє випадкових, ситуаційних, злісних та особливо небезпечних шахраїв.

В результаті аналізу праць вчених та емпіричного матеріалу, ми отримали змогу запропонувати наступну класифікацію особи шахрая: 1) «випадкові шахраї», що уперше скоїли злочини – їх меншість; 2) особи, раніше судимі за шахрайство та інші особи, що не мають постійного джерела доходу; 3) особи, що здійснюють так зване шахрайство, «що триває», полягає в отриманні яких-небудь матеріальних благ; 4) шахраї-професіонали, спосіб життя яких пов'язаний із систематичним здійсненням злочинів, які є для них основним джерелом отримання коштів для існування. Ці шахраї найбільш небезпечні та заподіюють значний матеріальний збиток громадянам [4, с. 51].

Доцільно класифікувати шахраїв за місцем скоєння злочину на осіб, що здійснюють шахрайство за місцем проживання та гастролерів.

Оскільки арсенал шахрайських прийомів різноманітний, то в науковій літературі зустрічається кваліфікація шахраїв ще по таких групах: шулери, аферисти, ляльокарі, шнеерзони і формазони [4, с. 53].

Особа шахрая значно відрізняється від особи інших злочинців (злодіїв, грабіжників, хуліганів), незважаючи на зовнішню схожість багатьох характеристик – вікових і соціальних груп, наприклад, часу та місць скоювання злочинів. В більшості своїй шахраї мають хитрий, виверткий розум, акторські здібності, розвинену фантазію, уміння орієнтуватися в складній обстановці та такій, що швидко змінюється, а також використовувати обстановку, що складається, у свою користь та отримувати з цього вигоду, тобто це люди, що мають певні знання в психології людини.

Шахраєві властивий розвинений інтелект, сила переконання, витончена наполегливість в реалізації злочинного задуму. Безпосередній контакт з потерпілим вимагає товариськості, уміння підтримувати розмову на різні теми, певної сміливості [5].

Розвитку здібностей до обману сприяють природні (природжені) властивості та постійний тренінг. Це – спостережливість (прозорливість), спритність (передусім рук), здатність до ризику, сміливість, авантюризм, винахідливість, відсутність або слабкі позитивні соціальні орієнтації (совість). Здатність до обману у шахраїв індивідуальна та варіюється в різних межах залежно від ціннісних орієнтацій. Шахрай ідеально володіє мімікою, особливо виразом очей, викликаючи до себе довіру, майстерно блефує, чуйно реагуючи на зміни зовнішніх обставин. Професійна орієнтація шахраїв стійка. На

формування особи злочинця великий вплив чинять економічні, соціальні протиріччя, особливості життя різних верств населення. Професійні шахраї досить легко розгадують собі подібних.

Вивчення особи шахрая свідчить про їх високий професіоналізм, вузьку спеціалізацію, досить широкий кругозір, правові знання [6, с. 21].

Підсумовуючи наведене, можна зробити умовивід, що виявлення типових моделей особи шахрая, знання основних рис цих людей дозволить звузити коло осіб, серед яких доцільно вести пошук суб'єктів, які вчинили шахрайство. Така характеристика дозволяє висунути версії про мотив та мету злочину, про спосіб здійснення і приховання злочину, про місце знаходження речей, що стали об'єктом злочинного посягання або якими незаконно заволоділи під час вчинення злочину.

Список використаних джерел:

1. Ахмедшин Р. Л. Криминалистическая характеристика личности преступника : автореф. дис. … д-ра юрид. наук / Ахмедшин Р. Л. – Томск, 2006. – 20 с.

2. Клейменов М. П. Криминологическая характеристика и профилактика мошеннических посягательств на личную собственность : учеб. пособие / М. П. Клейменов. – Омск, 1980.– С. 39–42.

3. Навроцкий В. О. Теоретичні проблеми кримінально-правової кваліфікації / В. О. Навроцький. – К. : Атіка, 1999. – 158 с.

4. Волженкин Б. В. Мошенничество / Б. В. Волженкин. – СПб., 1998. – 234 с. – (Серия «Современные стандарты в уголовном праве и уголовном процессе»).

5. Ермолович Д. В. Некоторые поисковые социально-психологические признаки личности мошенника [Електронний ресурс] / Ермолович Д. В., Широких С. В. – Режим доступу: http://www.shkolny.com/nekotoryie-poiskovyie-sotsialno-psihologicheskie-priznaki-lichnosti-moshennika/. – Сайт ж-ла «Юрист он-лайн», електрон. каталог б-ки юр.фак. СПбГУ.

6. Попов С. Зловживання довірою при шахрайстві // Кримінальне право. – № 9. – 2004. – С. 21-25.

Отримано 23.11.2012

УДК 343.53

Віталій Миколайович КІЙКОВ
викладач кафедри інформаційної безпеки факультету психології,
менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ
Олексій Павлович МАКАРЕНКО
магістрант групи СТЗІ АМ 12-1
Харківського національного університету радіоелектроніки

ВИКОРИСТАННЯ В УКРАЇНІ ЕЛЕКТРОННИХ ЗАСОБІВ КОНТРОЛЮ МІСЦЯ ЗНАХОДЖЕННЯ ОСОБИ

Розглянуто актуальність та шляхи використання трекінгових пристроїв в Україні. Проведено аналіз зарубіжного досвіду, розглянуто переваги та недоліки електронних моніторингових систем.

На даний час в Україні гостро стоїть питання з переповненістю закладів пенітенціарної системи осудженими та осіб, що перебувають у слідчих ізоляторах. В Україні запобіжний захід у вигляді утримання під вартою застосовується набагато частіше порівняно з іншими країнами світу. За результатами дослідження серед 217 країн за кількістю ув'язнених на 100 тис. населення Україна посідає 10 місце [1].

Зменшення кількості осіб, що перебувають у місцях позбавлення волі – одна із вимог на шляху інтеграції України до Європейського Союзу. На сьогодні дана проблема вирішується шляхом умовно-дострокового звільнення осіб з місць позбавлення волі. У вирішенні цього питання буде цікавим розглянути досвід країн, де запроваджений електронний моніторинг, як вид покарання, або як альтернатива запобіжному заходу – «взяття під варту».

Електронний моніторинг (далі – ЕМ) – технологія, що застосується тільки за рішенням суду по відношенню до особи та полягає в обмеженні його права на пересування. Системи ЕМ можуть включають у себе: пристрої для контролю домашнього арешту, ручні або ніжні браслети, GPS системи, алкотестери та пристрої розпізнавання голосу [2].

Питання електронного моніторингу засуджених досліджували такі закордонні вчені як, K.W. Cooprider and J. Kerby, William Bales, Karen Mann, Thomas Blomberg, Gerry Gaes, Kelle Barrick, Karla Dhungana, Brian McManus, Peter Hall, John F. Tewey. В Україні дана тема тільки набуває актуальності у науковому середовищі.

Закордоном технологія ЕМ широко використовується для домашнього арешту. Спеціальний прилад, що зазвичай закріплений на

засудженій особі, випромінює свій унікальний кодований сигнал на приймач, що знаходиться у помешканні. Радіочастотні прилади не відслідковують місцезнаходження засудженого, як GPS системи, а дозволяють встановити чи знаходиться засуджений вдома у певний час, чи виконує він визначені судом вимоги домашнього арешту.

Також існують пасивні GPS трекінгові системи, які відстежують рух і записують інформацію, що загружається на сервер пульту спостереження раз на добу. Активні GPS трекінгові системи відстежують місцезнаходження у реальному часі. В контролюючому пристрої запрограмована інформація про дозволені та заборонені райони для перебування особи.

Застосування електронних моніторингових приладів розглядається як альтернатива позбавленню волі за певний ряд злочинів, що має бути чітко визначеним законодавцем, або як альтернатива такому запобіжному заходу як взяття під варту. ЕМ системи можуть бути засновані у відношенні до осіб: умовно засуджених, достроково звільнених; як запобіжний захід на стадії досудового слідства та альтернатива підписки про невиїзд, яка у зв'язку з прийняттям нового Кримінального процесуального Кодексу України буде скасована. Натомість, вводиться новий вид запобіжного заходу – домашній арешт [4, ст. 195].

ЕМ офіційно впроваджений і працює у світі понад двадцять років. Дослідження застосування ЕМ одностайно вказують на значні фінансові заощадження коштів держави у порівнянні з традиційним ув'язненням [5]. Інший аспект преваг за даними досліджень – значне зменшення кількості рецидивів серед осіб по відношенню до яких було застосовано ЕМ, наприклад, до 75 % серед підлітків північної Кароліни, США [6].

Серед недоліків ЕМ виділяють проблематичність визначення місцезнаходження людини, що скоїла побіг і покинула визначений район, хоча засіб і надасть сигнал тривоги. Також, на стабільність роботи GPS системи, що передають сигнал за допомогою стільникового зв'язку впливає стабільність мережевого покриття та можливі технічні проблеми з живленням батареї пристрою стеження.

Ряд досліджень [7; 8] вказують на негативний емоційний та психологічний ефект, особливо серед підлітків, пов'язаний з використанням ЕМ.

Висновки. Отже, електронний моніторинг засуджених – тема нова для України і багатогранна, її актуальність не викликає сумнівів. Впровадження даних пристроїв потребує доопрацювання законодавчої бази, щоб повністю регламентувала їх використання. Також, науково-

технічний аспект використання трекінгових пристроїв, їх адаптація до специфіки України на сьогодні є невирішеною проблемою, що представляє нову площину для науково-дослідницької роботи. Саме з дослідженням у сфері технічного забезпечення імплементації ЕМ, оцінки ефективності роботи трекінгових приладів і буде пов'язана наша подальша робота.

Список використаних джерел:

1. Україна – десята у світі за кількістю ув'язнених [Електронний ресурс]. – Режим доступу: http://tsn.ua/ukrayina/ukrayina-desyata-u-sviti-za-kilkistyu-uv-yaznenih.html.

2. Keeping Track of Electronic Monitoring [Електронний ресурс] // Justnet: National Law Enforcement and Corrections Technology Center Bulletin. – Oct. 1999. – Режим доступу: http://www.justnet.org/Lists/JUSTNET%2520Resources/Attachments/859/Elec-Monit.pdf.

3. John F. Tewey, Maryland Task Force to Study Criminal Offender Monitoring by Global Positioning Systems. Final Report to the Governor and General Assembly (Dec. 31, 2005) [Електронний ресурс] / John F. Tewey – Режим доступу: http://www.ok-rsol.org/resources/GPS_Task_Force_Final_Report.pdf.

4. Кримінальний процесуальний Кодекс України [Електронний ресурс]: Закон України від 13.04.2012 № 4651-VI, редакція від 15.08.2012. – Режим доступу: http://zakon.rada.gov.ua/laws/show/4651-17/page2.

5. Charles M. Research Note: Juveniles on Electronic Monitoring / Michael T. Charles // Journal of Contemporary Criminal Justice. – August 1989. – № 5. – P. 165–172.

6. Sklaver Stacey, The Pros and Cons of Electronic Monitoring Programs in Juvenile Cases. [Електронний ресурс] / Stacey L. Sklaver. // American Bar Association. Criminal Justice. – Режим доступу: http://www2.americanbar.org/sections/criminaljustice/PublicDocuments/jjSklaver.doc.

7. Tarrant County, Immediate Home Detention – Electronic Monitoring [Електронний ресурс]. – Режим доступу: http://www.tarrantcounty.com/ejuvenile/cwp/view.asp?A=737&Q=427717.

8. Electronic Monitoring Program. Rules and Participation Agreement – Juvenile Program [Електронний ресурс] // City and County of Denver. – Режим доступу: http://www.denvergov.org/Portals/676/documents/Juvenile%20Rules.pdf.

Отримано 19.11.2012

УДК 351.74:004

Оксана Вікторівна КІОРЄСКУ
викладач кафедри інформатики та інформаційних систем і технологій в діяльності ОВС факультету психології, менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ
Артем Олександрович ЯСЬКО
викладач кафедри математичного моделювання та інформаційних технологій навчально-наукового інституту права та масових комунікацій
Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ ДОСВІДУ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ У ВПРОВАДЖЕННІ НОВІТНІХ ТЕХНОЛОГІЙ В ДІЯЛЬНІСТЬ ПРАВООХОРОННИХ ОРГАНІВ УКРАЇНИ

Роботу присвячено аналізу використання в діяльності російських правоохоронних органів додатку «Мобільна поліція» як позитивного досвіду для України в сфері застосування новітніх технологій в системі МВС.

З огляду на зміни, що відбуваються у всіх сферах суспільного життя в контексті євроінтеграційних процесів, Україна встала на шлях реформування правоохоронної системи з метою наближення її діяльності до міжнародних стандартів. За таких обставин проект закону «Про поліцію» містить ряд положень, які не тільки кардинально відрізняються від положень діючого сьогодні закону України «Про міліцію», а й зовсім не були враховані на час його прийняття. Слід підкреслити, що врахування позитивного досвіду таких держав, як Російська Федерація, Республіка Білорусь, Грузія, Республіка Польща, Ізраїль, Німеччина, Швеція та США, знайшло своє відображення в законодавчому закріпленні принципу використання досягнень науки і техніки, сучасних технологій та інформаційних систем у діяльності поліції (ст. 29) [1]. Таким чином, з прийняттям закону України «Про поліцію» передбачається створення та розвиток правового підґрунтя для впровадження досягнень науки і техніки в діяльність поліції.

Враховуючи позитивні практичні здобутки в сфері використання сучасних технологій в роботі правоохоронних органів, вважаємо за доцільним звернути увагу на пілотний проект в Російській Федерації «Мобільна поліція», як приклад впровадження новітніх технологій в повсякденну роботу працівників поліції, та можливість використання розробок російських фахівців задля оптимізації виконання вітчизняними правоохоронцями своїх функціональних

представників організації-виконавця проект є першим та являє собою спеціальний додаток для мобільних телефонів [4]. Розробка була ініційована громадською радою при головному управлінні МВС по Центральному федеральному округу, а виконавцем стала регіональна громадська організація «Наше місто».

Програма включає в себе три основні функції: оперативний виклик поліції, онлайн-визначення координат власника телефону та інформаційний довідник для людей, що опинилися у критичній ситуації. У «Мобільній поліції» екстрений виклик дублюється одночасної розсилкою SMS-повідомлень певному колу заздалегідь вибраних користувачем осіб, у яких також встановлено додаток. Отримавши сигнал і побачивши координати людини з прив'язкою до карти місцевості, друзі та родичі постраждалого можуть самі приймати рішення, піднімати або не піднімати тривогу [4].

Зчитувати координати і відслідковувати переміщення користувача можна і в реальному часі – без екстрених викликів і SMS (зрозуміло, якщо людина сама того забажає). Для економії трафіку координати будуть оновлюватися раз на п'ять хвилин, а їх видалення з пам'яті системи відбуватиметься рівно через добу. На думку члена правління «Наше місто» Д. Жабіна ситуації бувають різними і приватність не завжди розумна [4]. Наприклад, вирушаючи на мітинг, завжди варто бути готовим до різних провокацій. Водночас вирішується і питання батьківського контролю над дітьми, оскільки до певного віку доступність інформації про місцезнаходження дитини явно буде сприяти її безпеці.

Третя складова «Мобільної поліції» – інформаційна. У програмі є довідник з номерами телефонів різних служб і структур МВС і актуальне оперативне зведення про криміногенну обстановку. Крім того, розробники передбачили набір деяких шаблонів-пам'яток та інструкцій до дій в різних нестандартних і потенційно небезпечних ситуаціях.

Всі три складові "мобільного поліції" так чи інакше вже були десь реалізовані окремо, проте, за твердженням Д. Жабіна, комплексного аналога поки не робив ніхто на території Російської Федерації.

Додаток поки працює на рівні московського регіону і подальша його доля залежить від того, наскільки він буде затребуваним громадянами, а також від зацікавленості територіальних органів МВС.

Резюмуючи вищенаведені відомості, зазначимо, що впровадження вітчизняного аналогу російської системи «Мобільна поліція» в діяльність українських правоохоронців сприятиме реалізації превентивної функції майбутньої поліції та стане одним із важливих кроків до партнерських відносин з громадянами.

Список використаних джерел:

1. Про поліцію [Електронний ресурс] : проект закону України. – Режим доступу: http://www.rovenkipolice.org.ua/wp-content/files/proekt_police.pdf.

2. Про міліцію [Електронний ресурс] : закон України від 20.12.1990 № 565-XII. – Режим доступу: http://zakon.rada.gov.ua/laws/show/565-12/page3.

3. О полиции [Електронний ресурс] : Федеральный закон от 07.02.2011 № 3-ФЗ. – Режим доступу: http://www.zakonprost.ru/zakony/o-policii/.

4. Военков Д. Мобильная полиця – в телефоне гражданина [Електронний ресурс] / Д. Военков. – Режим доступу: http://www.newsland.ru/news/detail/id/943142/.

Отримано 12.11.2012

УДК 004.4

Максим Олександрович КНИЖЕНКО
старший державний податковий інспектор відділу супроводження інформаційних систем та адміністрування баз даних Дзержинської державної податкової інспекції м. Харкова
Сергій Леонідович ХАРЧЕНКО
старший викладач кафедри програмної інженерії Харківського національного університету радіоелектроніки

ДО ПИТАННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ

Розглянуто актуальні питання запровадження інноваційних технологій до оперативно-розшукової діяльності правоохоронних органів держави. Запропоновано шляхи вдосконалення системи управління баз даних, що забезпечують діяльність силових структур правоохоронних органів.

ног до роботи силових структур має
му та достовірному інформаційному
наявність розвиненої спеціалізованої інформаційної системи. Така система повинна забезпечити співробітника правоохоронних органів оперативною інформацією за його запитом, у будь якому місті, часі та в межах його функціональних обов'язків та повноважень.

Функціонування такої системи повинно бути засновано на взаємодії, на рівні обміну інформації, між інформаційними системами структурних підрозділів міністерства внутрішніх справ та інформаційних систем інших державних організацій, що мають бути поєднані у єдину державну інформаційну систему.

Організація роботи інформаційної системи має бути побудована на принципах застосування розподіленої система керування базами даних (далі – СКБД), де кожна структура відповідає за наповнення та ведення свого сегменту загальної бази даних та забезпечує можливість оперативного отримання довідкової інформації по контрольованому запиту, тільки в межах службових повноважень особи, яка виконує таку операцію. Будь-яке звернення, яке не відповідає службовим повноваженням або таке що скероване на отримання інформації з суміжних структур, до інформаційної системи, повинно бути зафіксоване у відповідних журналах безпеки, а його виконання заблоковано.

Інформацію яку може отримати співробітник суміжних структур або інших державних установ повинна відповідати його повноваженням та має відноситись до розряду звітної. Любі спроби

внести зміни до інформації, що зберігається у базі даних, повинні бути зупинені та зафіксовані у журналах безпеки, якщо цю операцію виконує не вповноважена особа.

Висока швидкість виконання пошукових запитів від співробітників правоохоронних органів на різних ділянках роботи унеможливить реалізацію окремих видів, що віднесені до традиційної злочинності. А появі нових видів злочинності, що відносяться до так званих «кіберзлочинів» можуть ефективно протидіяти фахівці що будуть готовитися у межах виконання поточного проекту.

Однією з головних складових інформаційної системи є СКБД, яка відповідає за роботу з інформацією. Сучасні вимоги до СКБД повинні враховувати такі види навантажень:

– безперервне завантаження даних;

– велика кількість стандартних звітів, які потребують відповідних робіт з SQL та створення індексів (слід враховувати можливість десятків тисяч запитів у годину);

– зростаюча кількість користувачів з нерегламентованими запитами;

– зростаючий обсяг аналітики та виконання специфічних завдань.

Вищевідзначене, вимагає, в свою чергу, дотримання двох важливих показників до обраної СКБД:

– можливість повноцінного функціонування та підтримки;

– повнота та завершеність.

Доцільно зауважити, що у 2006 році, згідно з оцінкою компанії Gartner, лідерами у цьому сегменті ринку були корпорації Teradata, IBM та Oracle.

Створення такої інформаційної системи вимагає наявності фахівців здатних проектувати, реалізовувати та адмініструвати систему такої складності і масштабу. Тому доцільно при підготовці кадрів передбачити таку можливість. Це обумовлено необхідністю у «відборі» кадрів, які матимуть доступ до структури інформаційної системи та інформації віднесеної до грифа «таємниця». Крім цього, такі фахівці повинні мати підготовку, яка відповідає статусу адміністратор ОС, СУБД, мережі та інформаційної системи і повинні бути здатні виконувати роботу по захисту інформації на різних рівнях функціонування.

Для цього пропонується створити на базі навчального закладу відповідну наукову лабораторію по розробці програмного забезпечення та адміністрування баз даних.

Таким чини запропонований підхід до створення загальнодержавної інформаційної системи відповідає вимогам часу та має перспективи в подальшому використанні.

Список використаних джерел:

1. Гнатуш А. Реинжиниринг: многое в малом / А. Гнатуш // «IT Manager». – 2004. – № 4 (16). – С. 24.

2. Ксензов М. В. Рефакторинг архитектуры программного обеспечения // Труды Института Системного Программирования РАН, Препринт 4. – Москва, 2004. – 30 с.

3. Пери Джеймс Введение в Oracle 10g / Пери Джеймс, Пост Джеральд ; [пер.с англ]. – М. : ООО «И.Д.Вильямс», 2006. – 704 с.

4. Власов А. И. Краткое практическое руководство разработчика информационных систем на базе СУБД ORACLE / А. И. Власов, С. Л. Лыткин, В. Л. Яковлев [Електроний ресурс]. – Режим доступу: http://www.citforum.ru/database/oraclepr/index.shtml.

Отримано 10.11.2012

—

УДК 681.004

Ігор Володимирович КОБЗЕВ
кандидат технічних наук, доцент,
доцент кафедри інформатики та інформаційних систем і технологій в діяльності ОВС факультету психології, менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ
Віталій Вікторович РЕЗЬ
курсант групи ФПТ-09-2 факультету психології, менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ

БЕЗПЕКА СИСТЕМИ ТЕСТУВАННЯ ПРИ ВИКОРИСТАННІ МУЛЬТИАГЕНТНИХ ТЕХНОЛОГІЙ В СИСТЕМАХ ДИСТАНЦІЙНОГО НАВЧАННЯ

Розглянуто питання протидії несанкціонованому витоку інформації при проведенні тестування в системах дистанційного навчання з використанням мультиагентних систем.

В наш час системи дистанційного навчання часто являють собою великі територіально розподілені комплекси, неоднорідні як за складом технічних засобів, так і програмному забезпеченню. Завдання дослідження та моделювання таких систем традиційними методами стає все більш важким, і вимагає нових підходів для свого рішення. Одним із таких підходів є теорія мультиагентних систем, що дозволяє описати будь-яку велику систему у вигляді безлічі інтелектуальних агентів різних видів, які взаємодіють між собою.

Одним з найважливіших інформаційних процесів систем дистанційного навчання є відтворення інформації, формування, управління і контроль над інформаційними потоками, що приводять до перерозподілу інформації. Найчастіше процес перерозподілу і доступу до інформації, що надається системою, регламентується низкою правил. Це призводить до необхідності створення різних механізмів контролю та обмеження доступу, а також ставить задачу виявлення порушень введених обмежень.

Найбільш поширеним базовим механізмом розмежування доступу є реєстрація і подальша аутентифікація користувача в системі. Ефективна протидія несанкціонованої витоку інформації можлива тільки при створенні багаторівневої інтелектуальної системи фільтрації інформації та обмеження прав доступу до неї. В системі тестування передбачається використовувати наступні обмежувальні механізми: механізм захисту від розкриття точних формулювань правильних відповідей; механізм захисту від розкриття інформації про

аріанту відповіді; механізм захисту від
що гарантують певну оцінку; механізм
аріанта відповіді для питання, на який відповідь вже була дана; механізм захисту від нерегламентованої навігації по системі під час проходження атестації і т.д.

Разом з тим досвід систем тестування системи переконує, що традиційних засобів протидії несанкціонованому витоку інформації в інфокомунікаційних системах недостатньо. Тому існує потреба в розробці нових систем контролю над інформаційними потоками, покликаних не тільки обмежити доступ до тих або інших даних, але і виявити зміни в інформаційних потоках і появи несанкціонованих просочувань в систему.

Базисом створення таких систем контролю над інформаційними потоками системи можуть стати мультиагентні системи (multi-agent system), побудовані на основі інтелектуальних агентів, які аналізують в режимі реального часу інформаційні потоки, з метою виявлення несанкціонованих просочувань інформації.

Критерієм виявлення несанкціонованих просочувань інформації можуть стати ентропійні характеристики системи, що описують невпорядкованість дій користувача або функціонування певних фрагментів системи. Успішне функціонування подібної системи залежить від двох основних факторів. По-перше, необхідно правильно побудувати модель мультиагентної системи, розмістивши інтелектуальні агенти відповідних типів у всіх ключових вузлах системи. що беруть участь в обробці інформації, витік якої необхідно запобігти. По-друге, необхідно правильно вибрати характеристики системи, ентропія яких буде використовуватися як індикатор несанкціонованого витоку інформації.

Сама ж система повинна вирішувати три основні завдання: виявлення несанкціонованого витоку інформації; виявлення причини і адресата несанкціонованого витоку інформації; блокування небажаної діяльності з метою запобігання витоку інформації.

Особливо звернемо увагу, що подібна система не просто складається з великої кількості однотипних агентів, а включає в себе велику кількість інтелектуальних агентів різних типів, які відповідають різним рівням абстракції (обробки) інформації, що захищається. Це дозволяє контролювати інформацію на всіх рівнях, які можуть стати джерелом витоку, а також використовувати велике число різних ентропійних характеристик, що підвищують надійність системи захисту. Крім того, різнотипність агентів і використовуваних «сигнальних» характеристик ускладнює адаптацію небезпечних процесів з метою маскування несанкціонованого витоку інформації регламентованими діями.

Вимоги до мультиагентної системи виявлення та запобігання несанкціонованих просочувань інформації закладають базис їх створення, одночасно підказуючи напрямок розвитку, що полягає в пошуку і формалізації ентропійних характеристик систем дистанційного навчання, які можуть служити індикаторами несанкціонованих просочувань інформації.

Отримано 05.11.2012

УДК 343.85:343

Валерій Васильович КОЛОСКОВ
кандидат юридичних наук, доцент,
професор кафедри спеціальних дисциплін факультету ОРД та права
Національної академії Державної прикордонної служби України
ім. Б. Хмельницького

ОКРЕМІ АСПЕКТИ ЗАКОНОДАВЧОГО РЕГУЛЮВАННЯ ЗАПОБІГАННЯ ЗЛОЧИНАМ НА ДЕРЖАВНОМУ КОРДОНІ УКРАЇНИ

Розглянуто окремі аспекти законодавчого регулювання запобігання злочинам на державному кордоні України.

Вже більше двадцяти років законодавці України намагаються вдосконалити правове регулювання протидії злочинній діяльності. Було прийнято ряд законодавчих актів, котрі визначають функції правоохоронних органів. У першу чергу, – це стосується суб'єктів оперативно-розшукової діяльності, їх обов'язків та прав.

Останній час, особливо 2012 рік, «відзначається» швидкоплинними змінами та доповненнями до законодавчих актів. Законодавці, намагаючись досягнути європейських стандартів захисту честі і гідності людини, протидії злочинності, недопущення правопорушень з боку працівників правоохоронних органів у процесі досудового розслідування, у ході судового слідства – вносять зміни і доповнення до діючих законодавчих актів. Проте, це не говорить про те, що якість законодавства стає кращою, діяльність працівників

об'єктивними, а рішення судів

оналості законодавчих актів, у першу чергу тих, що стосуються оперативно-розшукової, розвідувальної та контррозвідувальної діяльностей, – є те, що у їхньому створенні не беруть участі вчені-представники зазначених видів діяльності. Ця тематика є гострою проблемою сьогодення. Проте, хочеться сказати про один із останніх законодавчих актів, а саме – Кримінально-процесуальний кодекс України (КПК).

Немає сумніву, що його створення у відповідності до сьогодення та перспективи розвитку нашої держави є необхідним. Виникає питання: чи готові правоохоронні органи України, судова система до діяльності у відповідності до вимог прийнятого Кримінально-процесуального кодексу України. Ознайомившись із ним, виникає дуже багато питань: як працювати в сучасних умовах

оперативним підрозділам, адже згідно зі ст. 5 Закону України «Про оперативно-розшукову діяльність», таких суб'єктів уже є дев'ять. Це добре, адже те, що митні органи України теж здійснюватимуть оперативно-розшукову діяльність – великий позитив.

Не дивлячись на те, що назва даної роботи – «Окремі аспекти законодавчого регулювання запобігання злочинам на державному кордоні України», ця проблематика стосується усіх суб'єктів оперативно-розшукової діяльності України.

Враховуючи вимоги до об'єму роботи, хочеться зупинитись на декотрих моментах прийнятого Кримінального процесуального кодексу України.

У пункті 1 ст. 246 даного Кодексу, зазначається: «Негласні слідчі (розшукові) дії – це різновид слідчих (розшукових) дій, відомості про факт та методи проведення яких не підлягають розголошенню, за винятком випадків, передбачених цим Кодексом».

Далі, у пунктах 3 та 4 цієї статті, говориться:

«3. Рішення про проведення негласних слідчих (розшукових) дій приймає слідчий, прокурор, а у випадках, передбачених цим Кодексом, – слідчий суддя за клопотанням прокурора або за клопотанням слідчого, погодженого з прокурором. Слідчий зобов'язаний повідомити прокурора про прийняття рішення щодо проведення певних негласних слідчих (розшукових) дій та отримані результати. Прокурор має право заборонити проведення або припинити подальше проведення негласних слідчих (розшукових) дій.

4. **Виключно прокурор** (виділено нами – авт.) має право прийняти рішення про проведення такої негласної слідчої (розшукової) дії, як контроль за вчиненням злочину».

Питається: а яка ж тоді роль оперативного працівника? Чи має він право самостійно приймати рішення на здійснення негласної розшукової дії за наявності оперативно-розшукової справи? Судячи з пункту 4 ст. 246 Кримінального процесуального кодексу України – ні. Для чого ж тоді є оперативно-розшукові підрозділи, лише для того, щоб виконувати рішення проведення негласних слідчих (розшукових) дій слідчого, прокурора або слідчого судді за клопотанням прокурора або за клопотанням слідчого, погодженого з прокурором? Раз вони наділені правом здійснювати негласні слідчі (розшукові) дії, нехай тоді й здійснюють їх самостійно: готують клопотання, здійснюють підготовку за здійснення заходів, їхнього конспіративного забезпечення тощо.

В оперативно-розшукових підрозділах досвід здійснення таких заходів є і, очевидно, це буде перекладатись на їхні плечі, хоча в КПК це не передбачено.

Теж цікаво, виконання ст. 253 Кримінального процесуального кодексу України «Повідомлення осіб, щодо яких проводилися негласні слідчі (розшукові) дії». Виходячи з пункту першого даної статті, повідомляються усі особи, конституційні права яких були тимчасово обмежені під час проведення негласних слідчих (розшукових) дій, а також підозрюваний, його захисник мають бути письмово повідомлені прокурором або за його дорученням слідчим про таке обмеження.

Багато є питань й щодо статей параграфу другого глави 21 Кримінального процесуального кодексу. Проте у зв'язку з регламентним обмеженням розглянути їх не представляється можливим.

Хотілось би щоб це спонукало до подальшої полеміки на сторінках наукових видань з даної проблематики, подання до Верховної Ради України своїх пропозицій щодо покращання КПК України стосовно негласних слідчих (розшукових) дій.

Отримано 25.11.2012

УДК 621.37

Володимир Олександрович КОЧУРА
кандидат технічних наук, старший науковий співробітник
доцент кафедри інформатики та інформаційних систем і технологій
в діяльності ОВС факультету психології, менеджменту, соціальних
та інформаційних технологій
Харківського національного університету внутрішніх справ

АНАЛІЗ ПРИНЦИПІВ ПОБУДОВИ ЗАСОБІВ БЛОКУВАННЯ МОБІЛЬНОГО ЗВ'ЯЗКУ

Проаналізовано основні принципи побудови засобів блокування мобільного зв'язку.

У системі захисту каналів витоку інформації завдання блокування витоку по каналах мобільного зв'язку є надзвичайно актуальним. Це пов'язано як із зростанням об'єму інформації, що

передається по каналах мобільного зв'язку, так і розвитком технологій її перехоплення. Сучасні засоби дозволяють не лише здійснювати доступ до телефонних переговорів та СМС повідомлень, але також використовувати мобільний телефон як прихований підслуховуючий пристрій для негласного знімання даних і мовної інформації.

На сьогодні можна виділити декілька основних способів перехоплення інформації що передається засобами мобільного зв'язку.

По-перше, це прослуховування операторами мобільного зв'язку, що мають можливість здійснювати контроль переговорів, отримувати іншу інформацію по номеру телефону або по IMEI стільникового телефону.

Другий спосіб, це перехоплення даних (від телефону до базової станції і навпаки) спеціальним засобами, які, після отримання, розшифровують зашифрований цифровий сигнал. Цей спосіб, при придбанні відповідного устаткування, стає доступний не лише спеціальним службам.

Третій спосіб, це використання спеціального програмного забезпечення, яке встановлюється на стільниковий телефон, що прослуховується.

Крім того, завдання продавлення сигналів мобільного зв'язку виникає при проведенні антитерористичних заходів при нейтралізації радіоканалів дистанційного керування.

Для запобігання витоку інформації по каналах стільникового зв'язку використовують блокувачі стільникового зв'язку GSM, 3G, CDMA – пристрої, які блокують роботу мобільного зв'язку на заданих частотах.

По принципах побудови блокувачі стільникового зв'язку можна

яться блокувачі в основним елементом

яких є генератори, що забезпечують постановку загороджувальної перешкоди в діапазоні частот роботи базових станцій відповідного стандарту, тобто в діапазоні робочих частот приймачів телефонів стільникового зв'язку. Перешкода призводить до зриву управління телефоном стільникового зв'язку базовою станцією (втрати мережі), а отже – до неможливості встановлення зв'язку і передачі інформації.

До другої групи відносяться блокувачі стільникового зв'язку, які у своєму складі, окрім передавача перешкод мають ще і спеціальний приймач, що забезпечує прийом сигналів в діапазонах частот роботи передавачів телефонних апаратів відповідного стандарту. Враховуючи, що усі системи стільникового зв'язку працюють в дуплексному режимі, спеціальний приймач

використовується як засіб автоматичного управління передавачем перешкод. При виявленні сигналу (випромінювання, рівень якого перевищує встановлений поріг) в одному з діапазонів частот, приймач видає сигнал управління на включення передавача загороджувальних перешкод відповідного діапазону частот. При пропажі сигналу, приймач видає сигнал управління на виключення передавача перешкод відповідного діапазону.

До третьої групи відносяться «інтелектуальні» блокувачі стільникового зв'язку. Приймач такого блокував протягом короткого інтервалу часу (близько 300 мкс) виявляє в контрольованій зоні випромінювання працюючого або такого, що входить в зв'язку мобільного телефону, обчислює номер частотного каналу і часовий слот виділений цьому телефону. Після обчислення частотно-часових параметрів виявленого мобільного телефону передавач перешкод налаштовується на конкретний частотний канал в діапазоні частот роботи базової станції і включається на випромінювання в ті моменти часу, в які, відповідно до стандарту GSM, мобільний телефон приймає сигнал каналу управління від базової станції. Інтервал блокування відповідає часу встановлення мобільним телефоном вхідного або вихідного зв'язку, і складає близько 0,8-1 с. Блокування здійснюється короткими імпульсами тривалістю по 300 мкс кожен, з періодом 4,616 мс. Сумарний час, протягом якого в інтервалі блокування випромінюється сигнал перешкоди, не перевищує 0,05-0,07 с.

Якщо в контрольованій зоні опиняється працюючий мобільний телефон із вже встановленим зв'язком, інтервал блокування збільшується до 10–15 с, і, відповідно, збільшується час випромінювання сигналу блокування.

Після закінчення часу інтервалу блокування зв'язок припиняється. Таким чином, забезпечується неможливість здійснення вхідних та вихідних дзвінків, прийом і відправлення СМС, а також уривається вже встановлений сеанс зв'язку.

Випромінювання передавача перешкод блокувача носить строго адресний характер, впливає на мобільні телефони, що знаходяться усередині встановленої зони закриття, і не створює перешкод для роботи стільникової мережі в цілому. Рівень випромінювання передавача перешкод блокувача повністю еквівалентний рівню випромінювання стільникового телефону і відповідає вимогам міжнародного стандарту GSM для абонентської апаратури. Зона закриття визначається не потужністю сигналу перешкоди, а рівнем порогу спрацьовування пристрою виявлення приймача. Ефективність

роботи блокувача не залежить від близькості розташування базових станцій в зоні закриття, тобто від електромагнітної обстановки.

Отримано 16.11.2012

УДК 681.3

Олексій Феліксович ЛАНОВИЙ
кандидат технічних наук, доцент,
доцент кафедри інформатика та інформаційних систем і технологій
в діяльності ОВС факультету психології, менеджменту, соціальних
та інформаційних технологій
Харківського національного університету внутрішніх справ
Андрій Вікторович ГАЛИЧ
курсант групи ФПТ-09-2 факультету психології, менеджменту,
соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ

ДОСЛІДЖЕННЯ ІНСТРУМЕНТАРІЮ АНАЛІЗУ ВРАЗЛИВОСТІ ПРОГРАМНОГО КОДУ

Представлено порівняльне дослідження відомих програмних аналізаторів з відкритим вихідним кодом з точки зору безпеки додатків. Розглянуто динамічний і статичний аналіз програмного коду.

ці програмного забезпечення, часто, в коді, в тому числі ці помилки додатків. В даний час існує безліч різних інструментів статичного аналізу коду, за допомогою яких можна виявити проблеми безпеки, певна частина таких інструментів може розглядатися як застарілі. Одні, наприклад, інструменти можуть вирішувати тільки якісь певні завдання, інші підходять тільки для окремої мови програмування.

Матеріали та огляди, в яких би порівнювалися ці інструменти, аналізувалися принципи їх дії, а так само виявлялися б найбільш ефективні, практично відсутні. У силу цього становить інтерес порівняльне дослідження відомих аналізаторів з відкритим вихідним

кодом з метою виявлення найбільш ефективних. Таке завдання і ставиться в цьому дослідженні.

Існуючі способи аналізу захищеності програмного забезпечення можна умовно розділити на дві групи: це інструментальний аналіз і ручний аналіз. Тобто аналіз вихідного коду може проводитися, як вручну, так і за допомогою спеціального програмного інструментарію. Сам по собі інструментальний аналіз вихідного коду може бути статичним і динамічним.

Динамічний аналіз коду – це аналіз програмного забезпечення (ПЗ), вироблений за допомогою виконання програм на реальному або віртуальному процесорі.

Статичний аналіз коду – це аналіз програмного забезпечення, вироблений над вихідним кодом програми без реального виконання досліджуваної програми. Статичний аналіз вихідного коду може бути корисний тим, що дозволяє швидко знайти і усунути потенційні уразливості в вихідному коді, автоматизувати тестування на уразливості. Крім того статичний аналіз можна інтегрувати в цикл розробки ПЗ.

Можна також проводити аналіз вихідного коду або тестування методом «чорної скриньки» (black box testing). Тестування методом «чорної скриньки» – це тестування без знань про об'єкт, що тестується, з відсутністю доступу до вихідного коду. Такий спосіб може бути корисний для оцінки захищеності додатка з позицій визначення потенційних можливостей зловмисника.

УДК 343.85:343.915

Юлія Іванівна ЛАПТІЙ
інспектор групи адміністративної практики полку патрульної служби ХМУ ГУМВС України Харківській області

ШЛЯХИ ВИРІШЕННЯ ПРОБЛЕМИ ПРОГУЛІВ ЗАНЯТЬ НЕПОВНОЛІТНІМИ ОСОБАМИ У НАВЧАЛЬНИХ ЗАКЛАДАХ ЯК ОДИН ІЗ НАПРЯМКІВ ПОПЕРЕДЖЕННЯ ЗЛОЧИННОСТІ СЕРЕД НЕПОВНОЛІТНІХ В США

Розглядаються заходи, що вживаються працівниками міліції (поліції) з метою недопущення неповнолітніми особами

систематичного пропуску занять без поважних причин в навчальних закладах США та України, як один з важливих напрямків попередження злочинності серед неповнолітніх. Узагальнюється теоретичний та практичний досвід США щодо використання профілактичних програм у даному напрямку, та можливість запровадження деяких з них в Україні.

Відсутність неповнолітніх на заняттях без поважних причин в навчальних закладах є нагальною проблемою сучасності, що потребує комплексного вирішення. Як свідчить статистика, діти, які пропускають систематично заняття в школі, у подальшому мають проблеми із працевлаштуванням, в побуті та сім'ї, навіть зростає вірогідність їх подальшого ув'язнення у зв'язку з обраним шляхом злочинності ще зі шкільної лави [1, с. 27].

Тож своєчасна профілактична робота по недопущенню неповнолітніми особами систематичного пропуску занять без поважних причин в навчальних закладах є важливим напрямком у запобіганні злочинності неповнолітніх [6].

Аналізуючи підходи до вирішення даної проблеми в Україні, чинним законодавством передбачається проведення працівниками КМСД в середніх навчальних закладах наступних профілактичних заходів: відпрацювання навчального закладу (протягом двох-трьох днів співробітники органів внутрішніх справ, представники громадськості вивчають контингент учнів, контактують з вчителями, виступають з лекціями, проводять уроки, індивідуальні бесіди, перевіряють відвідування уроків, спілкуються з батьками тощо); операція «Урок» (у денний час – з 9 до 14 години – ті ж особи відвідують місця підвищеної криміногенності – сквери, покинуті будівлі, звалища тощо), а також розважальні заклади з метою виявлення бездоглядних дітей, а також тих, хто не пішов до школи, займається дрібною спекуляцією, миттям автомашин на вулицях;

І, проводять з ними виховну роботу).

бути ефективними лише за умови налагодженої співпраці між суб'єктами

їх здійснення. Але досить часто профілактичні та виховні заходи по правовому вихованню молоді працівниками правоохоронних органів сприймаються як додаткове навантаження у роботі, яке ніяким чином не вплине на основні показники, за якими оцінюється діяльність конкретного підрозділу чи служби, присутністю формалізму у роботі структурних підрозділів ОВС у зазначеній сфері.

Проте профілактична діяльність не буде достатньо ефективною, якщо при проведенні заходів не враховувати відповідний досвід інших країн, їх ефективну практику впровадження профілактичних програм.

Дана проблема існує і в інших країнах світу, зокрема і в США. Якщо брати до уваги статистичні дані по кількості поданих на розгляд з даного питання справ, то спостерігається тенденція зростання кількості прогулів занять, – якщо в 1995 році кількість таких справ становила 32800, то на 2005 рік зросла до 52400, тобто аж на 60 % [8, с. 7].

У навчальних закладах кожного штату США існують нормативні акти, що визначають допустиму кількість пропущених учнями та студентами занять за певний проміжок часу [5, с. 33].

Проблема пропусків занять неповнолітніми учнями та студентами в США була визнана такою, що потребує негайного втручання та участі громадськості, внаслідок поширеності вчинення правопорушень та злочинів серед неповнолітніх в години занять, та бажанням громадської спільноти зменшити кількість хуліганських дій [7, с. 4].

Для ефективної протидії прогулам неповнолітніми занять науковцями були розроблені наступні вимоги, які висуваються до профілактичних програм у даному напрямку, а саме:

– заручатись підтримкою родини, громадськості та працівників поліції;

– мати довгостроково орієнтований профілактичний напрямок у роботі, та чіткі цілі;

– повинні забезпечуватись висококваліфікованими спеціалістами з необхідними навичками роботи;

– розглядати кожний окремий випадок прогулу заняття неповнолітнім з урахуванням мікроклімату в його родині, взаємовідносин з батьками;

– налагодження співпраці вчителів з батьками та громадськими організаціями в даному напрямку [2, с. 12].

На сьогодні в США розроблені та застосовуються різноманітні підходи та стратегії спрямовані на зменшення шкільних пропусків занять, серед яких виділяють програми, у впровадженні яких першочергову роль відіграють працівники школи, та навіть працівники суду [3, с. 4].

Тож розглянемо детальніше програми попередження прогулів неповнолітніми особами, які базуються на співпраці громадських організацій та поліції. На сьогодні позитивні результати показала програма запобігання прогулам – програма труант рикавери (Truant

Recovery Program). Дана програма заснована на співпраці адміністрації шкіл та працівників поліції, носить профілактичний характер, та головним завданням має повернення до школи тих дітей, що допускають пропуски занять без поважних причин [4, с. 5].

Дана програма надає повноваження поліції проводити на вулицях профілактичну роботу зі студентами в години, коли тривають заняття в навчальних закладах. Студенти, що не перебувають на занятті без поважної причини, затримуються поліцією та доставляються до офісу (SWAT office), – центру дозвілля та контролю відвідування занять студентами, працівники якого повідомляють батьків про виявлені прогули їх дітьми занять, та запрошують до центру. Якщо повідомити батьків не надається можливим, то працівники даного центру доставляють неповнолітнього до навчального закладу. Про усі виявлені факти пропусків занять дітьми повідомляються адміністрації навчальних закладів, які в подальшому у співпраці з центром відслідковують стан відвідування занять даним учнем або ж студентом [9].

Тож важливим фактором, від якого залежить успішність таких програм, є наявність чітко визначених суб'єктів для її реалізації, та їх постійна взаємодія.

Таким чином, впровадження подібної практики розробки та реалізації програм зі скорочення випадків прогулів неповнолітніми занять у США може бути використана і в Україні, як один із важливих напрямків попередження злочинності серед неповнолітніх.

Список використаних джерел:

1. Dynamic imaging of the pancreas using real-time endoscopic ultrasonography with secretin stimulation. – Catalano M.F., Lahoti S., Alcocer E. et al. – 1998. – 275 p.

2. Cooney S. M. What research tells us about effective truancy prevention and intervention programs : What Works, Wisconsin Fact Sheet / S. M. Cooney & G. Eastman. – Madison, WI : University of Wisconsin ; Madison/Extension, 2008. – 56 p.

3. Dimock K. Truancy prevention in action:Best practices and model truancy programs executive summary / K. Dimock. – National Center for School Engagement. 2005. – 52 p.

4. Finding effective solutions to truancy : What Works, Wisconsin Research to Practice Series / G. Eastman, S. M. Cooney, C. O'Connor & S. A. Small. – 2007. – 15 p.

5. Henry L. Who's Skipping School: Characteristics of Truants in 8th and 10th Grade / L. Henry // Journal of School Health. – 2007. – P. 29–35.

6. National Juvenile Court Data Archive [Електронний ресурс]. – Режим доступу: http: //www.ojjdp.gov/.../sort_publication.asp.

7. Puzzanchera C. Juvenile Court Statistics 2008 : Report / C. Puzzanchera, B. Adams & M. Sickmund. – Pittsburgh, Pa : National Center for Juvenile Justice, 2011. – 5 p.

8. Puzzanchera C. Report / C. Puzzanchera, M. Sickmund. – Washington, DC : US Department of Justice, Office of Justice Programs, Office of Juvenile Justice and Delinquency Prevention, 2008. – 7 p.

9. Truancy Prevention. OJJDP Model Program Guide [Електронний ресурс]. – Режим доступу: http://www.ojjdp.gov/.../progTypesTruancy.aspx.

Отримано 22.11.2012

УДК 343.97

Сергій Іванович ЛЕКАРЬ
кандидат економічних наук,
заступник Міністра внутрішніх справ України – керівник апарату

ПОНЯТТЯ, ЗМІСТ ТА СТРУКТУРА АДМІНІСТРАТИВНО-ПРАВОВОГО МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

Досліджено механізм адміністративно-правового регулювання забезпечення економічної безпеки держави та його роль в українському праві. Проаналізовано позиції вчених щодо цієї проблеми. Запропоновано авторський підхід до дослідження цього питання.

Подальший розвиток нашої країни та входження її як рівноправного члена до загальновизнаних геополітичних об'єднань (ООН, Європейського Союзу, СНД, ГУУАМ), безумовно, передбачає необхідність забезпечення її суверенітету та незалежності, адже саме

аву як самодостатнього та самостійного ішніх відносин. Однією з основних

, поряд із політичною, інформаційною, військовою, яка забезпечує суверенітет та незалежність держави, є економічна безпека як гарантія незалежності країни, умова стабільності та ефективної життєдіяльності суспільства.

Адміністративно-правовий механізм забезпечення економічної безпеки держави є досить складним правовим явищем. Він включає в себе ряд елементів, які в своїй сукупності покликані підтримувати економічну стабільність у крані, а також попереджати та припиняти будь-які посягання на неї. На сьогоднішній день серед науковців відсутній єдиний погляд на структуру механізму правового регулювання, у тому числі на будову механізму забезпечення економічної безпеки.

На думку С. С. Алексєєва, до елементів механізму правового регулювання відносяться: юридичні норми, правовідносини, акти реалізації суб'єктивних юридичних прав і обов'язків, нормативні юридичні акти, правову культуру і правосвідомість. У цьому переліку наявні всі правові явища, які так чи інакше врегульовано впливають на суспільні відносини [1, с. 23].

Більш повною є структура механізму адміністративно-правового регулювання запропонована Х.П. Ярмакі, який вважає, що вона включає: норми адміністративного права, адміністративно-правові відносини, акти тлумачення норм адміністративного права і акти реалізації адміністративно-правових норм [2, с. 49]. Подібної думки притримується й О. П. Коренєв, який вважає, що до структури механізму правового регулювання вводить наступні елементи:

– норми права і його принципи, об'єктивовані в нормативно-правових актах, указах Президента та інших нормативних актах;

– акти тлумачення норм права, видані уповноваженими на те організаціями;

– акти застосування норм права;

– правові відносини [3, с. 40].

Таким чином, більшість науковців зійшлися на тому, що структурними елементами механізму адміністративно-правового регулювання, у тому числі механізму забезпечення економічної безпеки, є: правові норми, правовідносини, акти реалізації норм права та акти тлумачення правових норм. Деякі науковці до вказаної структури додають ще такі явища, як нормативні акти, юридичні факти, суб'єктів та об'єктів впливу, принципи та інструменти, методи регулювання, діяльність, спрямовану на забезпечення економічної безпеки та процедури і алгоритми її реалізації, а також техніки і технології управління; організаційні структури і управлінський персонал; відповідне забезпечення (політичне, правове та інформаційне).

Якщо проаналізувати зміст та значення кожного з наведених явищ, які, на думку відповідних вчених, входять до складу досліджуваного нами механізму, то можна відмітити, що не всі із

вказаних явищ дійсно слід відносити до елементів цього механізму. Наприклад, це стосується суб'єктів, адже саме вони застосовують цей механізм, а доцільність включення об'єкту викликає сумнів, бо саме щодо нього і застосовується цей механізм. Вказівка на діяльність по забезпеченню економічної безпеки є зайвою, бо вона характеризує спосіб практичного застосування механізму. Включення до його складу правовідносин є доволі суперечливим, хоча б з тих міркувань, що механізм як раз і впорядковує ці відносини, він щодо них спрямований, а тому навряд чи об'єкт упорядкуванням може сам себе упорядковувати.

Тому є всі підстави вказати на те, що лише ті з елементів, які за своєю спрямованістю та значенням здатні виконувати роль засобів впливу на певний об'єкт з метою забезпечення належного стану його існування варто включати до складу адміністративно-правового механізму забезпечення економічної безпеки держави. Такими є: норми права та нормативні акти; юридичні факти; акти застосування права, реалізації прав і обов'язків; принципи та інструменти, методи регулювання, а також процедури і алгоритми реалізації діяльності, включаючи техніки і технології управління; відповідне забезпечення (політичне, правове та інформаційне тощо). І саме ця сукупність явищ здана забезпечити цілеспрямований та системний вплив на відповідні відносини в сфері економіки з метою приведення її до такого стану, який характеризується як стан економічної безпеки.

В контексті нашого дослідження звернемо увагу на те, що наведена сукупність елементів адміністративно-правового механізму забезпечення економічної безпеки держави є неоднорідною за формою прояву, характером існування, природою походження та роллю в цьому механізмі. На цій підставі слід вести мову про те, що з наукової та практичної точок зору доцільно провести виділення поряд із змістом цього механізму (сукупність елементів) його структури (певних взаємопов'язаних блоків цих елементів). Такий підхід забезпечить можливість погляду на механізм забезпечення економічної безпеки як цілісне та системно організоване явище, що виступає частиною державного механізму, а також є засобом здійснення державного управління в економічній сфері, який носить системний та комплексний характер та здатний забезпечити стабільність економічної сфери.

В цьому контексті відмітимо точку зору О.С. Саєнко, який зазначає, що в основі системи зміцнення економічної безпеки країни лежить відповідний її механізм, який складається із взаємопов'язаних та взаємодіючих складових: нормативно-правових; інституційно-

організаційних; кадрових; інформаційно-аналітичних [4, с. 10, 12]. Якщо дещо уточнити структуру запропоновану О. С. Саєнком, враховуючи вище отримані результати, то до структури адміністративно-правового механізму забезпечення економічної безпеки держави доцільно включити такі блоки з наступним змістом: нормативно-правовий (сукупність норм права та нормативно-правових актів, юридичні факти); інституційно-організаційний (система уповноважених органів управління в сфері забезпечення економічної безпеки); процедурно-функціональний (принципи та інструменти, методи регулювання, а також процедури і алгоритми реалізації діяльності по забезпеченню економічної безпеки, включаючи техніки і технології управління); забезпечувальний (кадрове, інформаційне, матеріально-технічне та інше забезпечення); інформаційно-аналітичний (аналіз стану розвитку та існування об'єкта забезпечення). При такому підході ми отримуємо відповідну функціональну, організаційну та правову єдність, яка втілюється в цьому різновиді механізму правового регулювання, де єдність забезпечується спільною правовою основою механізму та єдиною природою його організаційної структури.

Список використаних джерел:

1. Алексеев С. С. Механизм правового регулирования в социалистическом государстве / С. С. Алексеев. – М. : Юрид. лит., 1966. – 167 с.

2. Ярмакі Х. П. Адміністративно-наглядова діяльність міліції в Україні : дис. … д-ра юрид. наук : 12.00.07 / Ярмакі Х. П. – Х., 2006. – 438 с.

3. Коренев А. П. Нормы административного права и их применение / А. П. Коренев. – М. : Юрид. лит., 1978. – 142 с.

4. Саєнко О. С. Зміцнення економічної безпеки як чинник ефективного функціонування економічної системи : автореф. дис. на здоб. наук. ступеня канд. екон. наук : спец. 08.00.01 «Економічна теорія та історія економічної думки» / Саєнко О. С. – О., 2010. – 20 с.

Отримано 05.11.2012

УДК 343.13;343.573

Андрій Миколайович ЛИСЕНКО
кандидат юридичних наук, старший науковий співробітник,
доцент кафедри оперативно-розшукової діяльності
навчально-наукового інституту підготовки фахівців кримінальної міліції
Харківського національного університету внутрішніх справ

ОПЕРАТИВНО-РОЗШУКОВА КЛАСИФІКАЦІЯ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ ІЗ ТЕРОРИСТИЧНОЮ ДІЯЛЬНІСТЮ

Робота присвячена наданню оперативно-розшукової класифікації злочинів, пов'язаних із терористичною діяльністю на підставі визначення загальних ознак даних злочинів, за якими доцільно здійснювати їх розподіл на умовні групи.

Актуальність проблеми дослідження класифікації злочинів, пов'язаних із терористичною діяльністю полягає у необхідності використання систематизованих у рамках оперативно-розшукової характеристики даних про вказані злочини – як інформаційної моделі злочинної діяльності, яка допомагає прогнозуванню дій злочинців та висуванню версій, особливо за умов недостатності інформації про злочин на початковому етапі їх розкриття.

Аналіз останніх досліджень і публікацій показав, що дана тема у вітчизняній науці залишається мало дослідженою, питання оперативно-розшукової характеристики злочинів терористичної спрямованості висвітлювалися у працях таких науковців, як Р. В. Мукоіда [1] та Г. С. Берест [2]. Разом з тим такий елемент оперативно-розшукової характеристики розглядуваних злочинів, як їх оперативно-розшукова класифікація залишається недостатньо розробленим.

Необхідно зазначити, що оперативно-розшукова характеристика злочинів включає до свого змісту класифікацію злочинів. Наукова класифікація являє собою особливий випадок застосування логічної операції поділу обсягу поняття відповідно до ознак, властивих об'єктам пізнання певного роду, що відрізняють їх від об'єктів (предметів, явищ) іншого роду. Ознаки, за якими здійснюється класифікація, мають бути істотними, стійкими і зрозумілими. Це допомагає проникати в сутність об'єктів, чітко їх розмежовувати і в той же час виявляти їх властивості, зв'язки і залежності, що є між ними, а також між елементами структури об'єктів. Як логічний засіб

пізнання класифікація властива різним галузям наукового знання [3, с. 18].

Одним із об'єктів класифікації в теорії ОРД є злочин. Класифікувати злочини означає розподіляти їх на окремі групи за специфічними ознаками, істотними для ОРД, на підставі яких можна відрізнити одні групи від інших. При цьому оптимальна класифікація злочинів передбачає правильне вирішення питання про підстави класифікації, тобто класифікаційні ознаки. Так, кримінально-правова класифікація здійснюється відповідно до статтей КК і дає лише загальне уявлення про характер і види злочинів, що вчиняються в певній сфері. Проте вона не в змозі забезпечити врахування всіх особливостей злочинних діянь, що мають істотне значення для їх виявлення та розкриття. Це й обумовлює потребу у класифікації злочинів у теорії ОРД, яка сприяє формуванню спеціальних методик розкриття злочинів.

Перш ніж перейти безпосередньо до розгляду класифікації злочинів, пов'язаних із терористичною діяльністю необхідно зазначити, що до даної групи злочинів відносяться діяння передбачені ст. 258–258-4, а також ст. 146, 147 за умови, якщо вони були вчиненні з метою вказаною у ст. 258 КК України [4].

На основі аналізу оперативно-розшукової практики, вітчизняних та закордонних наукових праць, ми пропонуємо класифікувати злочини, пов'язані з терористичною діяльністю за наступними критеріями, які слід враховувати при організації їх розкриття:

1. За територією на яку розповсюджуються дії злочинців: а) місцевого рівня; б) регіонального рівня; в) державного рівня; г) міжнародного рівня.

2. За способами вчинення, вчинені шляхом: а) використання вибухових пристроїв; б) використання вогнепальної зброї; в) підпалу; г) застосування отруйних чи сильнодіючих речовин; ґ) затоплення; д) поширення збудників заразних хвороб; е) захоплення заручників; є) викрадення людини; ж) погроз вчинення терористичного акту.

3. За кількістю осіб, причетних до вчинення злочину та формою їх організації, вчинені: а) однією особою; б) групою осіб; в) терористичною групою; г) терористичною організацією.

4. За наслідками вчинення злочину, що призвели: а) до загибелі особи; б) до загибелі групи осіб; в) до загибелі державного або громадського діяча; г) до знищення майна; ґ) без настання матеріальних наслідків (при погрозах).

5. За ідеологічними мотивами вчинення злочинів, вчинені по наступних мотивах: а) політичним; б) релігійним; в) етнічними; г) іншим.

6. За формою прояву об'єктивної сторони, злочини поділяється на: а) вчинення терористичного акту; б) погрозу вчинення терористичного акту; в) створення терористичної групи чи терористичної організації; г) керівництво такою групою чи організацією; г) участь у ній; д) матеріальне, організаційне чи інше сприяння вчиненню терористичного акту; е) втягнення у вчинення терористичного акту; є) публічні заклики до вчинення терористичного акту; ж) незаконне позбавлення волі або викрадення людини чи захоплення заручників з метою вказаною у ст. 258 КК України.

7. За місцем вчинення, вчинені: а) на вулиці; б) у житловому приміщенні; в) у виробничому приміщені; г) у автомашині; г) у метро; д) у потязі; е) на повітряному судні; є) на кораблі; ж) за межами населеного пункту; з) у місцях масового скупчення людей (ринки, магазини, ресторани, кафе тощо).

8. За способами впливу на об'єкт злочину, поділяється на: а) демонстративну; б) інструментальну.

Наприкінці зазначимо, що наведена оперативно-розшукова класифікація злочинів, пов'язаних із терористичною діяльністю носить певною мірою умовний характер та не є вичерпною, що обумовлено специфікою властивою даному виду злочинів. Викладене, на наш погляд, є одним із чинників підвищення ефективності застосування теоретичних основ ОРД під час розкриття розглядуваних злочинів.

Список використаних джерел:

1. Мукоіда Р. В. Організаційно-тактичні засади протидії злочинам, пов'язаним з терористичною діяльністю : дис. … канд. юрид. наук : 21.07.04 «Оперативно-розшукова діяльність» / Мукоіда Руслан Вікторович. – О., 2008. – 229 с.

2. Берест Г. С. Відомості про особу терориста та їх значення для виявлення, попередження і розкриття терористичного акту / Г. С. Берест // Вісник ЛДУВС. – 2008. – Спец. вип. № 4. – Ч. 2. – С. 211–216.

3. Белкин А. Р. Криминалистические классификации: монография / А. Р. Белкин. – М. : Мегатрон XXI, 2000. – 93 с.

4. Кримінальний кодекс України / Відомості Верховної Ради України. – К., 2001. – № 25–26. – Ст. 131.

Отримано 22.11.2012

УДК 342.536

Людмила Анатоліївна МАЗУР
здобувач кафедри оперативно-розшукової діяльності
навчально-наукового інституту підготовки фахівців кримінальної міліції
Харківського національного університету внутрішніх справ

ПРОТИДІЯ ОБІГУ МАЙНА, ОДЕРЖАНОГО ЗЛОЧИННИМ ШЛЯХОМ, – ПРІОРИТЕТНИЙ НАПРЯМОК РОБОТИ ПІДРОЗДІЛІВ КАРНОГО РОЗШУКУ

В результаті вивчення наукових праць вчених та оперативної обстановки доведено важливість роботи підрозділів карного розшуку щодо протидії обігу майна, одержаного злочинним шляхом.

Одними із завдань нового Кримінального процесуального кодексу є охорона прав, свобод та законних інтересів учасників кримінального провадження (ст. 2 КПК України) [1], серед яких: право не бути протиправно позбавленим права власності та право на непорушність приватної власності (ст. 41 Конституції України) [2].

Водночас, більша частина злочинів корисливо-насильницької спрямованості вчиняється задля незаконного викрадення чужого майна, яке після встановлення особи суб'єкта злочину, у більшості випадків не повертається потерпілому через ряд причин. Однією із них є низький рівень протидії підрозділами карного розшуку обігу майна, одержаного злочинним шляхом.

Взагалі, окремими проблемами протидії підрозділами карного розшуку обігу майна, одержаного злочинним шляхом, у радянський період займалися такі вчені, як: В. М. Аполлонов, В. М. Атмажитов, В. А. Батєнав, І. І. Бондаренко, І. І. Велікошин, В. І. Давидов, В. А. Ільїчов, А. А. Лискін, Б. Я. Нагіленко, В. Г. Самойлов, В. І. Ткаченко та інші.

Серед вітчизняних науковців у сфері ОРД в різних аспектах даному питанню приділяли увагу А. В. Баб`як, О. М. Бандурка, В.Я. Горбачевський, О.Ф. Долженков, В. П. Захаров, В. А. Некрасов, Д. Й. Никифорчук, В. Л. Ортинський, Ю. Ю. Орлов,

М. А. Погорецький, В. Д. Пчолкін, В. В. Плукар, О. П. Снігерьов, Н. Є. Філіпенко, В. В. Шендрик, О. О. Юхно та ін.

Принагідно зазначимо, що своєчасна та ефективна протидія підрозділами карного розшуку обігу майна, одержаного злочинним шляхом, сприяє: підвищенню авторитету карного розшуку та органів внутрішніх справ цілому; своєчасному розшуку такого майна; встановленню суб'єктів злочину та збору доказів їхньої причетності

-протиправних дій; забезпеченню вчиненням злочину.

апрямку роботи також підтверджується п. 3.8 Положення про департамент карного розшуку МВС України, затвердженого наказом МВС України від 30.06.2009 № 285, де зазначено, що відповідно до покладених завдань підрозділи карного розшуку перекривають джерелами оперативної інформації місця концентрації злочинного елементу (вокзали, місця розпусти, ринки, розважальні заклади) та збування викраденого майна (речові, продуктові та стихійні ринки, території, прилеглі до вокзалів, ломбарди, різноманітні скупки) [2].

Таким чином, означений напрям роботи є особливо важливим як для підрозділів карного розшуку ОВС України, так і для суспільства в цілому.

На жаль, теоретично-прикладні засади протидії підрозділами карного розшуку обігу майна, одержаного злочинним шляхом, поки що не стали об'єктом спеціальної уваги вчених у сфері оперативно-розшукової діяльності. Це підтверджується відсутністю методичних рекомендацій з питань протидії підрозділами карного розшуку обігу майна, одержаного злочинним шляхом.

На підставі наведеного, можна констатувати, що сьогодні виникла необхідність здійснення комплексної розробки означеної тематики.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України [Електронний ресурс] : закон України від 13.04.2012 № 4651-VI. – Режим доступу: http://zakon.rada.gov.ua/laws/show/4651-17/page4. – Редакція від 05.07.2012.

2. Конституція України [Електронний ресурс] : закон України від 28.06.1996. – Режим доступу: http://www.gska2.rada.gov.ua/pls/zweb_№/webproc4_1?id.

3. Положення про Департамент карного розшуку МВС України : затв наказом МВС України від 30.06.2009 № 285.

Отримано 21.11.2012

УДК 65.012.8+004

Олександр Володимирович МАНЖАЙ
кандидат юридичних наук,
доцент кафедри інформаційної безпеки факультету психології,
менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ

ОКРЕМІ ПРАВИЛА РОБОТИ ПРАЦІВНИКІВ ОВС У КОМП'ЮТЕРНИХ СОЦІАЛЬНИХ МЕРЕЖАХ

Розкрито окремі питання забезпечення інформаційної безпеки під час роботи працівників органів внутрішніх справ у комп'ютерних соціальних мережах. Запропоновано розробити відповідну інструкцію та внести до неї низку заборон та рекомендацій щодо користування комп'ютерними соціальними мережами.

Останнім часом спостерігається збільшення інтересу працівників органів внутрішніх справ як і значної частки людей у світі до комп'ютерних соціальних мереж. У зв'язку з цим збільшується кількість загроз, що можуть зашкодити оперативно-службовій діяльності, серед яких найбільш значущими є ті, що можуть призвести до витоку інформації з обмеженим доступом або псуванню іміджу правоохоронних органів, а відтак держави в цілому.

Ось чому важливо розробити та затвердити на відомчому або загальнодержавному рівні правила інформаційної безпеки під час роботи у комп'ютерних соціальних мережах (далі Правила).

Правила необхідно розробляти з урахуванням нормативної бази та сучасних методик і порад фахівців у галузі інформаційних технологій та захисту інформації [1–4]. Їх чітке дотримання дасть змогу забезпечити ефективне виконання поставлених завдань.

Основні моменти, що повинні висвітлюватись у вказаних Правилах мають бути наступними.

Заборони:

– обміну інформацією з обмеженим доступом невстановленими телекомунікаційними каналами. Тобто, потрібно ще раз наголосити на тому, що працівник ОВС не має права відсилати інформацію з

обмеженим доступом за допомогою соціальної мережі, не дивлячись на впевненість, що одержувач має право доступу до такої інформації;

– передачі облікових даних (імені користувача та паролю) стороннім особам. Ця заборона стосується облікових даних від електронної пошти, сторінок у соціальних мережах, форумів та чатів, зокрема, їх передачі у відповідь на прохання про це в листах або повідомленнях, що надійшли в соціальній мережі, навіть якщо вони надійшли від імені друзів, а також більше сторонніх людей;

[illegible]ланнями. Ніколи не можна переходити [illegible]ться в сумнівних повідомленнях, які розміщені на веб-сайтах у мережі, та були надіслані в соціальній мережі або електронною поштою;

– розміщення фотографій особистого характеру, які можуть дискредитувати особу або орган, у якому він працює;

– використання у повідомленнях неприйнятних виразів: грубих жартів і злої іронії, висловлювань, що можуть бути сприйняті і витлумачені як образи на адресу певних соціальних або національних груп, виразів образливого характеру, пов'язаних з фізичними вадами людини, нецензурної лайки, лихослів'я і виразів, що підкреслюють негативне ставлення до людей. Тобто, працівники ОВС під час розміщення повідомлень на веб-сайтах та в соціальних мережах зобов'язані дотримуватися загальноприйнятих правил мови і використовувати офіційно-діловий стиль.

Рекомендації:

– щодо складності паролів, яка має відповідати загальноприйнятим нормативам у сфері захисту інформації;

– надійного збереження особистих даних. Номери телефонів, адреси, електронна пошта тощо можуть стати для шахраїв ключем до безпеки їх власника;

– збереження пильності. Необхідно мати на увазі що особисті дані користувачів у кіберпросторі можуть не співпадати з їх особистим даними у фізичному просторі. Потрібно не забувати, що співрозмовник у Мережі не завжди переслідує позитивні наміри, навіть якщо особа вважає що спілкується зі знайомою людиною. Краще спілкуватися в Інтернеті з тими людьми, кого знаєте в реальному житті;

– потрібно пам'ятати, що електронна пошта є слабкою ланкою в системі будування безпеки інформації в соціальних мережах.

Дані рекомендації підлягають корегуванню в залежності від кожного окремого випадку. У результаті їх дотримання буде збережено не лише імідж особи, але й органу внутрішніх справ, у

якому особа проходить службу, та держави в цілому. Адже формування позитивного іміджу держави входить до числа стратегічних і першочергових завдань більшості країн. Імідж країни та її органів виконавчої влади формується у тому числі і завдяки іміджу працівників владних організацій.

Список використаних джерел:

1. Башлыков М. Социальные сети как угроза корпоративной информационной безопасности [Електронний ресурс] / М. Башлыков. – Режим доступу: http://www.itsec.ru/articles2/Inf_security/social-networks.

2. Термины и определения по социальным сетям [Електронний ресурс]. – Режим доступу: http://www.social-networking.ru/az/11/.

3. Черняк Л. Сервисы и теории социальных сетей [Електронний ресурс] / Л. Черняк. – Режим доступу: http://www.osp.ru/os/2008/08/5660961/.

4. Кузнецов М. В. Социальная инженерия и социальне хакеры / М. В. Кузнецов, И. В. Семдянов. – СПб. : БХВ-Петербург, 2007. – 356 с.

Отримано 10.11.2012

УДК 343.102:621.39

Андрій Олександрович МУСИК
головний оперуповноважений-інспектор
Управління боротьби з кіберзлочинністю МВС України

ОРГАНІЗАЦІЯ ВЗАЄМОДІЇ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ ОРГАНІВ ВНУТРІШНІХ СПРАВ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Зроблено аналіз організації взаємодії оперативних підрозділів органів внутрішніх справ у протидії кіберзлочинності. Надано пропозиції стосовно подолання нагальних проблем, що виникають під час взаємодії.

Однією з найбільш характерних особливостей злочинів, які вчиняються у сфері використання інформаційних, телекомунікаційних або інформаційно-телекомунікаційних систем, є їх транснаціональний характер. Зазначена ознака обумовлює неабияку складність виявлення,

документування та припинення злочинів цієї категорії, встановлення особистості злочинців та доведення їх вини, формуючи таким чином майже стовідсоткову латентність кіберзлочинів.

У зв'язку з цим Управлінням боротьби з кіберзлочинністю МВС України (далі – Управління) на постійній основі уживаються організаційні та практичні заходи, спрямовані на налагодження, підтримання та розвиток міжнародного співробітництва в напрямку протидії високотехнологічним правопорушенням.

Окрім цього слід зазначити, що для організації ефективної протидії таким видам злочинних проявів є необхідність у налагодженні взаємодії між усіма службами і підрозділами органів внутрішніх справ України.

Так, з метою забезпечення ефективної взаємодії між підрозділами боротьби з кіберзлочинністю МВС України та іншими службами і підрозділами ОВС у попередженні та протидії злочинності Управлінням розроблено тимчасові Рекомендації з організації взаємодії органів та підрозділів внутрішніх справ у попередженні та протидії злочинам і правопорушенням у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, які 27.06.2012 дорученням МВС № 9940/Чн для впровадження в оперативно-службову діяльність направлено на адресу підрозділів ОВС.

Метою цих Рекомендацій у першу чергу є організація сприяння підрозділів боротьби з кіберзлочинністю іншим службам ОВС у виявленні й розкритті злочинів, віднесених до їх компетенції, на етапах підготовки, вчинення або приховування яких використовувались комп'ютери чи мережа Інтернет.

Необхідно зауважити, що вже майже два роки на базі Управління діє Контактний пункт з реагування на кіберзлочини (далі – Контактний пункт), який є складовою частиною міжнародної цілодобової мережі контактних пунктів з реагування на кіберзлочини, заснованої на підставі ст. 35 Конвенції Ради Європи про кіберзлочинність, ратифікованої законом України № 2824-IV від 07.09.2005 (із змінами, внесеними згідно із законом № 2532-VI від 21.09.2010). За допомогою зазначених контактних пунктів активно здійснюється постійний обмін інформацією з поліцейськими різних країн світу, що спеціалізуються на протидії злочинам у сфері інформаційних технологій.

У даний час до мережі контактних пунктів приєднались більшість європейських держав, країн Азії, Північної та Південної Америки, Австралія (кількість країн-учасниць вже налічує 60). Але не

зважаючи на цей факт, можливості Контактного пункту на сьогодні мало використовуються структурними підрозділами органів внутрішніх справ України під час здійснення оперативно-службової діяльності.

Так, оперативні служби та слідчі підрозділи ОВС можуть ініціювати звернення до підрозділів боротьби з кіберзлочинністю з метою витребування відомостей технічного характеру у провайдерів та операторів телекомунікацій, постачальників інтернет-послуг, які діють за межами території України, у випадках:

– розслідування й оперативного супроводження кримінальних справ;

– проведення перевірок за заявами та повідомленнями про злочини, що вчинені або готуються (ЖРЗПЗ);

– провадження в оперативно-розшукових справах (ОРС).

Слід звернути увагу, що служби ОВС також можуть з використанням можливостей Контактного пункту ініціювати звернення до іноземних суб'єктів інформаційно-телекомунікаційних послуг щодо забезпечення збереження інформації в електронній формі з метою подальшого її отримання в рамках міжнародно-правової допомоги та використання в кримінальному судочинстві.

Приклад:

У разі необхідності встановлення особистості та фактичного місцезнаходження користувача українського сегменту мережі Інтернет, причетного до розповсюдження наркотичних засобів та за наявності інформації про його електронну поштову скриньку, наприклад «mail.ru», керівник оперативного підрозділу може направити до підрозділу боротьби з кіберзлочинністю відповідний запит, згідно із додатком, розробленим Управлінням до тимчасових Рекомендацій. Підрозділ боротьби з кіберзлочинністю каналами Контактного пункту звертається до Управління «К» Російської Федерації. Останні у свою чергу звертаються до адміністрації «mail.ru» з метою отримання інформації про особу, що зареєструвала та використовує відповідну електронну поштову скриньку, дату та час реєстрації скриньки, IP-адреси, з яких здійснюється доступ до неї, останній сеанс такого доступу та інших відомостей технічного характеру. У подальшому за наявності перелічених відомостей технічного характеру є можливість витребувати у національного суб'єкта інформаційно-телекомунікаційних послуг відомості щодо особистості і фактичного місцезнаходження правопорушника.

Поряд з цим, рекомендуємо ініціювати збереження іноземним оператором або провайдером Інтернет інформації (листування з цієї

поштової скриньки) в електронній формі з метою подальшого її отримання в установленому законом порядку та використання в кримінальному судочинстві.

У разі необхідності також можливо інші канали чи механізми отримання такої інформації від правоохоронних органів іноземних держав, передбачені чинним законодавством, наприклад НЦБ Інтерпол.

Витребування відомостей технічного характеру від національних суб'єктів інформаційно-телекомунікаційних послуг оперативні служби та слідчі підрозділи ОВС повинні здійснювати безпосередньо.

До відомостей технічного характеру, які можна запитати відносяться:

– відомості щодо використання IP-адрес (унікальних числових номерів мережевого рівня, що використовуються для адресації комп'ютерів чи пристроїв у мережі Інтернет). Іншими словами це аналог абонентських номерів у мережах стільникового зв'язку.

Таким чином, будь-якого комп'ютерного злочинця – користувача мережі Інтернет можна ідентифікувати за IP-адресою комп'ютеру чи пристрою, що ним використовується (за винятком коли злочинець використовує технології заплутування маршрутизації трафіку при наявності спеціального обладнання або програмного забезпечення);

– використання мережевого обладнання (пристроїв, призначених для з'єднання декількох вузлів комп'ютерної мережі в межах одного сегмента).

На сьогодні, більшість комп'ютерних злочинів у мережі Інтернет здійснюється шляхом віддаленого доступу до комп'ютеру. Відтак злочинця можна спробувати встановити за ідентифікаторами мережевого обладнання, що ним використовується.

Так, наприклад до ідентифікаторів мережевого обладнання можна віднести MAK-адресу. Це аналог IMEI-номерів мобільних телефонів у мережах стільникового зв'язку (проте національним законодавством не передбачено збереження такого ідентифікатору мережевого обладнання, як MAK-адреса).

– електронних поштових скриньок (відомості щодо осіб, які зареєстрували та використовують певні електронні поштові скриньки);

– веб-сторінок у соціальних мережах, веб-форумів, блогів (відомості щодо власників певних веб-сторінок, блогів або авторів висловлювань на веб-форумах);

– відомості про електронні комерційні сайти (Інтернет-аукціони та магазини) (відомості щодо приналежності електронних комерційних сайтів певним суб'єктам господарської діяльності);

– відомості щодо окремих мережевих технологій та послуг (сховище даних та інше) (відомості щодо користування та оплати певними особами послуг сховища даних, які у свою чергу були протиправно отримані та розповсюджуються);

– використання та суборенда доменних імен (унікального алфавітно-цифрового позначення, яке є необхідним елементом адреси (сайта) Інтернет (послідовність слів, що користувачі вводять в адресний рядок для того, щоб відвідати певний сайт)). За доменним ім'ям наприклад можна встановити особу, яка реєструвала та звідки оплачувала послуги реєстрації доменного імені сайту, що використовується у протиправних цілях;

– відомості про реєстрацію та адміністрування веб-сайтів. Наприклад, за доменним ім'ям та IP-адресою веб-сайту, що використовується у протиправних цілях, можна встановити його фізичне місце розміщення (хостінг), що у подальшому надає можливість встановити особу, яка розмістила його на технічному майданчику суб'єкта інформаційно-телекомунікаційних послуг, оплачує ці послуги, з яких IP-адрес наповнює та вносить зміни до даного веб-сайту;

– дані з білінгових систем (програмне забезпечення для підтримки комплексних процесів, відповідальних за збір інформації про використання телекомунікаційних послуг, їх тарифікацію, обробку платежів та інформації про абонентів) окремих суб'єктів господарювання відносно їх користувачів. Наприклад, зазвичай з таких систем отримуються відомості щодо інтернет-розрахунків за реалізацію заборонених товарів та послуг (дані стосовно дати,часу та суми операції, технічні відомості про учасників операції).

Строки зберігання перелічених відомостей технічного характеру залежать від законодавства кожної країни окремо.

Запити структурних підрозділів апарату МВС України стосовно сприяння їм у виконанні завдань щодо боротьби зі злочинністю відповідно до Рекомендацій повинні надсилатися безпосередньо до Управління. Запити територіальних ОВС – до територіальних підрозділів боротьби з кіберзлочинністю.

Так, за результатами проведеного аналізу взаємодії оперативних служб та слідчих підрозділів ОВС із підрозділами боротьби з кіберзлочинністю на зазначеному напрямку оперативно-службової діяльності за період з червня поточного року по теперішній час

встановлено наступне: за три місяці поточного року до Управління та його територіальних підрозділів з інших служб ОВС надійшло більш ніж 200 звернень щодо надання допомоги (сприяння) у виявленні та розкритті злочинів і правопорушень. Звернення надходили у переважній більшості від підрозділів карного розшуку, боротьби з незаконним обігом наркотиків апарату Міністерства та міськрайлінорганів ОВС.

Характерними прикладами взаємодії є ужиття працівниками підрозділів боротьби з кіберзлочинністю заходів, спрямованих на встановлення фактичного місцезнаходження користувачів українського сегменту мережі Інтернет – осіб, причетних до вчинення правопорушень, осіб, що розшукуються або переховуються від слідства чи дізнання.

Непоодинокі випадки, коли працівники підрозділів боротьби з кіберзлочинністю за зверненням інших служб ОВС уживають заходів із встановлення та припинення функціонування веб-ресурсів мережі Інтернет за допомогою яких розповсюджуються протиправні або заборонені товари та послуги, встановлення та притягнення до відповідальності організаторів функціонування таких веб-ресурсів.

Проблеми, що виникають під час здійснення взаємодії:

– не використання працівниками підрозділів ОВС під час виявлення й розкриття злочинів, віднесених до їх компетенції, на етапах підготовки, вчинення або приховування яких використовувались комп'ютери чи мережа Інтернет, тимчасових Рекомендацій, розроблених Управлінням (хоча після вступу нового КПК в дію Управлінням планується розроблення проекту наказу МВС «Про затвердження Інструкції „Про організацію взаємодії органів та підрозділів внутрішніх справ у попередженні та протидії злочинам і правопорушенням у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку"»);

– звернення служб ОВС до підрозділів боротьби з кіберзлочинністю з приводу надання допомоги у витребування відомостей технічного характеру від національних суб'єктів інформаційно-телекомунікаційних послуг;

– безпідставне направлення службами ОВС до підрозділів боротьби з кіберзлочинністю матеріалів дослідчої перевірки за фактами вчинення правопорушень, виявлення і розкриття яких не віднесено до компетенції служби;

– звернення служб ОВС до підрозділів боротьби з кіберзлочинністю з приводу надання загальнодоступних відомостей,

що не є відомостями технічного характеру (наприклад інформація щодо відповідності IP-адрес певному національному суб'єкту інформаційно-телекомунікаційних послуг).

Пропозиції стосовно подолання нагальних проблем, що виникають під час взаємодії: з метою налагодження найбільш ефективної взаємодії органів та підрозділів внутрішніх справ у попередженні та протидії злочинам і правопорушенням у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, виявлення та усунення негативних факторів, що можуть виникати під час такої взаємодії, уникнення їх у подальшому, керівникам оперативних служб та слідчих підрозділів ОВС необхідно забезпечити вивчення та практичне застосування в оперативно-службовій діяльності підлеглих тимчасових Рекомендацій, розроблених Управлінням.

У разі наявності проблемних питань та пропозицій щодо вдосконалення оперативно-службової діяльності на зазначеному напрямку роботи направляти їх до Управління для використання під час розроблення проекту наказу МВС «Про затвердження Інструкції „Про організацію взаємодії органів та підрозділів внутрішніх справ у попередженні та протидії злочинам і правопорушенням у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку"».

Отримано 06.11.2012

УДК 004,343.97

Віталій Вікторович НОСОВ
кандидат технічних наук, доцент,
професор кафедри інформаційної безпеки факультету психології,
менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ
Артем Олексійович ПУГАЧ
курсант групи ФПТ-09-3 факультету психології, менеджменту,
соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ

ФІКСАЦІЯ ДИНАМІЧНИХ ДАНИХ ОС WINDOWS ПРИ РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ

Наведено одне із можливих рішень із фіксації динамічних даних ОС Windows при проведенні слідчих дій з розслідування кіберзлочинів.

За сучасних умов широкого розвитку інформаційних технологій успішне розслідування злочинів не можливе без широкого використання науково-технічних засобів і спеціальних знань для виявлення, фіксації і вивчення слідів і речових доказів. Кіберзлочини, як правило успішно можливо розкрити, якщо на початковому етапі

ні дані операційної системи злочинця,
ня комп'ютерної системи.
і дії кіберзлочинців по отриманню прав адміністратора до Web-серверу, після чого цей сервер використовується як платформа для проведення подальших атак на інші інформаційні ресурси глобальної мережі. При встановленні факту несанкціонованого використання Web-серверу потрібна фіксація динамічних даних операційної системи, які можуть бути використанні в подальшій комп'ютерно-технічній експертизі при розслідуванні кіберзлочину.

Пропонується технічна реалізація фіксації динамічних даних ОС Windows у вигляді пакетного файлу, який запускається або із зовнішнього носія, або із локального диску, і який фіксує:

– системні дату і час;
– список процесів що виконуються в даний момент;
– список відкритих в даний момент з'єднань;
– додатки, що очікують на відкритих з'єднаннях;
– список користувачів, зареєстрованих в системі в даний момент;
– список систем, що мають поточні або мали недавні з'єднання з системою.

Результатом роботи пакетного файлу буде створення файлу звіту у текстовому форматі, який потім можливо проаналізувати і спланувавши можливий подальший огляд системи.

Список використаних джерел:

1. Джонс К. Д. Компоновка и использование набора инструментов для расследования хакерских атак, то есть для «живого ответа» в системе Windows [Електронний ресурс] : лекция // Инструментальные средства обеспечения безопасности / К. Д. Джонс, М. Шема, Б. С. Джонс. – Режим доступу: http://www.intuit.ru/department/security/issec/18/2.html.

2. Russinovich M. PsLoggedOn v1.34 [Електронний ресурс] / Mark Russinovich. – Режим доступу: http://technet.microsoft.com/en-us/sysinternals/bb897545.aspx.

3. Ochsenmeier M. Query the New Windows Audit Policies Programmatically [Електронний ресурс] / Marc Ochsenmeier. – Режим доступу: http://www.codeproject.com/Articles/61658/Query-the-New-Windows-Audit-Policies-Programmatica.

4. Мандиа К. Защита от вторжений Расследование компьютерных преступлений / Кевии Мандиа, Крис Просис. – М. : ЛОРИ, 2005. – 493 с.

5. Доказування у справах про злочини, вчинені шляхом незаконних операцій з використанням електронно-обчислювальної техніки : метод. рек. – К. : ДНДЕКЦ, 2012. – 40 с.

Отримано 29.11.2012

УДК 004

Віталій Вікторович НОСОВ
кандидат технічних наук, доцент,
професор кафедри інформаційної безпеки факультету психології,
менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ
Андрій Володимирович СТАВЕР
курсант групи ФПТ-09-3 факультету психології, менеджменту,
соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ

ЗАСТОСУВАННЯ ХМАРНИХ ОБЧИСЛЕНЬ В ДІЯЛЬНОСТІ ОВС УКРАЇНИ

Зроблена попередня оцінка потрібності та перспективності застосування хмарних обчислень у службовій діяльності органів внутрішніх справ.

В середині минулого десятиріччя почала поширюватися інформаційно-телекомунікаційна технологія, відома під назвою «хмарні обчислення». Одним із різновидів застосовування даної технології є операційні системи, що знаходяться в «хмарі» – вебОС. Така вебОС завантажується у браузер ОС телекомунікаційного пристрою користувача, а потім нею користуються як звичайною традиційною ОС, на якій може бути встановлено необхідне користувачу прикладне програмне забезпечення.

При виконанні службових обов'язків у працівників ОВС України є потреба у зміні місця перебування, прибутті на місце вчинення злочину і використання деякого потрібного програмного забезпечення (ПЗ) і баз даних.

У деяких випадках мати із собою робочий комп'ютер із потрібним ПЗ і даними не тільки не зручно, а часом, навіть і

ми є застосування технології хмарних
и наявність тільки доступу до мережі Інтернет. Крім необхідних програм, хмарні обчислення дозволяють використовувати хмари для збереження файлів.

Поки що в України технології хмарних обчислень ще не набули широкого розвитку. Проте, в останні роки підвищується зацікавленість правоохоронних органів інших країн до хмарних сервісів. Наприклад, у США вже почали екіпірувати патрульні машини планшетними комп'ютерами з застосуванням хмарних обчислень. У Російській

федерації вже ставляться задачі для окремих підрозділів щодо переходу на використання хмарних обчислень.

Технології хмарних обчислень створюють цілу низку додаткових можливостей і водночас із можливостями виникають інформаційні загрози. Аналіз загроз і можливих сервісів захисту від них дає змогу оцінювати перспективність впровадження хмарних обчислень у діяльність ОВС України.

Достатньо складно створити захисні механізми функціонування хмарних обчислень, при цьому зберігши швидкість обробки інформації.

Застосування хмарних обчислень у правоохоронній діяльності є перспективним та пов'язано з теоретичним і емпіричним дослідженням ефективності і безпечності цієї технології. Також є потреба у створенні правової бази регулювання застосування хмарних обчислень у правоохоронній діяльності.

Отримано 29.11.2012

—

УДК 347.73

Олеся Дмитрівна ОЛІЙНИК
курсант 4 курсу факультету податкової міліції
Національного університету державної податкової служби України

СТАН ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ В ОПЕРАТИВНИХ ПІДРОЗДІЛАХ ПОДАТКОВОЇ МІЛІЦІЇ

Розглянуто шляхи протидії та попередження податковій злочинності на предмет інформаційного забезпечення оперативно-розшукової діяльності.

Враховуючи посилену правозастосовчу діяльність підрозділів податкової міліції, злочинність в сфері оподаткування існує і розвивається все більш досконаліше і замаскованіше у порівнянні до правоохоронних органів. Як не дивно, з метою незаконного приховування доходів від оподаткування, легалізації незаконно отриманих грошових коштів, як на території України так і за її межами, зловмисники вдаються до різних форм порушення податкового, зокрема кримінального законодавства. Цьому сприяє

поширення та використання новітніх інформаційних технологій, що так досконало використовують окремі суб'єктами господарської діяльності з метою ухилення від сплати податків.

Відповідно, варто приділи достатню увагу пошуку шляхів для попередження та протидії податковій злочинності, окільне дане питання сьогодні стоїть на досить актуальному рівні.

Ефективність діяльності оперативних та слідчих підрозділів в сучасних умовах неможлива без належного інформаційного та довідкового забезпечення оперативно-розшукової діяльності податкової міліції, створення, удосконалення та застосування нею спеціальних баз і банків даних оперативно-розшукового призначення.

Оцінка практичної діяльності підрозділів податкової міліції свідчить про те, що сьогодні все ж існують проблеми щодо запровадження та використання сучасних інформаційних технологій для виявлення та розкриття податкових злочинів. Потребує удосконалення як законодавче, так і матеріально-технічне й інформаційно-аналітичне забезпечення оперативно-розшукової діяльності. Відповідно, існує потреба у підготовці та перепідготовці кадрів для вирішення цих завдань.

Інформаційне забезпечення розслідування злочинів у сфері оподаткування виступає вагомою проблемою, яка потребує постійного спостереження та дослідження, що пов'язано зі стрімким розвитком науки і техніки. Інформаційне забезпечення, дійсно є передумовою здійснення оперативно-розшукових заходів підрозділами податкової

зазначених оперативно-розшукових

ння оперативної інформації, і виступає

як інформаційне забезпечення подальшої пізнавальної діяльності оперативних працівників.

Оперативно-розшукова діяльність здійснюється з метою отримання інформації, її накопичення, обробки, аналізу і висновків, а також вжиття відповідних заходів. Для ефективної боротьби зі злочинністю оперативним підрозділам необхідно мати актуальну оперативну інформацію відносно діяльності кримінальних структур, процесів, що відбуваються у злочинному середовищі.

Одним із завдань процесу інформаційного забезпечення підрозділів податкової міліції ДПС України є досягнення таких стандартів, які б відповідали європейському та світовому рівню правоохоронної діяльності у сфері боротьби з податковою злочинністю, створювали у вітчизняному суспільстві новітню атмосферу взаєморозуміння та довіри між державою та бізнесом,

сприяли становленню партнерських взаємовідносин між податковими органами та платниками податків.

Відповідно до цих аспектів Україні потрібне створення оновленої стратегії міжнародного співробітництва та взаємодії підрозділів податкової міліції з іншими зарубіжними правоохоронними органами в сфері інформаційного сприяння.

Аналізуючи стан інформаційно-аналітичного забезпечення підрозділів податкової міліції, очевидними стали такі процеси: застаріла матеріально-технічна база, комп'ютерна техніка та бази і банки даних; відсутність на робочих місцях доступу до мережі Internet; складність отримання інформації про рух коштів по банківських рахункам; відсутність чіткого плану розвитку й удосконалення автоматизованих систем та ряд інших невирішених проблем, що гальмують розслідування податкових злочинів.

Таким чином, дослідивши проблемні питання інформаційного забезпечення підрозділів податкової міліції, ми вважаємо, що ефективними способами їх вирішення є: збільшення фінансування щодо забезпечення підрозділів податкової міліції необхідним обладнанням та технікою; удосконалення навчальної бази кадрів податкової міліції в користуванні інформаційними системами та застосування спеціальних автоматизованих банків даних оперативно-розшукового призначення, а також своєчасне оновлення та вдосконалення інформаційних систем оперативних підрозділів згідно розвитку світових інноваційних технологій.

Список використаних джерел:

1. Податковий кодекс України. – Х. : Одіссей, 2012. – 536 с.

2. Про оперативно-розшукову діяльність: закон України [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2135-12. – З остан. змін., що вступ. в силу 19.11.2012.

3. Лисенко В. В. Ухилення від сплати податків: виявлення та розслідування : монографія / В. В. Лисенко, О. С. Задорожний, О. П. Дзісяк. – К. : Істина, 2008. – 216 с.

4. Бандурка О. М. Оперативно-розшукова діяльність. Ч. 1 : підручник / О. М. Бандурка. – Х. : Вид-во Нац. ун-ту внутр. справ, 2002. – 336 с.

Отримано 20.11.2012

УДК 343.98

Юрій Миколайович ОНИЩЕНКО
викладач кафедри інформаційної безпеки факультету психології, менеджменту, соціальних та інформаційних технологій Харківського національного університету внутрішніх справ
Максим Володимирович НІЧИК
курсант групи ФПТ-09-3 факультету психології, менеджменту, соціальних та інформаційних технологій Харківського національного університету внутрішніх справ

ПРОБЛЕМНІ АСПЕКТИ ЗАСТОСУВАННЯ ПОЛІГРАФА В ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ ПО РОБОТІ З ПЕРСОНАЛОМ ОВС УКРАЇНИ

Розглянуто проблемні аспекти застосування поліграфа в діяльності підрозділів по роботі з персоналом ОВС України.

У сучасному світі важко представити суспільство без кримінальних елементів: майже у складі кожного підприємства, органа, відомства обов'язково є хоча б одна людина схильна до правопорушень або, навіть, правопорушник. Хоча зараз майже всі установи намагаються автоматизувати процес за допомогою машин та все ж людина відіграє не останню роль у будь-якому виді діяльності. Тому все більш нагальною стає потреба у приладах та методах в. Одним із таких приладів є поліграф. ивна робота з приводу виявлення них органах та приватних установах за допомогою поліграфа, а саме у США, Великобританії, Франції, Росії, Казахстані тощо. В Україні також прийнято та затверджено відповідну нормативну базу – наказ МВС України від 28.07.2004 № 842.

Використання поліграфа викликає багато суперечок з приводу того, що його використання порушує ряд прав і свобод людини та принижують людську честь та гідність. Слід враховувати той факт, що поліграф ніяким чином не впливає на психіку та організм людини, а лише фіксує фізіологічні показники людини та візуалізує їх відхилення, та використовується лише за умови згоди піддослідного.

Варто зважати, що багато залежить від людини, яка застосовує поліграф та інтерпретує динаміку фізіологічних показників допитуваної особи [1; 2]. Експерт може неправильно тлумачити результати (наприклад, у зв'язку з упередженим ставленням експерта до допитуваного, непрофесійністю експерта, нервовістю допитуваного та багатьма іншими факторами) [3], тому відповідну увагу слід

приділити підготовці кваліфікованих сертифікованих спеціалістів по роботі з поліграфом, адже наслідком непрофесійності експерта може стати обвинувачення чесної людини.

Що ж до ОВС України, то поліграф може принести неабияку допомогу, а саме при підборі кандидатів на службу в ОВС України та при проведенні службових розслідувань. Численні реформи в правоохоронних органах, які проводилися з метою «чистки» рядів міліціонерів, значних результатів не принесли.

Працівники міліції, вступаючи на службу, піддаються деяким обмеженням у правах, наприклад, в можливості бути політичним діячем, займатися підприємницькою діяльність тощо. Пропонується при проведенні співбесід з кандидатами на службу в ОВС передбачити на законодавчому рівні можливість застосування поліграфа за ініціативою працівників центру практичної психології або підрозділу кадрового забезпечення, які приймають активну участь у підборі кандидатів на службу в ОВС України.

Також, на наш погляд, потребує нормативного закріплення використання поліграфа при проведенні службових розслідувань за фактами грубих порушень дисципліни, невиконання або неналежного виконання службових обов'язків як за ініціативою підрозділу ОВС, який проводить службове розслідування, так і самої особи, відносно якої ведеться перевірка.

Застосовуючи поліграф при підборі кандидатів на службу в ОВС України, можливо відсіяти кандидатів з неприйнятною мотивацією для вступу на службу, а також зі схильностями до девіантної поведінки [1]; при проведенні службових розслідувань можливо достовірно (з упевненістю на 97–98 відсотків [3]) виявити винну особу. У зв'язку з вищезазначеним необхідно внести зміни до нормативних документів щодо обов'язкового дослідження на поліграфі працівників ОВС України та кандидатів на службу в ОВС. На нашу думку, потребують внесення змін наступні нормативні документи: Закон України «Про міліцію», «Положення про проходження служби рядовим і начальницьким складом ОВС», наказ МВС України від 28.07.2004 № 842 «Про подальший розвиток служби психологічного забезпечення оперативно-службової діяльності органів внутрішніх справ України», а також затверджена цим наказом «Інструкція щодо застосування комп'ютерних поліграфів у роботі з персоналом органів внутрішніх справ України».

Список використаних джерел:

1. Варламов В. А. Детектор лжи / В. А. Варламов. – 2-е изд. – М. : ПЕР СЭ-Пресс, 2004. – 352 с.

2. Журін С. І. Практика та теорія використання детекторів брехні / С. І. Журін. – К. : Радіо і зв'язок, 2004. – 143 с.

3. Український поліграфологічний журнал [Електронний ресурс]. – Режим доступу: http://www.ukrpolygraph.org.

Отримано 19.11.2012

—

УДК 004.49

Олександр Валентинович ОРЛОВ
кандидат технічних наук, доцент,
завідуючий кафедри інформатизації державного управління
Харківського регіонального інституту Національної академії
державного управління при Президентові України
Анна Ігорівна КОБЗЕВА
студент групи КН-12-4
Харківського національного університету радіоелектроніки

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ WEB-САЙТУ, ПОБУДОВАНОГО НА СИСТЕМІ УПРАВЛІННЯ КОНТЕНТОМ

Розглянуто питання захисту веб-сайту, побудованого на системі управління контентом. Розглянуто методи несанкціонованого доступу та запропоновано варіанти захисту подібних сайтів.

Системи управління контентом (CMS), як і багато інших видів програмного забезпечення досить уразливі. На відміну від CMS власної розробки, якщо зловмисники або хакери знаходять уразливі місця в одній конкретній тиражованій CMS – виникає загроза злому всіх подібних CMS даного виробника. При цьому, чим більш поширеною є система і чим частіше вона використовується на популярних сайтах, тим більше грошей і зусиль зловмисники інвестують в пошук її проблемних місць. Крім того, більшість сучасних CMS складаються з модулів, і більшість уразливих місць

пов'язані з плагінами, які зазвичай написані і протестовані на безпеку гірше, ніж основний код системи.

Використовуючи різні недоліки CMS, зловмисники намагаються отримати для себе вигоду за рахунок чужих сайтів і відвідувачів. Розглянемо більш детально способи захисту від несанкціонованого доступу до системи, яка базується на використанні Next Generation CMS, що розповсюджується по ліцензії GNU.

Через URL-базовані впровадження, хакери намагаються знайти «слабкі» місця web-сайту, використовуючи запити, які виконуються але при нормальному адмініструванні хостингу повинні видавати помилку. Одним із способів захисту від такого роду запитів є використання файлу. Htaccess в якості Firewall. В цьому файлі є можливість задати набір правил, які будуть автоматично блокувати запити та містять рядкові змінні в адресному рядку.

Наприклад, використання дужок в HTTP-запиті говорить про те, що хтось намагається виявити «дірку» в системі. В даному випадку

сторінку «403 Forbidden – доступ
м. У файл htaccess необхідно ввести
рядок, що будуть заблоковані будь-які запити, що містять квадратні дужки. Firewall має модульну структуру, що дає можливість видалити будь-який рядок без порушення функціональності системи

Ще одним способом захисту системи є обмеження доступу до тек сервера. За лістинг файлів відповідає директива Indexes (показувати відвідувачу список файлів, якщо у вибраній теці немає файлу index). Необхідно створити в даній теці файл htaccess, який містить один рядок: Options - Indexes. Заборонити доступ до окремих файлів або групам файлів можна використовуючи директиву deny from all.

Крім зазначеного вище можна обмежити доступ до сайту з окремих або діапазонів IP-адрес, поставити паролі на конкретні каталоги, використовувати перенаправлення (redirect) тільки при запиті певних сторінок або тільки відвідувачів з певним IP-адресою, заборонити скачування файлів тощо.

Наступний різновид проблем виходить від користувачів, які потрапляють в адміністративну частину системи.

Наприклад, тільки адміністратор системи має права на виконання функцій редагування контента сайту. Тобто якщо відбувається спроба редагування / зміни контенту необхідно бути впевненим, що користувач має права на такі дії.

Додатковий рівень безпеки необхідний для забезпечення цілісності особливо важливих даних системи. Особливу увагу слід приділити захисту від впровадження SQL-коду (SQL-injection). Це один з розповсюджених способів злому сайтів і програм, що працюють з базами даних, заснований на впровадженні в запит довільного SQL-коду. Впровадження SQL, залежно від типу використовуваної СУБД і умов запровадження, може дати можливість «хакеру» виконати довільний запит до бази даних (наприклад, прочитати вміст таблиць, видалити, змінити чи додати дані), отримати можливість читання або запису локальних файлів і виконання довільних команд на сервері.

Для недопущення таких впроваджень в першу чергу необхідно перевіряти правильність введених даних.

Крім вищесказаного, схоронність даних можна забезпечити, захистивши їх за допомогою SSL. SSL – протокол шифрування, який використовується в мережах, таких як Інтернет. Використання SSL пов'язано лише з однією проблемою: не всі компанії, що пропонують послуги хостингу, підтримують даний вид шифрування.

Сфера інформаційної безпеки – актуальне питання сучасності. Захист сайту від «хакерів» стає глобальною проблемою, над вирішенням якої працюють фахівці всього світу. Бізнес, побудований в агресивному середовищі Інтернет, вразливий і схильний нападам з боку конкурентів і недоброзичливців.

Єдиного інструменту для усунення всіх загроз несанкціонованого доступу до сайтів побудованим на основі систем управління контентом – просто не існує. Забезпечення захисту сайту – це комплексне завдання.

Отримано 05.11.2012

УДК 65.012.8+004

Микола Миколайович ПЕРЕПЕЛИЦЯ
кандидат юридичних наук, доцент,
доцент кафедри оперативно-розшукової діяльності
навчально-наукового інституту підготовки фахівців кримінальної міліції
Харківського національного університету внутрішніх справ

СЛУЖБОВІ РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ ПОРУШЕННЯ КОМП'ЮТЕРНОЇ БЕЗПЕКИ У ПРИВАТНИХ КОМПАНІЯХ

Розкрито окремі підходи до розслідування інцидентів порушення інформаційної безпеки у приватних компаніях та відповідні пропозиції на ринку послуг. Досліджено вітчизняний та зарубіжний досвід.

Останніми роками від кіберзлочинів все частіше стали потерпати інтереси великих корпорацій, що викликало необхідність у розробці методик внутрішніх розслідувань так званих «інцидентів інформаційної безпеки».

У багатьох випадках керівники компаній вважають, що інформування правоохоронних органів про вчинений проти них кіберзлочин, може спричинити небажані репутаційні наслідки. Це може вплинути на прибутки підприємства. Тому розроблені внутрішні

інцидентів інформаційної безпеки
причин та фактичних даних події,
ыомогою сил і засобів самої компанії.
Здебільшого функцій щодо внутрішнього розслідування виконує служба безпеки підприємства, але у деяких випадках до цієї діяльності можуть бути залучені зовнішні особи за принципом аутсорсінгу. Відомою компанією подібного роду є, наприклад, Group-IB.

Ринок послуг у цій сфері має приблизно такі напрями:

– реагування на інциденти (Incident response);
– розслідування інцидентів (eDiscovery);
– комп'ютерна криміналістика (Digital Forensic);
– моніторинг інцидентів;
– юридичне супроводження інцидентів.

Найбільш поширеним документом, який регламентує проведення внутрішніх розслідувань є «Фундаментальне керівництво з розслідування комп'ютерних подій для Windows» [1]. Дане керівництво було розроблено фахівцями компанії Microsoft та є

найбільш докладним із загальнодоступних документів подібного штибу.

Модель розслідування комп'ютерних подій припускає систематизацію різних елементів дослідження комп'ютерів в логічну послідовність (рис. 1).

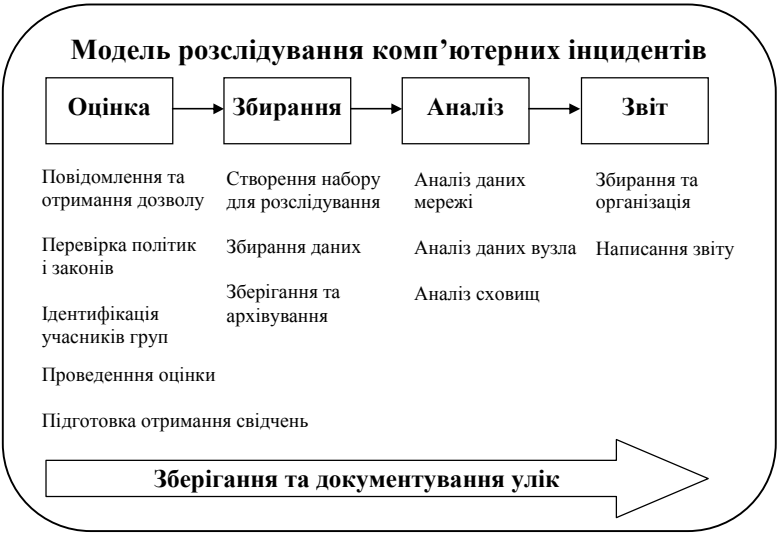

Рис. 1. Модель розслідування комп'ютерних подій

Під час роботи з цифровими доказами застосовуються чотири етапи проведення розслідування і супровідні процедури. Ці етапи можна коротко охарактеризувати таким чином:

– оцінка ситуації. Аналіз рамок розслідування, що проводиться, і необхідних дій;

– збирання даних. Збір, захист і збереження початкових доказів;

– аналіз даних. Вивчення і зіставлення цифрових доказів з подіями для успішного звернення в правоохоронні органи;

– звіт про розслідування. Збір і організація отриманої інформації, написання підсумкового звіту.

В Україні систему управління інцидентами інформаційної безпеки було створено в рамках розробки та впровадження типових рішень щодо комплексної системи захисту інформації в АІС Національної академії наук України.

Відповідний документ містить пропозиції щодо розробки та впровадження системи управління інцидентами інформаційної

безпеки, що включає процеси, нормативно-розпорядчу документацію і засоби автоматизації.

Система управління інцидентами інформаційної безпеки є базовою частиною загальної системи управління інформаційною безпекою і дозволяє виявляти, враховувати, реагувати й аналізувати події та інциденти інформаційної безпеки. Без реалізації цих процесів неможливо забезпечити рівень захищеності, що адекватний сучасним стандартам і галузевим нормам. Управління інцидентами, це важливий процес, який забезпечує організації можливість спочатку виявити інцидент, а потім за допомогою коректно обраних засобів підтримки якомога швидше його вирішити.

Основна задача управління інцидентами – якомога швидше відновити нормальну роботу служб і звести до мінімуму негативний вплив інциденту на роботу організації для підтримки якості і доступності служб на максимально можливому рівні. Нормальною вважається робота служб, що не виходить за рамки угоди про рівень обслуговування.

Цілі управління інцидентами:

– відновлення нормальної роботи служб в найкоротші терміни;

– зведення до мінімуму впливу інцидентів на роботу організації;

– забезпечення злагодженої обробки всіх інцидентів і запитів обслуговування;

– зосередження ресурсів підтримки на найбільш важливіших напрямах;

– надання відомостей, що дозволяють оптимізувати процеси підтримки, зменшити кількість інцидентів і запланувати управління [2].

Список використаних джерел:

1. Фундаментальное руководство по расследованию компьютерных происшествий для Windows [Електронний ресурс]. – Режим доступу: http://technet.microsoft.com/ru-ru/library/cc162846.aspx.

2. Розробка та впровадження типових рішень щодо комплексної системи захисту інформації в АІС НАНУ [Електронний ресурс]. – Режим доступу: http://www.isofts.kiev.ua/c/document_library/get_file?p_l_id=15462&folderId=15767&name=DLFE-508.doc.

Отримано 19.11.2012

УДК 343.97

Михайло Олексійович ПЕСТРЕЦОВ
ад'юнкт кафедри оперативно-розшукової діяльності
Національної академії внутрішніх справ

ЩОДО НОВІТНІХ ФОРМ ПРОТИДІЇ ЗЛОЧИННИМ ПОСЯГАННЯМ НА ПОМЕШКАННЯ ГРОМАДЯН

Присвячено новітнім формам протидії злочинним посяганням на помешкання громадян, зокрема співробітництву з міжнародними організаціями, такими як Європол – Європейської міжурядової організації поліційного напрямку з питань протидії організованій злочинності.

На даний час, незважаючи на заходи, що вживаються правоохоронними органами, криміногенна ситуація в Україні є складною. Більше половини всіх злочинів складають протиправні посягання майнової спрямованості, зокрема пов'язані із злочинними посяганнями на помешкання громадян.

Зберігається стійка тенденція зростання рівня злочинності у сфері незаконного обігу наркотичних засобів, психотропних та сильнодіючих речовин. Це свідчить як про подальшу наркотизацію населення та підвищення навантаження на працівників міліції.

Таким чином, рівень забезпечення безпеки країни і її жителів від різного виду загроз життю, здоров'ю та майну не повною мірою відповідає загальновизнаним стандартам безпеки, притаманним, зокрема, європейським столицям.

ого стану справ є розрізненість системи
опорушень усіх рівнів, відсутність
блеми забезпечення безпеки України.

У цих умовах пріоритетними напрямками є запровадження новітніх форм протидії злочинним посяганням на помешкання громадян, комплексного забезпечення безпеки населення, яке, в свою чергу, вимагає розробки та реалізації довгострокових заходів організаційного, практичного, профілактичного та нормотворчого характеру. Початковим етапом у цьому напрямку, на наше переконання, має стати активніше співробітництво з міжнародними організаціями, а також з конкретними державами на двосторонній основі з метою узгодження форм і методів протидії злочинним посяганням на помешкання громадян, з підходами Європейського Союзу та Ради Європи. Важливим кроком на цьому шляху є взаємодія

з Європолом – Європейської міжурядової організації поліційного напрямку з питань протидії організованій злочинності.

Службові особи Європолу мають доступ до національних інформаційних систем, пов'язаних з кримінальним переслідуванням осіб (органи внутрішніх справ, митниця, державні прикордонні служби, прокуратура, органи юстиції і виконання покарань), а також до різних адміністративних реєстрів. Крім того, службові особи Європолу мають можливість забезпечувати розслідування певних фактів та проведення експертиз у різних країнах. Отримання належної інформації цілодобово на всіх мовах Європейського Союзу дозволяє здійснити необхідний аналіз та оцінку її національними слідчими органами [1, с. 5].

У сфері протидії організованій злочинності, зокрема пов'язаної із злочинними посяганнями на помешкання громадян Європол також здійснює координацію розслідування діяльності міжнародних організованих груп у тому випадку, коли паралельно в кількох країнах-членах ЄС порушені і розслідуються кримінальні справи щодо однієї і тієї організованої групи.

Іншим основним завданням Європолу є здійснення аналітичної роботи щодо дій, структури, членів та бази діяльності міжнародних організованих груп. Завдяки цій діяльності Європол надає законодавцям, урядам та поліційним органам відомості, що використовуються для кримінально-політичних та правових заходів протидії організованій злочинності. Указані аналітичні відомості мають стратегічне значення при виробленні окремими країнами-членами політики протидії злочинним посяганням на помешкання громадян.

Виходячи з того, що в національних слідчих органах при протидії злочинним посяганням на помешкання громадян виникає необхідність у отриманні інформації про підозрюваних осіб, підприємства, банки, речі, їх правовий статус тощо, з іншої країни Європи, одним із найважливіших завдань Європолу є накопичення і надання такої інформації. При цьому Європол отримує необхідну інформацію з країн-членів ЄС, третіх країн, міжнародних організацій. Важливим аспектом діяльності Європолу є той, що така інформація повинна надходити тільки з відкритих джерел [2, p. 350].

На наше переконання, вказаний досвід роботи Європолу може бути позитивно використаний у роботі вітчизняних органів внутрішніх справ: з перенесенням пріоритету не на наказові повноваження та підпорядковані обов'язки, а на командне, рівноправне співробітництво, яке підлягає регулярному звітуванню з метою

узагальнення та здійснення аналітичної роботи. Слід наголосити також, що введення та апробація нових методів та техніки протидії злочинним посяганням на помешкання громадян на рівні Європолу матиме ефективне значення для вітчизняних органів внутрішніх справ. Методи, що їх застосовують країни ЄС з метою протидії злочинним посяганням на помешкання громадян, очевидно, повинні бути адаптовані правоохоронними органами України. Тим більше, що такі вимоги висуваються до потенційних держав-кандидатів на вступ до ЄС.

Список використаних джерел:

1. Проневич О. С. Європол: правові та організаційні засади участі у боротьбі з транснаціональною злочинністю / О. С. Проневич // Вісник Запорізького державного університету. – 2003. – № 1. – С. 5–8.

2. Storbeck J. Die Rolle von Europol bei der Bekaempfung der Organisierten Kriminalitaet / J. Storbeck // Organisierte Kriminalitaet: Bestandsaufnahme, transnational Dimension, Wege der Bekaempfung. – Berichte und Studien der HSS. B. 1. – Muenchen : Hanns-Seidel-Stiftung, 1999. – P. 349–432.

Отримано 26.11.2012

УДК 004.932.2:681.3.06

В'ячеслав Олексійович РАДЧЕНКО
аспірант Харківського національного університету радіоелектроніки

ЗАСТОСУВАННЯ ІМОВІРНІСНИХ ХАРАКТЕРИСТИК ФУНКЦІОНАЛЬНИХ ЗАЛЕЖНОСТЕЙ У РЕСТРУКТУРИЗАЦІЇ РЕЛЯЦІЙНИХ БАЗ ДАНИХ

Розглянуто використання методу перевірки коректності функціональних залежностей, що базується на обчислюванні їх ймовірностей для поточного набору даних у РБД.

На сьогоднішній день інформаційні системи є невід'ємною частиною будь-якої сфери людської діяльності, бо вони дозволяють значно спростити збереження, обробку й аналіз великої кількості даних, що використовуються у робочому процесі. Такі системи

знайшли своє відображення у програмно-апаратних комплексах, що впроваджують інноваційні технології у правоохоронну діяльність та боротьбу зі злочинністю. Автоматизовані системи обробки інформації дозволяють значно спростити облік, пошук та аналіз службових даних.

Одним із новітніх напрямів розвитку є підтримка баз даних, зокрема реляційних (найпоширеніших на даний час), що входять до складу будь-якої сучасної інформаційної системи. Підтримка складається з комплексу заходів, що направлені на забезпечення надійності, швидкості роботи, збільшення терміну служби існуючої БД. Складовою частиною даного комплексу є реструктуризація – внесення змін до структури БД з метою оптимізації функціонування чи задоволення нових потреб, що накладаються на існуючу інформаційну систему.

Однією з конкретних задач у процесі реструктуризації є перевірка функціональних залежностей (ФЗ), що є основою для обрання тієї чи іншої структури БД, на їх коректність відносно даних, які зберігаються. ФЗ закладаються у структуру під час створення БД. Якщо інформація о залежностях була втрачена, є можливим відновити її за допомогою методів виявлення. Такі методи використовують факт дотримання даними початкових обмежень, що були закладені у вигляді ФЗ [1, с. 204]. Ці обмеження зазвичай мають вигляд зв'язків типу «один-до-багатьох», що можна подати у вигляді твердження, наприклад: «у камері може знаходитися декілька злочинців, і кожний з них може бути присутній тільки у одній камері». Таким чином, злочинець однозначно ідентифікує камеру, у який він знаходиться. Розглянуті обмеження підтримуються БД автоматично згідно з її структурою.

Використання методів виявлення має недолік: існує великий

ежностями будуть знайдені випадкові –
оведення обробки, але можуть зникнути
нових даних у БД. Тому перевірка виявлених ФЗ має велике значення для подальшого використання.

Результатом вирішення цієї задачі є метод для отримання імовірнісних характеристик множини функціональних залежностей. Отримані характеристики можуть бути використані для формування експертного висновку щодо оптимізації існуючої структури БД чи потреби внесення змін у структуру. Метод базується на використанні поняття «класів еквівалентності» даних, що знаходяться у БД, і оцінки відношення розміру класу еквівалентності до загальної кількості рядків даних [2]. Так як імовірність ФЗ є чисельною характеристикою, стає можливим використання граничного значення допустимої

ймовірності ФЗ, нижче якого ФЗ буде розглядатися як помилкова. Особливістю даного методу є залежність від обсягу вибірки даних, що використовується для аналізу – чим більша кількість рядків у вибірці, тим вищі кінцеві ймовірності ФЗ, тому бажане його використання для великих обсягів даних.

Напрямками для подальшої роботи є розробка шляхів використання кінцевої множини ФЗ для рекомендацій щодо побудови оптимальної структури БД та засобів для адаптації існуючих даних до запропонованих змін без втрат значущої інформації.

Список використаних джерел:

1. Радченко В. А. Выявление скрытых зависимостей между данными в задачах реинжиниринга информационных систем / В. А. Радченко, С. С. Танянский // Системи обробки інформації. – 2012. – Вип. 3 (101). – С. 203–205.

2. Cormode G. Estimating the Confidence of Conditional Functional Dependencies [Електронний ресурс] / Graham Cormode, Lukasz Golab, Flip Korn // SIGMOD ‘09 Proceedings of the 2009 ACM SIGMOD International Conference on Management of data. – P. 469–482. – Режим доступу: http://people.cs.umass.edu/~mcgregor/papers/09-sigmod.pdf.

Отримано 05.11.2012

—

УДК 343.982.323

Едуард Олександрович РАЗУМОВ
старший викладач Сумської філії
Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ У ПРОФІЛАКТИЦІ ЗЛОЧИНІВ

Розглянуто основні напрямки використання систем відеоспостереження з метою профілактики злочинів. Проаналізовано можливості деяких видів систем для вироблення відповідних рекомендацій.

Добре відомо, що в роботі правоохоронних органів може успішно використовуватися габітоскопічна інформація, що дозволяє

здійснювати розшук осіб за отриманими з різних джерел даними про ознаки зовнішності людини. Видається, ці методи можуть успішно використовуватися і для профілактики злочинів з використанням сучасних технологій. У зв'язку з цим є необхідність розглянути ці питання з урахуванням сучасного стану технічних засобів накопичення та обробки зображень зовнішності, телекомунікаційних систем і устаткування для відеореєстрації.

Для запобігання злочинів може використовуватися візуальна інформація, отримана в процесі різноманітних спостережень. Зараз відеоконтрольні системи спостереження знаходять широке застосування в діяльності банків, торговельних центрів, розважальних закладів, промислових підприємств і т. п. У разі виникнення кримінальних ситуацій, дані системи дозволяють вжити заходів щодо запобігання злочинів, а також зафіксувати процес вчинення злочинів і злочинців за допомогою відеозапису, який може бути використаний в оперативно-розшукових заходах і розглянутий як один з доказів у суді.

Вважаємо, що треба ширше впроваджувати автоматизовані системи пошуку і розпізнання зовнішності за допомогою спеціалізованих програм. Аналіз показує, що такі системи в даний час розроблені і можуть бути адаптовані до розпізнавання образів, що зафіксовані відеоконтрольними пристроями. Найбільш відомими є автоматизована система портретної ідентифікації (АСПІ) «ПОРТРЕТ 2005», автоматизована система портретної ідентифікації «Crime Face», апаратно-програмний комплекс (АПК) «ОБРАЗ + +» («СОВА»). В результаті проведеного тестування цих трьох систем на масиві в 110 тисяч підоблікових осіб кращою визнано АІПС «Портрет 2005» [1]. Представляє також інтерес використання для цілей ідентифікації осіб, знятих відеоконтрольними пристроями, системи: ZN-SmartEye (Vijsage FaceFinder), а також КРІМНЕТ ®, яка є інтелектуальною

шуку за ознаками зовнішності людини,
методики криміналістичного опису
учних нейронних мереж (штучного інтелекту) та інтернет-технологій [2]. У цього програмного комплексу – велике майбутнє, його можна використовувати для фейс-контролю в офісах, спостереження за фанатами на футбольних матчах, забезпечення безпеки в місцях масових гулянь. Серед перспективних планів - «пошук» злочинців на вулицях великих міст в автоматичному режимі розпізнання в потоці відеоінформації з викликом групи затримання.

Для вирішення цих важливих завдань можуть бути використані інтелектуальні відеокамери, розроблені в інституті кібернетики

ім. В. М. Глушкова НАН України, що дозволяють в потоці габітоскопічної інформації виділяти, розпізнавати і відстежувати осіб по заданих для розпізнання ознаками зовнішності даними [3]. Для забезпечення цієї роботи можуть бути використані численні відеореєстраційні пристрої, що встановлюються в громадських місцях. Завдання полягає в тому, щоб ці, зазвичай відомчі системи цифрового відеоспостереження, були об'єднані в єдину телекомунікаційну мережу або, в крайньому випадку, зафіксована відеоінформація могла бути при необхідності використана правоохоронними органами. Важко перелічити всі можливі випадки, коли в цьому може виникнути необхідність. Наприклад, на місці події виявлено рецепт, ліки куплені в аптеці, в якій працює система відеореєстрації. У результаті перегляду відеофайлів може бути отримана інформація про зовнішність людини, що купила дані ліки. Відеокамери, встановлені в квартирах, заміських будинках, дозволяють зафіксувати дії злодіїв, своєчасно направляти слідчо-оперативні групи на місце злочину, через системи відеореєстрації на автомобілях можна отримати інформацію про події, що відбуваються на дорогах. Існують відеосистеми, що дозволяють реагувати на кримінальні дії людей на автостоянках і задіяти відповідні заходи реагування. Кількість встановлюваних відеокамер спостереження росте і треба навчитися користуватися обширними масивами криміналістичної інформації не тільки при розкритті злочинів, але і в цілях їх запобігання. Для цього треба забезпечувати інформування населення про всі випадки позитивного використання відеокамер спостереження для викриття злочинців. У літературі, в ЗМІ досить часто наводяться приклади, коли відеокамера фіксує дії злодія в офісі, розбійний напад в ліфті і пр. У м. Суми на вул. Черепіна в нічний час відбулося зіткнення 2 – х автомашин, водії яких вперто заперечували свою провину. Перевірили наявність відеокамер, встановлених в безпосередній близькості аварії, і змогли отримати відеоінформацію, зафіксовану камерою, встановленою на будівлі автомагазину. Перегляд відеоматеріалу дозволив експертам-автотехнікам НДЕКЦ УМВС України в Сумській області розібратися в складній ситуації.

Таким чином, використання інформації про ознаки зовнішності, що одержані з різноманітних систем цифрового відеоспостереження, які встановлені в банкоматах, магазинах, вокзалах, громадських місцях, дозволяє підвищити ефективність роботи правоохоронних органів при попередженні злочинів. Представляється важливим при цьому подолати відомчу роз'єднаність систем спостережень і закільцювати всі відеокамери в єдину комп'ютерну мережу або

забезпечити доступ до баз відеоінформації співробітників правоохоронних органів, що накопичуються.

Список використаних джерел:

1. Габитоскопический поиск [Електронний ресурс]. – Режим доступу: http://www.portret.tomsk.ru/index.php?page=informations&subject=gabitoskopia.

2. Каракулин П. А. Опыт использования признаков внешности человека в АИПС МВД по Удмуртской республике / П. А. Каракулин, А. Р. Поздеев // Вісник Луганського державного університету внутрішніх справ. – 2010. – № 1, спец. вип. – С. 145–148.

3. Высокие технологии послужат Закону [Електронний ресурс] // Именем закона. – Режим доступу: http://www.imzak.org.ua/articles/article/id/2003.

Отримано 08.11.2012

—

УДК 378.126

Олексій Михайлович РВАЧОВ
викладач кафедри інформаційної безпеки факультету психології, менеджменту, соціальних та інформаційних технологій Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ ВІДЕОКОНФЕРЕНЦІЙ ДЛЯ ФОРМУВАННЯ ПРОФЕСІЙНИХ ЯКОСТЕЙ КУРСАНТІВ ЩОДО БОРОТЬБИ ІЗ КІБЕРЗЛОЧИНАМИ

Розглянуто ефективність застосування новітніх освітніх технологій, а саме відеоконференцій, у процесі викладання дисциплін професійної спрямованості курсантам у вищих навчальних закладах МВС України.

Становлення інформаційного суспільства не лише дає змогу будувати більш ефективне та успішне суспільство, але й надає нових імпульсів традиційним загрозам безпеки держави та створює принципово нові складнощі для системи національної безпеки. В таких умовах особливого значення набуває пошук нових можливостей забезпечення безпеки держави з огляду на формування нового поля протиборства – кіберпростору.

Більшість представників відомств, що задіяні в системі забезпечення кібербезпеки України, відмічають незадовільне кадрове забезпечення відомств відповідними фахівцями у сфері інформаційної безпеки [1].

Під час навчання у вищому навчальному закладі системи МВС України курсантів – майбутніх фахів боротьби із кіберзлочинністю, питання отримання ними знань, вмінь, професійних навичок щодо попередження та розкриття правоохоронцями кіберзлочинів набуває ще більшої актуальності.

Проблема викладання навчальних дисциплін, що пов'язані з проблемами боротьби зі кіберзлочинами, полягає в тому, правопорушення у сфері інформаційних технології мають динамічний характер. В.М. Бабакін з цього приводу відмічає, що в результаті швидкого розвитку нових технологій не менш швидкими темпами з'являються нові форми комп'ютерної злочинності, які отримують поширення при використанні нових методів [2].

Через те, в навчальному процесі виникає проблема – щойно підготовлена навчально-методична продукція у сфері боротьби з кіберзлочинністю може бути вже неактуальною. Одним із шляхів вирішення даної проблеми є залучення до навчального процесу знань не тільки осіб, які мають досвід щодо боротьби із кіберзлочинами, а також осіб, що мають досвід вчинення кіберзлочинів та виявили

нфіденційні основі з правоохоронними

ьному процесі.

Основна частина. А.В. Мовчан зазначає, що вищими навчальними закладами МВС активно використовується така форма взаємодії «теорії і практики» як залучення практичних працівників, які прибувають за запрошенням до ВНЗ та безпосередньо залучаються до проведення навчальних занять з курсантами у формі семінарів, круглих столів за напрямами їх діяльності і спеціалізації підготовки. Одним із напрямів залучення практичних працівників до участі в навчальному процесі є проведення бінарних занять, коли заняття з курсантами і слухачами проводить не лише викладач, а й практичний працівник ОВС [3].

Але таке залучення практичного працівника до участі у навчальному процесі вимагає «відірвати» його від виконання його безпосередніх функціональних обов'язків не тільки на час проведення такого заняття, але й на час, що йому необхідний щоб дістатися до навчального закладу та у зворотному напрямку. Тому, нажаль, частіше до навчального процесу залучаються лише практичні працівники, що

працюють у тому ж населеному пункті або області, в якому знаходиться навчальний заклад.

В МВС України для проведення нарад, колегій, конференцій та інструктивно-методичних зборів вже не перший рік використовується відеоселекторий зв'язок керівництва апарату МВС України з керівниками та працівниками територіальних органів внутрішніх справ. Такий відеозв'язок можна організовувати як шляхом використання відомчої телекомунікаційної мережі, так і через всесвітню мережу Інтернет.

У сучасних навчальних аудиторіях ВНЗ встановлюються стаціонарні комп'ютери або розгортаються бездротові мережі, через які можна отримати доступ до мережі Інтернет. Якщо до такого комп'ютера, що встановлений в навчальні аудиторії, підключити вебкамеру, акустичні колонки, радіомікрофон та мультимедійний проектор, то його можна використовувати для проведення Інтернет відеоконференцій між особами, що навчаються, та співрозмовником, що може знаходиться, навіть, у іншій частині світу. З'являється можливість залучити до навчального процесу будь-якого практичного працівника з будь-якого куточку світу, навіть із-за кордону. У такого працівника зникає необхідність діставатися до навчального закладу, через що економиться його робочий час. А навчальний заклад розширює «географію» та перелік осіб, що можуть бути залучені до навчального процесу щоб поділитися своїм практичним досвідом та напрацюваннями.

Отже, завдяки використанню інноваційних новітніх педагогічних інструментів, таких як відеоконференції, процес підготовки майбутніх фахівців у сфері боротьби з високотехнологічними злочинами набуває нового рівня, дозволяє зробити навчальний процес більш ефективним, а у інформативному плані більш інтенсивним, насиченим. Також, відеоконференції дозволяють заповнити навчально-методичний вакуум, що утворюється з об'єктивних причин відставання оновлення розвитку методичної бази відносно процесу еволюції кіберзлочинності.

Список використаних джерел:

1. Сучасні тренди кібербезпекової політики: висновки для України [Електронний ресурс] : аналіт. записка / Нац. ін-т стратег. дослідж. при Президентові України. – Режим доступу: http://www.niss.gov.ua/articles/294/.

2. Бабакін В. М. Особливості міжнародного співробітництва при розслідуванні кіберзлочинів / В. М. Бабакін // Форум права. – 2011.

– № 4 [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/2011-4/11bvmprk.pdf.

3. Мовчан А. В. Актуальні проблеми підготовки фахівців для оперативних підрозділів органів внутрішніх справ [Електронний ресурс] / А. В. Мовчан // Науковий вісник Львівського державного університету внутрішніх справ. – 2009. – № 1. – Режим доступу: http://www.nbuv.gov.ua/portal/Soc_Gum/Nvlduvs/2009_1/09mavovs.pdf.

Отримано 15.11.2012

—

УДК 343.96

Олександр Сергійович РОЗУМОВСЬКИЙ
курсант групи ФДС-09-5 факультету з підготовки слідчих
Харківського національного університету внутрішніх справ

СУЧАСНІ ЗАГРОЗИ: КОМП'ЮТЕРНИЙ ТЕРОРИЗМ ЯК ОСНОВНА ПРОБЛЕМА БОРОТЬБИ З КІБЕРТЕРОРИЗМОМ ТА КІБЕРЗЛОЧИННІСТЮ

Досліджено такі явища сучасних загроз, як кібертероризм та кіберзлочинність. Розкрито зміст понять кіберзлочинність та кібертероризм. Запропоновано низку заходів щодо удосконалення боротьби з цими явищами.

Розвиток інформаційних та телекомунікаційних технологій призвів до того, що сучасне суспільство все більше залежить від управління різними процесами за допомогою комп'ютерної техніки, електронної обробки, збереження, доступу та передачі інформації. Таким чином, об'єкти енергетичного забезпечення, транспортні системи, фінансові і банківські структури, військові відомства та правоохоронні органи, торгівельні, медичні й наукові установи – усі, хто використовує всесвітню мережу Інтернет, є потенційними жертвами комп'ютерного тероризму.

Поняття «комп'ютерний тероризм», «кібертероризм», «інформаційний тероризм» достатньо давно використовують у засобах масової інформації та наукових публікаціях. При цьому, з огляду на новизну, цей термін досить складний для розуміння і має різноманітне трактування щодо своїх кваліфікуючих ознак.

В українській і зарубіжній науковій літературі, пов'язаній з дослідженням кіберзлочинності, наявні різні підходи до визначення кібертероризму та його кваліфікації.

Прихильники першого підходу відносять кібертероризм до категорії комп'ютерних злочинів. Ними зауважується, що комп'ютерний тероризм слід розглядати як один із різновидів неправомірного доступу до комп'ютерної інформації, розміщеної в окремій обчислювальній машині чи в мережі ЕОМ, він здійснюється з метою модифікації, знищення зазначеної інформації чи ознайомлення з нею, що забезпечує формування обстановки, за якої функціонування даної ЕОМ чи мережі виходить за межі, передбачені штатними умовами експлуатації, й виникає небезпека загибелі людей, заподіяння майнового збитку або настання будь-яких інших суспільно небезпечних наслідків. При цьому основними цілями здійснення вищезазначених дій вважається тиск на органи влади, дестабілізація суспільно-політичної обстановки за рахунок залякування, ускладнення

аслідок, вплив на транспортні засоби, кі ними використовуються, що майже сі переслідує тероризм [1].

Прихильники другого підходу, вважають, що кібертероризм – це різновид тероризму, в основу якого покладено спосіб здійснення терористичних дій, що виник у процесі розвитку інформаційно-телекомунікаційних технологій та впровадження їх у всі сфери сучасного суспільства [2; 3].

У дослідників з проблем тероризму існує й інша точка зору щодо природи кібертероризму. Вони вважають, що кібертероризм проявляється у двох формах: по-перше, комп'ютерні економічні злочини, які вчиняються за допомогою спеціалістів-хакерів, по-друге, розголошення таємниці – отримання комерційної та конфіденційної інформації (що нерозривно пов'язане з першим видом) [5].

Слід зауважити, що до комп'ютерного тероризму правоохоронці відносять і дії, пов'язані з розміщенням у глобальній мережі Інтернет інформації терористичного та екстремістського змісту через створення відповідних сайтів.

У першу чергу, таке розходження думок пов'язане з тим, що до структурицього поняття належать дві рівнозначні правові категорії: тероризм і комп'ютерна злочинність (кіберзлочинність).

Зауважимо, що під категорією кіберзлочини слідрозуміти злочини, що вчиняються з використанням кіберпростору.

Таким чином, до цієї категорії необхідно віднести злочини, у яких способом їх вчинення є використання кіберпростору, а основною

метою вчинення таких злочинів у більшості випадків є одержання матеріальної вигоди.

Відповідно до статті 1 Закону України «Про боротьбу з тероризмом» «тероризм – суспільно небезпечна діяльність, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя чи здоров'я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей» [8].

Що ж до чинного законодавства України, то поняття комп'ютерного тероризму не знайшло свого закріплення і роз'яснення в жодному нормативному акті.

Таким чином, чинна вітчизняна нормативно-правова база у сфері протидії злочинам у кіберпросторі лише частково задовольняє потреби часу та не завжди охоплює всі ключові елементи, які необхідні для ефективної протидії кіберзлочинам всіх рівнів складності. На сьогоднішній день в Україні діє низка Законів України та нормативних документів різних рівнів, що охоплюють проблеми забезпечення кібербезпеки держави. На нашу думку доцільним є проведення засідання Ради національної безпеки і оборони з метою більш повного обговорення на найвищому рівні проблем забезпечення кібернетичної безпеки України. Це додатково дозволить формалізувати та прискорити процес підготовки законопроекту «Про кібернетичну безпеку України», перевівши контроль за його виконанням на президентський рівень.

Список використаних джерел:

1. Малышенко Д. Г. Противодействие компьютерному терроризму – важнейшая задача современного общества и государства / Д. Г. Малышенко ; ВНИИ МВД России // Вестник РАЕН. – 2004.– № 4. – Т. 3.

2. Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинами : монографія / В. О. Голубєв. – Запоріжжя : ГУ «ЗІДМУ», 2003. – 250 с.

3. Старостина Е. Терроризм и кибертерроризм – новая угроза международной безопасности [Електронний ресурс] / Е. Старостина. – Режим доступу: http://www.crime-research.ru/articles/starostina.

4. Журавльов В. П. Тероризм: сучасний стан та міжнародний досвід боротьби / В. П. Журавльов, Б. В. Романюк, В. В. Коваленко. – К. : Нац. акад. внутр.справ України, 2003. – 403 с.

5. Про боротьбу з тероризмом : закон України // Відомості Верховної Ради. – 2003. – № 25. – Ст. 180.

6. Науково-практичний коментар до Кримінального кодексу України : за станом законодавства і постанов Пленуму Верховного суду України на 1 груд. 2001 р. / за ред. С. С. Яценка. – К., 2002. – 936 с.

Отримано 20.11.2012

УДК 004.932.2:681.3.06

Діана Олександрівна РУДЕНКО
кандидат технічних наук, старший науковий співробітник,
доцент кафедри інформатики
Харківського національного університету радіоелектроніки
Анастасія Романівна КРАСЮК
студент Харківського національного університету радіоелектроніки

ОПТИМІЗАЦІЯ ЗАПИТІВ В ЗАДАЧАХ ІНТЕГРАЦІЇ ІНФОРМАЦІЙНИХ СИСТЕМ ПІДРОЗДІЛІВ ОВС

Розглянуто задачу вдосконалення якості інформаційних систем для оперативних прийнять рішень керівників підрозділів. Для рішення цієї задачі запропоновано використовувати неповне з'єднання при реалізації запиту, що дає можливість реалізувати більш ефективний план з'єднання відношень.

Динамічність соціальних процесів, постійно змінні умови криміногенної ситуації, що зростає, обсяг інформації, необхідної для рішення задач керування, потребують від органів внутрішніх справ (ОВС) нового підходу до організації інформаційного забезпечення керування та підвищення його оперативності.

Рішення даної проблеми пов'язане з використанням сучасних інформаційних технологій, що дозволяють вирішити задачі оптимального забезпечення інформаційних потреб керівників ОВС як верхнього, так і нижнього рівнів керування.

Одним з основних напрямів удосконалювання інформаційної системи ОВС є комплексна автоматизація окремих технологічних ланок обробки даних і наступне об'єднання цих ланок у єдиний,

повністю автоматизований комплект. Основу такого комплексу повинні скласти інтегровані бази даних (БД), які дозволять створити ефективне робітниче середовище для керівника.

Говорячи про ефективну роботу БД, матиме на увазі аспект оптимізації запитів, тобто такий спосіб виконання запитів, коли по його початковому поданню шляхом синтаксичних і семантичних перетворень виробляється процедурний план виконання запиту, найбільш оптимальний при існуючих у базі даних керуючих структурах. Відповідні перетворення початкового подання запиту виконуються спеціальним компонентом системи керування БД – оптимізатором. Оптимальність виробленого їм плану запиту носить досить умовний характер – план оптимальний відповідно до критеріїв, закладеними в оптимізаторі [1].

Простір пошуку в контексті реляційних запитів можна представити у вигляді або лінійної послідовності операцій з'єднання, ті [2]. Наприклад, лінійна а *Join*(*Join*(*A*,*B*), *Join*(*C*,*D*)), де *Join* – з'єднання, а *A*,*B*,*C*,*D* – відношення БД.

Такі послідовності логічно еквівалентні, оскільки з'єднання мають властивості асоціативності та комутативності. Для їхньої реалізації можна використовувати методи вкладених циклів або сортування та злиття. Хоча попарне з'єднання приводить до більш дешевого плану виконання запиту, воно значно збільшує витрати на перебір простору пошуку. Так найбільші витрати виникають при генерації синтаксичних порядків з'єднань.

На відміну від природного з'єднання послідовність однобічних з'єднань не можна довільно змінювати. Таку проблему можна частково вирішити використавши тотожне перетворення *Join*(*A*,*B LRJoin C*) = *Join*(*A*,*B*) *LRJoin C*, де *LRJoin* – однобічне з'єднання.

Якщо продовжувати застосовувати це правило асоціативності, одержимо еквівалентне вираження, у якому обчислення блоку природних з'єднань буде передувати блоку однобічних з'єднань. У такий спосіб подальше переупорядкування природних з'єднань приведе до зниження виконання запиту.

Проблема вибору відповідного набору параметрів для визначення вартості заслуговує на значну увагу. В оцінних моделях необхідно враховувати аспекти фізичного проекту, Однак забезпечення можливості дійсно точних оцінок вартості інформаційних потоків даних залишаються досить важкими запитаннями оптимізації запитів.

Говорячи про необхідність створення в системі органів внутрішніх справ інформаційних систем з використанням інтегрованих баз даних, було б несправедливо обійти проблеми, що виникають при їхній практичній реалізації. Основні з них можна об'єднати у дві групи:

– проблеми технічного характеру;

– проблеми, пов'язані із програмним, методичним і нормативним забезпеченням.

Рішення першої проблеми пов'язана зі створенням незалежних структур БД, що не залежать від технічних засобів для яких розробляється інформаційна система. Для розв'язання другої проблеми необхідно розробити науково обгрунтовану й практично реалізовану єдину концепцію планомірного оснащення органів внутрішніх справ автоматизованими робітниками місцями та підключення їх до інформаційної мережі ОВС.

Таким чином, рішення розглянутих проблем дозволить раціоналізувати інформаційні потоки й забезпечити своєчасне одержання інформації, підвищити швидкість реагування на зміну обстановки, а також рівень оперативного керування підрозділами внутрішніх справ.

Список використаних джерел:

1. Мейер Д. Теория реляционных баз данных / Д. Мейер. – М. : Мир, 1987. – 608 с.

2. Пономаренко Л. А. Построение оптимальной послідовательности соединения отношений в запросах реляционной базы данных / Л. А. Пономаренко, С. С. Танянский, В. А. Филатов // Системні дослідження та інформаційні технології. – 2003. – № 2. – С. 53–58.

Отримано 05.11.2012

УДК 351.746.2

Тетяна Іванівна САВЧУК
кандидат юридичних наук,
старший викладач кафедри криміналістики, судової медицини
та психіатрії факультету з підготовки слідчих
Харківського національного університету внутрішніх справ

ДЕЯКІ ПРОБЛЕМИ ВИКОРИСТАННЯ НОВІТНІХ ТЕХНОЛОГІЙ У ДІЯЛЬНОСТІ СЛІДЧИХ ПІДРОЗДІЛІВ ОВС

Розглянуто деякі проблемні питання використання новітніх технологій у розкритті та розслідуванні кримінальних правопорушень.

Загально відомо, що досягнення науково-технічного прогресу покликані полегшити умови життєдіяльності людини. Це стосується будь-якого виду діяльності в тому числі і правоохоронної. Новітні технології зараз використовуються будь-де і будь-ким, проте, коли це стосується діяльності з розкриття та розслідування злочинів, то виникає ряд питань, пов'язаних з правовою регламентацією їх використання. Однак не лише процесуальне закріплення є проблемою, яку в тій чи іншій мірі намагаються вирішити за допомогою положень нового кримінального процесуального законодавства, але і незадовільне матеріально-технічне забезпечення підрозділів ОВС.

оворити про слідчі підрозділи, то, на користуватися власною технікою, тому ю – вже давно застаріла.

Дані питання набувають актуальності у світлі нового Кримінального процесуального кодексу, так як його положення закріплюють використання у кримінальному процесі деяких сучасних технічних досягнень. Проте, як вказують працівники практичних підрозділів, наявна у їх розпорядженні комп'ютерна техніка поки що не дозволяє виконувати деякі положення кодексу.

Наприклад, внесення відомостей до Єдиного реєстру досудових розслідувань передбачає наявність у кожного слідчого комп'ютера підключеного до Internet, спеціального програмного забезпечення та паролю доступу. І вже на цьому етапі виникають проблеми, адже у більшості райвідділів по-перше, комп'ютери не підключені до мережі Internet, по-друге, технічні характеристики не дозволяють встановити на застарілі комп'ютери вказане програмне забезпечення.

Інший приклад: положеннями кодексу передбачена можливість проведення дистанційно слідчих дій у режимі відеоконференції. Звісно

це повинно забезпечити комфортність та швидкість процесу, однак, коли така можливість стане доступною для більшості слідчих – невідомо, адже є райвідділи, в яких до Internet підключений лише один комп'ютер, котрий може навіть не мати необхідних комплектуючих.

Потрібно також зазначити, що в деяких випадках слідчим необхідно працювати з інформацією, яка становить державну таємницю, тому комп'ютерно-апаратний комплекс на якому проводиться опрацювання та оформлення матеріалів кримінального провадження, які містять державну таємницю повинен мати певний рівень захисту. Крім того в таких випадках слід суворо дотримуватись вимог, які ставляться до зберігання такого виду документації.

Отже, можна відзначити, що законодавче закріплення використання досягнень науково-технічного прогресу у кримінальному процесі покликано позитивно вплинути на діяльність щодо розкриття та розслідування кримінальних правопорушень, однак постає питання матеріально-технічного забезпечення правоохоронних органів, яке є основною перепоною до використання новітніх технологій у правоохоронній діяльності.

Отримано 15.11.2012

—

УДК 371:004

Ірина Костянтинівна СЕЗОНОВА
кандидат технічних наук,
професор кафедри інформатики та інформаційних систем
і технологій у діяльності ОВС факультету психології, менеджменту,
соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЯК ІНСТРУМЕНТ ПОПЕРЕДЖЕННЯ КОРУПЦІЙНИХ ДІЯНЬ

Розглянуто питання інформаційної технології як інструменту попередження корупційних діянь.

Інформаційна закритість суспільства завжди була живильним середовищем для розвитку корупції. З появою усесвітньої комп'ютерної мережі Інтернет та запровадженням інформаційних

технологій ситуація почала змінюватися на краще. Простота і швидкість, яку отримують громадяни при контакті з державними органами за допомогою комп'ютерних мереж щодо ухвалення якого-небудь документа або обговорення будь-якого питання з вищим державним чиновником, не викликає сумнівів. Але, нажаль, інформаційні технології не є панацеєю від корупції. При некоректному їх використанні вони можуть навидь сприяти її поширенню в нових, ще більш завуальованих формах.

Зазначимо, що корупція існує не тільки в органах державної влади, але і в приватному бізнесі. У крупних компаніях менеджери часто безконтрольно розпоряджаються майном і здійснюють операції, далеко не завжди бездоганні з етичної точки зору.

Як і всяка новина, інформаційні технології несуть в собі нові небезпеки, які можуть слугувати дестабілізуючим чинником. Помилки (а частіше, використання некоректних алгоритмів), зроблені в процесі проектування комп'ютерної системи, дають про себе знати досить швидко в процесі експлуатації системи і не завжди піддаються усуненню. Тому процес проектування системи вимагає особливої уваги і залучення фахівців.

До типових проектних помилок комп'ютерних систем можна віднести:

– відсутність чіткого розділення прав доступу в систему (з можливістю зміни даних) відповідно до посадових обов'язків співробітників;

– відсутність модуля-аналізатора процесів зміни даних в системі, який позволяє відстежити підозрілі або неправомірні трансакції;

– відсутність протоколювання дій системного адміністратора;

– відсутність системи ідентифікації користувача (на який доступ продемонстрував свою неспроможність);

– відсутність правил ведення архіву, які адекватні проектованій технології документообігу.

Створений електронний архів повинен забезпечувати оперативний і повноцінний доступ до всіх документів, які зберігаються і поступають в систему.

Інформаційні технології сприяють прозорості дій владних структур тільки в тому випадку, якщо принцип прозорості спочатку закладається в проектовану комп'ютерну систему. На жаль, так буває далеко не завжди. Англійські журналісти стверджують, що британська ініціатива переводу державних органів на роботу через Інтернет може привести до створення онлайнового варіанту традиційної бюрократії.

Такий висновок зроблено в сумісному звіті фахівці англійської медійної групи Demos і компанії EzGov, що спеціалізується на технологіях онлайнової роботи урядових установ [1].

Інтернет може допомогти вирішити безліч проблем в питаннях антикорупційної профілактики, які довгі роки не вирішувалися у зв'язку з відсутністю інформаційної прозорості, пов'язаної з бюджетними процесами, як на державному, так і на місцевому рівнях.

В Україні, наприклад, з'явилася можливість подавати митні декларації в електронному вигляді і тим самим *уникати прямого контакту* між митником і декларантом. З початком застосування електронних цифрових підписів такого роду технології повинні набути широкого поширення, що також сприятиме зменшенню рівня корупції.

Наведені приклади свідчать про реальність протидії корупції за допомогою нових технологій. Важливо не переоцінити роль інформаційних технологій в житті соціуму. *Корупціонери напевно спробують пристосуватися до реалій інформаційного суспільства*. Але те, що технології дозволяють зробити державні структури «прозорими», вже можна вважати важливим кроком в боротьбі з корупційними проявами.

Відповідаючи на виклики інформаційного суспільства, нашій країні ще належить пройти довгий шлях в питаннях захисту прав громадян на інформацію про діяльність державних структур, а також до використання досягнень науково-технічного прогресу для протидії корупції. При цьому важливо враховувати, що інформаційні технології роблячи діяльність держави «прозоріша», не можуть автоматично знищити таке соціальне явище як корупція. В ході реалізації концепції «електронного уряду» необхідно буде розробити і реалізувати на практиці зведення визначень, принципів, норм, правив, пов'язаних з інформаційною відкритістю державних інститутів, які повинні бути основою антикорупційних взаємин між громадянином, громадськістю і державою.

Список використаних джерел:

1. Уильямс Ф. Организованная преступность и преступность в сфере компьютерных технологий: симбиоз, тенденции развития и ответные действия [Електронний ресурс] / Ф. Уильямс. – Режим доступу: http://www.pitt.edu/~rcss/toc.html.

2. Пономарев Д. А. Информационные технологии как криминогенный фактор организованной преступности в условиях глобализации [Електронний ресурс] / Д. А. Пономарев. – Режим доступу: http://www.ifap.ru/pi/05/ponomarev.htm.

3. Скаццо А. Сражаясь с коррупцией в цифровом формате [Електронний ресурс] / А. Скаццо. – Режим доступу: http://crime.vl.ru/docs/stats/stat_66.htm.

Отримано 16.11.2012

—

УДК 343.85:343

Микола Володимирович СТАЩАК
кандидат юридичних наук, старший науковий співробітник,
доцент кафедри оперативно-розшукової діяльності
навчально-наукового інституту підготовки фахівців кримінальної міліції
Харківського національного університету внутрішніх справ

ЗНАЧЕННЯ ТА МІСЦЕ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Розглянуто значення та місце нового кримінального процесуального законодавства для оперативно-розшукової діяльності.

Розробка та прийняття нового Кримінального процесуального кодексу (далі – КПК) України стали одним із послідовних кроків законодавця у оновленні системи кримінальної юстиції, концепція реформування якої визначена рішенням Ради національної безпеки і оборони України від 15 лютого 2008 р. «Про хід реформування системи кримінальної юстиції та правоохоронних органів», ента України від 8 квітня 2008 р. рамні вимоги цього документу, Україна озі радикальних змін самої системи кримінального переслідування, у контексті якої здійснюється поступальний розвиток оперативно-розшукового законодавства тощо [1, с. 186].

Водночас, у зв'язку з прийняттям нового Кримінального процесуального кодексу України та набранням ним чинності, діяльність правоохоронних органів у найближчому часі буде вимагати суттєвої оптимізації, відповідно до новітніх засад здійснення кримінального провадження.

Неабиякою мірою це стосується місця оперативно-розшукової діяльності у структурі досудового розслідування [2, с. 39] та кримінального провадження в цілому.

Подальше вивчення обраної нами проблематики показало, що у розділі 2 КПК України від 13.04.2012 «Сторона обвинувачення» закріплено ст. 41 «Оперативні підрозділи». У ній визначено, що оперативні підрозділи органів внутрішніх справ здійснюють слідчі (розшукові) дії та негласні слідчі (розшукові) дії в кримінальному провадженні за письмовим дорученням слідчого, прокурора (ч. 1). У ч. 2 ст. 41 КПК зазначено, що під час виконання доручень слідчого, прокурора співробітник оперативного підрозділу користується повноваженнями слідчого. Співробітники оперативних підрозділів не мають права здійснювати процесуальні дії у кримінальному провадженні за власною ініціативою або звертатися з клопотаннями до слідчого судді чи прокурора [3].

На наш погляд, доцільно зупинитися на зазначених положеннях із КПК України більш детально. По-перше, викликає запитання доцільність поміщення законодавцем ст. 41 «Оперативні підрозділи» у розділ 2 «Сторона обвинувачення». Це фактично відносить оперативні підрозділи до сторони обвинувачення, хоча останні повинні збирати первинну інформацію та докази як винуватості, так і невинуватості осіб. Наш погляд, у суспільства можуть виникнути певні побоювання стосовно місця оперативних підрозділів у системі кримінального провадження.

По-друге, у ч. 1 ст. 41 КПК України від 13.04.2012 зазначено, що оперативні підрозділи органів внутрішніх справ здійснюють слідчі (розшукові) дії та негласні слідчі (розшукові) дії в кримінальному провадженні за письмовим дорученням слідчого, прокурора [3]. Із цього положення формується враження, що лише за письмовим дорученням слідчого чи прокурора, оперативні підрозділи можуть проводити негласні слідчі (розшукові) дії (іншими словами «оперативно-розшукові заходи»). Однак, це враження є хибним, оскільки у новій редакції Закону України «Про оперативно-розшукову діяльність» закріплено наступне: «Негласне обстеження публічно недоступних місць, житла чи іншого володіння особи, аудіо-, відеоконтроль особи, аудіо-, відеоконтроль місця, спостереження за особою, зняття інформації з транспортних телекомунікаційних мереж, електронних інформаційних мереж, накладення арешту на кореспонденцію, здійснення її огляду та виїмки, установлення місцезнаходження радіоелектронного засобу проводяться на підставі ухвали слідчого судді, постановленої за клопотанням керівника

відповідного оперативного підрозділу або його заступника, погодженого з прокурором» (ч. 3 ст. 8) [4, с. 323]. Таким чином, оперативні підрозділи в передбачених законом випадках можуть самостійно ініціювати проведення негласних слідчих (розшукових) дій, про що, на жаль, не відмічено у КПК України від 13.04.2012.

По-третє, виходячи із положень ч. 2 ст. 41 КПК України, де вказано, що під час виконання доручень слідчого, прокурора співробітник оперативного підрозділу користується повноваженнями слідчого, можна зробити висновок про чергове повернення до термінологічної плутанини. Зміст її полягає в тому, що законодавець у КПК України від 13.04.2012 почав застосовувати до оперативного складу оперативних підрозділів термін «співробітники», незважаючи на те, що в Законі України «Про оперативно-розшукову діяльність» вживається поняття «працівники».

Підсумовуючи наведене, ми дійшли висновку, що положення КПК України потребують певних уточнень з точки зору оперативно-розшукової діяльності, що може бути досягнено лише за допомогою загальних зусиль вчених і практичних працівників у вигляді розробки пропозицій і рекомендацій, які будуть впроваджені у правозастосовній сфері.

Список використаних джерел:

1. Скулиш Є. Д. Кримінальний процесуальний кодекс України 2012 року – імпульс оновлення оперативно-розшукової діяльності / Є. Д. Скулиш // Оперативно-розшукова діяльність ОВС: проблеми теорії та практики : матеріали Всеукр. наук.-практ. конф. (Дніпропетровськ, 21 верес. 2012 р.). – Д. : ДДУВС, 2012. – С. 183–186.

2. Варава В. В. Концепт інституту негласних слідчих дій у контексті нового кримінального процесуального законодавства України / В. В. Варрава // Оперативно-розшукова діяльність ОВС: проблеми теорії та практики : матеріали Всеукр. наук.-практ. конф. (Дніпропетровськ, 21 верес. 2012 р.). – Д. : ДДУВС, 2012. – С. 39–43.

3. Кримінальний процесуальний кодекс України : закон України від 13.04.2012 № 4651-VI [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/4651-17/page4. – Редакція від 05.07.2012.

4. Кримінальний процесуальний кодекс України. Закон України «Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Кримінального процесуального кодексу України». – Х. : Одіссей, 2012. – 360 с.

Отримано 21.11.2012

УДК 351.74:57.087.1

Володимир Михайлович СТРУКОВ
кандидат технічних наук, доцент,
завідувач кафедри інформаційних комунікацій,
захисту інформації та документознавства
навчально-наукового інституту права та масових комунікацій
Харківського національного університету внутрішніх справ

ОКРЕМІ АСПЕКТИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ БІОМЕТРІЧНИХ ТЕХНОЛОГІЙ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Зазначено прол актуальність та проблеми застосування біометричних систем і технологій в правоохоронній діяльності. Розглянуто питання точності і достовірності результатів в автоматизованому режимі, шляхи її підвищення. Розглянуто також організаційно-технічні аспекти застосування біометричних систем.

На поточний момент залишається актуальною проблема оптимального використання напрацьованих і розробка нових, більш ефективних методів запобігання і розслідування скоєних злочинів з використанням біометричних технологій. Проблема полягає в тому, що існуючі системи в багатьох випадках поки що не забезпечують або не гарантують необхідної точності розв'язання задачі, особливо коли мова йде про автоматичний, а не автоматизований режим роботи

лькома причинами. На наш погляд з
я увага, але які визначають або суттєво
и, є наступні: 1) відсутність строгого формального підходу на етапі постановки задачі і 2) відсутність чіткої систематизації в плані визначення сфери застосування як окремих методів розв'язання так і комбінацій цих методів.

Стосовно першого слід відзначити, що навіть для таких класичних задач, як ідентифікація особи за відбитками пальців (дактилоскопія), для розв'язання яких широко і досить ефективно використовуються автоматизовані дактилоскопічні інформаційні системи (АДІС), не існує строгої математичної моделі об'єкта

ідентифікації і відповідної математичної постановки задачі, яка б дозволяла здійснити коректний аналіз задачі з метою: 1) оцінки складності, 2) теоретичної можливості її точного розв'язання, 3) обґрунтованого вибору або розробки метода розв'язання. Навіть у найбільш точній геномній дактилоскопії вірогідність ідентифікації дуже близька, але не дорівнює 100 %. Інші біометричні технології забезпечують значно меншу точність ідентифікації. Так, ідентифікація за обличчям згідно з одними даними дає середнє значення відсотку достовірності 50–60 %, хоча за іншими даними деякі системи дозволяють досягти точність ідентифікації за обличчям 90 %.

На теперішній час у контексті активізації міжнародного тероризму в усьому цивілізованому світі є розуміння необхідності точної ідентифікації особи під час перетину кордону, перевірки документів, у місцях масового скопичення людей (аеропорт, вокзал, морський порт, метрополітен, футбольний стадіон та ін.). Особливо це актуально для паспортно-візових, митних, міграційних і оперативних служб. Звичайних паспортів і фейс-контролю виявилося явно недостатньо. Великі надії тепер пов'язані з використанням біометричних технологій, що дозволяють оперативно перевіряти особистості великої кількості людей, що проходять через точку контролю. Найбільш перспективними методами в цьому напрямі вважаються безконтактні біометричні системи. Тобто, такі традиційні і найбільш відпрацьовані системи, як дактилоскопічні та за сітківкою ока в таких випадках не можуть бути використаними. А такі безконтактні системи як за малюнком обличчя не дають необхідної точності автоматичної ідентифікації внаслідок перелічених раніше причин.

Вже традиційно слабким місцем інноваційних систем в діяльності ОВС є нерозвинена нормативно-правова база їх застосування і юридичної інтерпретації результатів. В цілому можна сказати що до теперішнього часу інформаційні технології у правозастосовній галузі розвиваються в основному екстенсивним шляхом, а саме:

1) нарощуванням кількості комп'ютерної техніки;

2) накопиченням кількості даних у існуючих базах даних;

3) використанням для пошуку необхідної інформації як правило простих пошукових процедур. Тобто користувач із наявної іноді величезної купи даних має можливість знайти лише ту інформацію, яка «лежить на поверхні». Для виявлення внутрішньої структури накопичених масивів даних, явних або неявних зв'язків другого, третього і т.д. рівнів між об'єктами необхідно застосування більш

складних засобів глибинного пошуку, заснованих на математичних моделях, що мають більш високий степінь адекватності.

На сучасному етапі екстенсивні шляхи підвищення ефективності використання інформаційних технологій у правозастосовній галузі себе практично вичерпали. Подальше підвищення ефективності їх застосування можливе лише із залученням науковомістких технічних і інтелектуальних засобів. Нажаль, можна констатувати той факт, що зараз у правозастосовній сфері дуже повільно впроваджуються науковомісткі (і, відповідно, коштовні) системи і технології.

Основними причинами такого стану є:

1) висока наукоємність і, відповідно, трудоємність цих задач;

2) висока вартість проектування, розробки і впровадження;

3) необхідність залучення висококваліфікованих фахівців для реалізації цих задач, їх мотивація;

4) необхідність «підтягування» до відповідного рівня користувачів відповідних застосувань;

5) відсутність ефективного державного механізму реалізації задач такого класу та ін.

Підсумовуючи перелічене, можна впевнено сказати, що подальше суттєве підвищення ефективності розробки і застосування науковомістких технологій в діяльності ОВС неможливе без координації, фінансової і організаційної підтримки з боку держави.

Отримано 05.11.2012

УДК 004.932.2:681.3.06

Сергій Станіславович ТАНЯНСЬКИЙ
доктор технічних наук, доцент,
професор кафедри електронних обчислювальних машин
Харківського національного університету радіоелектроніки
Юлія Сергіївна ЛАГУТКІНА
студент Харківського національного університету радіоелектроніки

ВИКОРИСТАННЯ НЕВИЗНАЧЕНИХ ЗНАЧЕНЬ В ЗАДАЧАХ ПІДТРИМКИ БЕЗПЕКИ БАЗ ДАНИХ

Розглянуто питання використання невизначених значень у базах даних для розмежування доступу до інформації. Для рішення цієї задачі запропоновано скористатися трьохзначною логікою SQL і властивістю унікальності атрибутів.

При використанні сучасних інформаційних технологій виникає гостра необхідність удосконалення інформаційних систем і баз даних з метою підвищення їхньої безпеки, що прямо залежить від структури, об'єму збережених даних і кількості користувачів. Безпека баз даних протягом довгого часу перебувала на другому плані в порівнянні з такими областями, як безпека мереж і комунікацій.

На самому елементарному рівні концепції забезпечення безпеки баз даних досить прості. Необхідно підтримувати два фундаментальних принципи: перевірку повноважень і перевірку справжності. Якщо всі користувачі, що працюють в інтерактивному режимі або запускають пакетні додатки, досить надійні і мають доступ до максимально закритої інформації, збереженої в системі, то сполучення засобів перевірки повноважень і перевірки справжності може бути цілком достатнім.

Однак така система виявляється незадовільної, якщо необхідно організувати багаторівневе середовище захисту інформації. Багаторівневий захист означає, що:

– в обчислювальній системі зберігається інформація, що ставиться до різних класів таємності;

– частина користувачів не мають доступу до максимально захищеного класу інформації.

Багаторівневий захист баз даних будується звичайно на моделі Белл-ЛаПадула (Bell-LaPadula), що призначена для керування активними процесами, що запитують доступ до інформації, файлами, записами, полями або іншими об'єктами даної інформаційної моделі [1]. Хоча ці принципи самі по собі цілком застосовні на практиці,

вимога підтримки декількох рівнів захисту в межах одній базі даних пов'язано з рядом проблем.

Якщо розширити структуру таблиці, додавши властивість таємності не тільки для кожного рядка, але й для кожного стовпця (тобто значення кожного стовпця усередині кожного рядка повинне мати свою класифікацію), то можна зіштовхнутися з новими серйозними проблемами, оскільки кожний стовпець у рядку може приймати одне з декількох можливих значень, залежно від класифікації. Таке положення порушує вимога першої нормальної форми (1НФ), тому що множинні значення можуть розглядатися як повторювані групи

Проблема в цілому пов'язана із практичними потребами зберігати в базі даних не тільки достовірну і повністю визначену інформацію, але й таку, котра частково невизначена, тобто інформація існує, але в даний момент не визначена.

У стандарті мови SQL виділяється спеціальне значення *Null*, що вважається автоматично вхідним у будь-який вбудований тип даних і будь-який визначений користувачем домен [2]. При цьому, що мається на увазі під невизначеним значенням у кожному конкретному випадку, визначається семантикою предметної області. Можна казати, що в SQL використовується в, деякому змісті, тризначна логіка. Таким чином, тризначної логіки в тому вигляді, у якому вона введена в SQL, виявляється достатньої у тих випадках, коли за змістом невизначене значення є заборонним.

Наприклад, у відповідь на запит «отримати імена співробітників, що виконують завдання з кодом «секретно»», користувач із нижчою категорією доступу не одержить ім'я співробітника, що виконує «невизначене» завдання (*Null* завдання). Таким чином, для різних категорій доступу можуть генеруватися різні запити й тим самим визначатися різні результуючі значення.

Також слід зазначити, що якщо класика реляційної теорії говорить, що в будь-якому відношенні існують хоча б один можливий ключ, а первинний ключ вибирається з набору можливих ключів, то в SQL є деякі допущення. Відповідно до визначення ключа, первинний ключ не може містити невизначених значень, проте, ключі, що мають властивість *Unique*, - можуть містити невизначені значення. Отже, у таблиці бази даних підтримуючої SQL може існувати можливий ключ і одночасно не існувати первинного ключа, що дозволяє зберігати у відношенні дублюючі кортежі.

У зв'язку із цим, визначення семантики баз даних з багаторівневим захистом вимагає точно визначати, які дії зробить,

наприклад, операція *Delete* або *Update*. Отже, у загальному випадку, для підтримки багаторівневого захисту в умовах багатозначності необхідно також розширити визначення семантики операцій маніпулювання даними, довівши їх до рівня, прийнятного у реалізації конкретної системи керування базами даних.

Список використаних джерел:

1. Емелин И. В. Обеспечение многоуровневой защиты в информационных и вычислительных системах / И. В. Емелин, Р. В. Эльгиян. – М. : ВНИИМИ, 1979. – 26 с.

2. Грофф Д. SQL: полное руководство / Д. Грофф, П. Вайнберг. – Киев : BHV, 1999. – 608 с.

Отримано 05.11.2012

—

УДК 342.536:343

Олександр Васильович ТАРНОПОЛЬСЬКИЙ
здобувач кафедри оперативно-розшукової діяльності
навчально-наукового інституту підготовки фахівців кримінальної міліції
Харківського національного університету внутрішніх справ

ОСОБЛИВОСТІ ВЗАЄМОДІЇ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ ОВС З ОРГАНАМИ ДЕРЖАВНОЇ ФІНАНСОВОЇ ІНСПЕКЦІЇ ПІД ЧАС ПРОТИДІЇ ЗЛОЧИНАМ У СФЕРІ СПЕЦІАЛЬНОГО ФОНДУ БЮДЖЕТУ

Розглянуто особливості взаємодії оперативних підрозділів органів внутрішніх справ з органами державної фінансової інспекції під час протидії злочинам у сфері спеціального фонду бюджету.

Аналіз практичної діяльності оперативних підрозділів під час протидії злочинам у сфері спеціального фонду бюджету продемонстрував, що для початку кримінального провадження у більшості випадків необхідно провести ревізію, оскільки це дозволяє визначити розмір матеріальних збитків, завданих злочином. Останнє є можливим за допомогою залучення оперативними підрозділами до

процесу перевірки бюджетних установ працівників Державної фінансової інспекції.

Відповідно до ст. 2 Закону України «Про державну контрольно-ревізійну службу в Україні», головними завданнями державної контрольно-ревізійної служби є здійснення державного фінансового контролю за використанням і збереженням державних фінансових ресурсів, необоротних та інших активів, правильністю визначення потреби в бюджетних коштах та взяття зобов'язань, ефективним використанням коштів і майна, станом і достовірністю бухгалтерського обліку і фінансової звітності в міністерствах та інших органах виконавчої влади, в державних фондах, у бюджетних установах і у суб'єктів господарювання державного сектору економіки, а також на підприємствах і в організаціях, які отримують (отримували в періоді, який перевіряється) кошти з бюджетів усіх рівнів та державних фондів або використовують (використовували у періоді, який перевіряється) державне чи комунальне майно, виконанням місцевих бюджетів, розроблення пропозицій щодо усунення виявлених недоліків і порушень та запобігання їм у подальшому.

Згідно з ч. 3 ст. 4 означеного законодавчого акту, Державна контрольно-ревізійна служба координує свою діяльність з державною податковою службою, іншими контролюючими органами, органами прокуратури, внутрішніх справ, служби безпеки та ін. [1]. Враховуючи наведене є очевидним той факт, що проведення оперативними підрозділами ОВС України перевірки підприємств, організацій чи установ, які фінансуються з бюджету, без залучення спеціалістів Державної фінансової інспекції, унеможливить виявлення та фіксацію порушень фінансової дисципліни.

Необхідно відмітити, що у п. 3 «Порядку взаємодії органів державної контрольно-ревізійної служби, органів прокуратури, внутрішніх справ, Служби безпеки України» зазначено, що працівники органів ДКРС за зверненнями правоохоронних органів можуть брати участь у перевірках, що проводяться правоохоронними органами у підконтрольних установах, та на інших об'єктах контролю, – як спеціалісти.

Працівники органів ДКРС направляються для участі в перевірках, що проводять правоохоронні органи, на підставі листа відповідного органу ДКРС.

Залучення працівників органів ДКРС в якості спеціалістів до участі в перевірках, що проводять правоохоронні органи, може здійснюватися на строк до 10 робочих днів. За письмовим зверненням

правоохоронного органу цей строк може бути подовжений службовою особою органу ДКРС, визначеною в п. 2.5 Порядку взаємодії органів державної контрольно-ревізійної служби, органів прокуратури, внутрішніх справ, Служби безпеки України.

У ході участі у перевірці спеціаліст використовує свої спеціальні знання і в межах компетенції надає консультації та відповіді на порушені питання, при цьому фіксує факти порушення законодавства з питань використання і збереження фінансових ресурсів, необоротних та інших активів, правильності визначення потреби в бюджетних коштах та взяття зобов'язань, стану і достовірності бухгалтерського обліку і фінансової звітності, визначає розмір заподіяної матеріальної шкоди (збитків) та посадових (службових) осіб, внаслідок дій або бездіяльності яких допущено порушення законодавства та завдано матеріальну шкоду (збитки).

У разі можливості виконання звернення про виділення спеціалістів у зв'язку з проведенням планових та позапланових виїзних ревізій, орган ДКРС протягом двох робочих днів письмово повідомляє про це відповідний правоохоронний орган і визначає дату, з якої буде можливим направлення спеціаліста [2].

Таким чином, постійна і належним чином організована взаємодія оперативних підрозділів ОВС України з органами державної фінансової інспекції є запорукою ефективної і якісної протидії злочинам у сфері спеціального фонду бюджету.

Список використаних джерел:

1. Про державну контрольно-ревізійну службу в Україні [Електронний ресурс] : закон України від 26 січ. 1993 р. – Режим доступу: http://zakon.rada.gov.ua/laws/show/509-12.

2. Порядок взаємодії органів державної контрольно-ревізійної служби, органів прокуратури, внутрішніх справ, Служби безпеки України : затв наказом ГоловКРУ України, МВС України, СБУ, Ген. прокуратури України від 19 жовт. 2006 р. № 346/1025/685/53 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/z1166-06.

Отримано 21.11.2012

УДК 343.346.8:004.056.53

Володимир Володимирович ТОРЯНИК
кандидат фізико-математичних наук, доцент,
доцент кафедри інформаційних комунікацій,
захисту інформації та документознавства
навчально-наукового інституту права та масових комунікацій
Харківського національного університету внутрішніх справ
Олександра Володимирівна СТРУКОВА
викладач кафедри інформатики та інформаційних систем і технологій
в діяльності ОВС факультету психології,
менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ

СОЦІАЛЬНИЙ АСПЕКТ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Проаналізовано соціальний аспект кіберзлочинності в Україні, виявлено найбільш уразливі категорії населення, запропоновано освітні, організаційні та законодавчі напрями діяльності для профілактики кіберзлочинів.

Аудиторія користувачів всесвітньої мережі Інтернет в Україні динамічно розширюється, переважно за рахунок молоді. Діти та підлітки повністю не усвідомлюють реальні загрози віртуального простору. Відомі факти залучення підлітків через Інтернет до сексуального насильства, до екстремістських формувань. Однак не визначено, хто у правоохоронних органах повинен займатися цими проблемами [1]. Всеукраїнське соціологічне дослідження, проведене Інститутом соціології НАН України в 2009 році, виявило тривожні тенденції: понад 28 % опитуваних дітей готові надіслати свої фотокартки незнайомцям у Мережі, 17 % без коливань діляться персональною інформацією , 22% дітей періодично потрапляють на сайти для дорослих, 28 % дітей, побачивши в Інтернеті рекламу алкоголю або куріння, хоча б один раз спробували їх купити, а 11 % − спробували купувати наркотики, близько 14 % опитуваних час від часу відправляють платні SMS за бонуси в онлайн-іграх і не звертаючі увагу на вартість послуги. Лише у 18 % випадків дорослі перевіряють, які сайти відвідує дитина, тільки 11 % батьків знають про такі онлайн-загрози, як «дорослий» контент, азартні ігри, онлайн-насилля та кіберзлочинність [2].

За результатами дослідження «Майкрософт Україна» про рівень комп'ютерної безпеки в Україні, проведеного у 2012 р. в Києві, 92 %

українців недостатньо обізнані про кіберзагрози. У більшості українців легко виманити пароль від пошти чи спонукати дати доступ до власної інформації у соціальній мережі і тільки 8 % розуміють, як можна захиститися від таких кіберзагроз як фішинг, крадіжки особистих даних, тощо. Саме соціальна інженерія сьогодні стає основним джерелом загроз у мережі. Тільки 30 % респондентів опікується своєю репутацією в Інтернеті, третина користувачів, у яких є діти, майже нічого не знають про загрози в мережі. Також критично вразливі для кіберзлочинів користувачі, старші за 49 років – вони нічого не роблять для того, аби захиститися від кіберзагроз [3]. За даними системи моніторингу та швидкого реагування на комп'ютерні загрози Kaspersky Security Network у березні цього року на території Росії у середньому за день було зафіксовано понад 800.000 спрацювань системи захисту дітей від небажаного контенту в Інтернеті [4].

В Україні органом, на який покладаються повноваження щодо створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі, є Міністерство внутрішніх справ України [5].

Враховуючи наведене доцільна розробка наступних напрямів [6]**:**

– поширення інформації щодо правил безпечного користування мережею Інтернет;

– внесення теми онлайн-безпеки у шкільну програму для дітей віком від 7 до 14 років, а також у програму навчання та підвищення кваліфікації вчителів;

– вивчення та використовування міжнародного досвіду боротьбі з кіберзлочинністю;

– визначення поняття «дитяча порнографія» у законодавстві України;

– передбачити законодавством України покарання за виробництво чи володіння матеріалами, що характеризуються як дитяча порнографія;

– вдосконалення ресурсної бази підрозділів МВС щодо боротьби та запобігання кіберзлочинів;

– на законодавчому рівні затвердити процедуру блокування Інтернет-ресурсів, що містять інформацію в порушення українського законодавства;

– створення зони довіри в українському сегменті Інтернету.

На жаль, батьки багато чого не знають [7].

Список використаних джерел:

1. Дети и Интернет, как защитить ребенка от асоциальных сайтов? [Електронний ресурс]. – Режим доступу: http://www.svobodanews.ru/ content/transcript/462683.html.

2. Безпека дітей в Інтернеті [Електронний ресурс]. – Режим доступу: http://www.mon.gov.ua /index.php/ua/117-pozashkilna-osvita-vikhovna-robota-ta-zakhist-prav-ditini/4433-bezpeka-d%D1%96tey-v-%D1%96nternet%D1%96.

3. 92 % українців недостатньо обізнані про кіберзагрози [Електронний ресурс]. – Режим доступу: http://www.onlandia.org.ua/ SocialAction/Details/7.

4. Kaspersky Security Network [Електронний ресурс]. – Режим доступу: http://www.kaspersky.ru/downloads/pdf/kaspersky_security_ network.pdf.

5. Дети в интернете: как научить безопасности в виртуальном мире : (Пособие для родителей) / Литовченко И. В. и др. – Киев : Аванпост-Прим, 2010.

6. Про внесення зміни до Закону України «Про ратифікацію Конвенції про кіберзлочинність» : закон України [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/ show/2532-17.

7. Региональный обзор об изображениях сексуального насилия над детьми посредством использования информационных и коммуникационных технологий в Беларуси, Молдавии, России и Украине [Електронний ресурс].– Режим доступу: http://www.ecpat.net.

Отримано 15.11.2012

УДК 343.915

Назарій Дмитрович ТУЗ
здобувач кафедри кримінального права та кримінології
Львівського державного університету внутрішніх справ

ЗАПОБІГАННЯ ЗЛОЧИННОСТІ НЕПОВНОЛІТНІХ ЗАСОБАМИ СІМЕЙНОГО ВИХОВАННЯ

Досліджено вплив сімейного виховання на формування у неповнолітніх схильності до вчинення злочинів, розглянуто основні

дефекти сімейного виховання та заходи, необхідні для покращення умов сімейного виховання.

Боротьба зі злочинністю неповнолітніх на сьогоднішній день є однією з найважливіших та найактуальніших проблем українського суспільства. Зростання підліткової злочинності пов'язано, перш за все, з соціально-економічною кризою, що супроводжується деформацією фундаментальних морально-етичних цінностей, ускладненнями матеріального характеру, утвердженням культу сили, загальним падінням моралі в суспільстві, безвідповідальністю навчальних закладів за процес виховання і відпочинку учнів. у сучасних умовах набуває і така специфічна причина злочинів неповнолітніх як недоліки сімейного виховання.

Сімейне виховання виступає необхідною умовою успішного формування особистості завдяки природній близькості між вихователями і вихованцем, особливому емоційно-психологічному мікроклімату, створити який можливо лише в умовах родини.

Виховання є один із чинників, під впливом якого здійснюється розвиток дитини. Виховання формує внутрішній світ молоді, проникнути в який дуже важко. Тому воно вимагає таких методик, які давали б змогу не тільки виявляти погляди, переконання і почуття вихованців, а й збагачували їх духовністю, за потреби коригувати якості психіки [1].

Враховуючи криміногенну ситуацію в Україні, а також те, що саме негативні компоненти родинних стосунків часто виступають тим «гострим каменем», з якого починається злочинний шлях неповнолітнього, робота по вивченню кримінологічних аспектів сімейного виховання, зокрема, визначення шляхів його вдосконалення набуває суттєвої вагомості та особливої актуальності. Проблема поліпшення умов виховання в родині, хоча й неодноразово піднімалася кримінологами, ще й досі не знайшла свого повного і всебічного розв'язання.

Дитяча злочинність зростає з кожним роком. Склалася загрозлива статистика злочинності неповнолітніх, котра у декілька разів перевищує темпи зростання злочинності дорослих. Потрібно наголосити, що кримінально-активні підлітки стають резервом для дорослої злочинності.

Жертвами малолітніх злочинців зазвичай стають тварини, люди похилого віку, однолітки або молодші за віком особи. Не поодинокими є випадки, коли процес знущання над такими «жертвами» неповнолітні

знімають на мобільний телефон, щоб згодом розмістити у соціальній мережі Інтернет, що на сьогоднішній день є досить розповсюдженим.

За деякими даними, більше половини дітей, які вчиняють злочини, походять з «проблемних» сімей, кожний третій підліток-правопорушник має неповну сім'ю, у 14 % таких дітей батьки є алкоголіками, у 4 % неповнолітніх злочинців останні ведуть аморальний спосіб життя, а у майже 10 % – родичі (батьки, брати, сестри) були позбавлені волі [2].

За статистичними даними на сьогодні злочинність неповнолітніх має таку структуру: злочини проти власності – 70,5 %, хуліганство – 8,2 %, злочини, пов'язані з наркотиками – 7,8 %, злочини проти життя та здоров'я – 2,1 %, інше – 11,4 %. Загалом із початку поточного року неповнолітніми вчинено 12,5 тисяч злочинів загально-кримінальної спрямованості [3].

В Україні існує одинадцять виховних колоній, де, на даний час, проходять «перевиховання» 2215 неповнолітніх. Більше половини з них були засуджені за крадіжки, чверть – за грабіж і розбій, а 10 % – за нанесення тяжких тілесних ушкоджень та вбивство. Вікова статистика така: 14–16-літніх злочинців у колоніях – 13 %, 15–16-літніх – 28 %, 17–18-літніх – 39 %. У колонії щорічно потрапляють 70–90 % засуджених, які не мають повної середньої освіти [4].

Дефектами сімейного виховання насамперед є дефекти морально-правової позиції сім'ї, дефекти з відхиленнями у педагогічній позиції сім'ї, дефекти, що пов'язані зі структурною неповнотою родини а також дефекти пов'язані з матеріально-побутовими умовами родини. Пияцтво, алкоголізм і наркоманія дорослих, часто це супроводжується зі спробами втягнення неповнолітніх у це, аморальний спосіб життя батьків, постійні конфлікти, які виливаються у сварки, скандали, бійки, скоєння ними злочинів та інших правопорушень, негативний вплив судимих осіб – все це впливає на формування психіки людини та сприяє злочинності неповнолітніх. Окреме місце займає бездоглядність і безпритульність дітей та підлітків як одних з найнебезпечніших виявів недоліків сімейного виховання.

Сприяти поліпшенню умов сімейного виховання покликані відповідні заходи держави. Держава має передбачати підвищення матеріального добробуту родин, покращання житлових та побутових умов родин надання адресної допомоги найбільш вразливим сім'ям, посилення просвітницької діяльності з соціальних, правових, педагогічних, психологічних, економічних, медичних проблем сім'ї,

підвищення якості медичного обслуговування родин, доступність повноцінного відпочинку і оздоровлення дітей, організацію змістовного дозвілля підлітків та їх сімей тощо.

Саме родина відіграє головну роль у здійсненні всіх напрямів процесу виховання, тому завдяки цілеспрямованим виховним зусиллям батьків можна сформувати творчу, гармонійну, всебічно розвинену особистість, повноцінного члена суспільства та не допустити переходу неповнолітнього на злочинний шлях.

Отож, підсумовуючи вище наведене, можна сказати, що виховання формує особистість, сприяє її розвитку, орієнтує на процеси, які не визріли, але перебувають у стадії становлення. Виховання вносить у долі людей різний внесок: від незначного до максимально можливого. Вихованням можна багато досягти, але повністю змінити людину не можна.

Список використаних джерел:

1. Максименко С. Д. Загальна психологія : навч. посіб. / С. Д. Максименко. – Вид. 2-ге, переробл. та доповн. – К. : Центр навч. л-ри, 2004. – С. 387–388.

2. Васильківська І. Сімейне виховання в Україні : шляхи вдосконалення в аспекті запобігання злочинності неповнолітніх // Право України. – 2000. – № 4. – С. 99–102.

3. Стан та структура злочинності в Україні [Електронний ресурс]. – Режим доступу до сайту: http://mvs.gov.ua.

4. Червоненко Г. О. Актуальні питання протидії злочинності неповнолітніх / Г. О. Червоненко // Протидія злочинності неповнолітніх: досвід та сучасні проблеми : матеріали Міжнар. наук.-практ. конф. (22–23 квіт. 2010 р.). – Кіровоград : Кіровогр. юрид. ін-т ХНУВС, 2010. – С. 214.

Отримано 05.11.2012

УДК 65.012.8+004

Володимир Володимирович ТУЛУПОВ
кандидат технічних наук, доцент,
начальник кафедри інформаційної безпеки факультету психології,
менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ
Павло Валентинович МАКАРЕНКО
кандидат психологічних наук, доцент,
заступник начальника з навчально-методичної роботи факультету
психології, менеджменту, соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ

ОСОБЛИВОСТІ ПІДГОТОВКИ ТА ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ ФАХІВЦІВ ПО БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ У ВНЗ МВС УКРАЇНИ

Розкрито окремі завдання підрозділів боротьби з кіберзлочинністю МВС України, проаналізовано досвід та особливості підготовки фахівців по боротьбі з кіберзлочинністю у ХНУВС, обґрунтовано доцільність підготовки відповідних фахівців для МВС України на базі напрямів «системи технічного захисту інформації» та «правознавство»

У Міністерстві внутрішніх справ України на постійному контролі перебуває питання щодо підготовки, підвищення кваліфікації та спеціалізації фахівців по боротьбі з кіберзлочинністю. Кіберзлочинність є одним з нових видів негативних соціальних явищ, яке на сьогодні кидає виклик національній безпеці України.

Аналіз криміногенної ситуації свідчить про складність виявлення та документування таких злочинів, високий професійний рівень осіб, задіяних у вчиненні правопорушень з використанням інформаційно-телекомунікаційних систем, різке збільшення частки світової індустрії кіберзлочинів, яка припадає на долю України, що викликає значне занепокоєння не лише в Україні, але й у інших державах світу.

Керівництвом МВС неодноразово наголошувалося, що без використання інноваційних технологій дуже скоро неможливо бути розкрити жодного серйозного злочину. Отже, перед суб'єктами боротьби з кіберзлочинністю постає проблема підготовки кваліфікованих кадрів, які здатні на належному рівні забезпечити правопорядок у сфері використання інформаційно-телекомунікаційних систем.

У системі МВС України основні функції щодо боротьби з кіберзлочинністю покладено на підрозділи боротьби з кіберзлочинністю у складі однойменного Управління. Згідно з Положенням про Управління боротьби з кіберзлочинністю Міністерства внутрішніх справ України, затвердженого наказом МВС України від 31.05.2012 № 494 [1], одними з функцій управління є:

1) відповідно до законодавства здійснення оперативних заходів щодо об'єктів сфери телекомунікацій та інтернет-послуг, банківських установ та платіжних систем з метою отримання інформації, яка сприятиме розкриттю злочинів, віднесених до компетенції територіальних підрозділів боротьби з кіберзлочинністю;

2) проведення спеціальних комп'ютерно-технічних досліджень та відновлення видалених і втрачених комп'ютерних даних відповідно до вимог законодавства та інших нормативно-правових актів.

Крім вищенаведених функцій, по яких, цілком очевидно, є бажаною технічна підготовка оперативного працівника, до функцій управління входить цілий ряд аналітичних завдань, що дає підстави говорити про необхідність підготовки для згаданих підрозділів системного аналітика з технічною освітою.

Позицію щодо необхідності укріплення підрозділів боротьби з кіберзлочинністю технічними спеціалістами підтримано також керівництвом Управління боротьби з кіберзлочинністю МВС України.

Підготовка означених фахівців у цивільних вишах викликає низку складнощів, основною з яких є те, що більшість відповідних методик та нормативних документів мають гриф обмеження доступу. Крім того, існує складний довготривалий процес атестації цивільного фахівця, початкової підготовки, надання йому допуску. Стартове матеріальне забезпечення оперативного працівника на сьогоднішній день також не надто привабливе для фахівця, який може (за матеріалами рекрутингових агентств) у цивільній компанії отримувати заробітну платню від 5 тис. грн. [2].

Для прикладу, в Російській Федерації відповідні кадри для Бюро технічних заходів МВС (куди входить і досить відоме Управління «К» – боротьби з кіберзлочинністю) комплектують з числа цивільних спеціалістів та випускників Московського університету МВС Росії, яких готують за спеціальністю «Інформаційна безпека» [3]. У 2012 році Президент Російської Федерації виступив з ініціативою значно розширити Управління «К» підрозділами, орієнтованими на розкриття дуже складних у технологічному плані злочинів, при цьому зауваживши, що підрозділ має комплектуватися лише

високопрофесійними кадрами, найсучаснішою технікою та забезпечуватися високим фінансуванням [4].

Підготовку кадрів для системи МВС України у галузі «інформаційна безпека» здійснює лише Харківський національний університет внутрішніх справ (ХНУВС). З 1998 року проводиться набір за відповідною спеціальністю (нині напрямом – системи технічного захисту інформації): випускаюча кафедра – «Інформаційної безпеки», наявна матеріально-технічна база та навчально-методичне забезпечення відповідає встановленим вимогам. Ряд розробок викладачів та курсантів за вказаним напрямом впроваджено у практичну діяльність ОВС України.

На сьогоднішній день випускники ХНУВС, що пройшли підготовку у галузі «інформаційна безпека», проходять службу у підрозділах боротьби з кіберзлочинністю, технічного захисту інформації, оперативно-технічних заходів, боротьби з організованою злочинністю, експертно-криміналістичних центрах, Державній службі охорони при МВС України, режимно-секретних органах тощо, де успішно використовують знання та навички, набуті під час навчання.

З метою забезпечення сучасних потреб слідчих та оперативних підрозділів фахівцями по боротьбі з кіберзлочинністю , університетом, з початку 2012/2013 навчального року здійснюється підготовка фахівців для вищевказаних підрозділів за освітньо-кваліфікаційним рівнем «бакалавр», напрямом підготовки «правознавство» спеціалізацією «боротьба з кіберзлочинністю».

Згідно плану-рознарядки підвищення кваліфікації та спеціалізації працівників ОВС у 2012 році проведено курси підвищення кваліфікації працівників НДЕКЦ МВС, ГУМВС, УМВС, які спеціалізуються на проведенні комп'ютерно-технічної експертизи та старших слідчих в особливо важливих справах, старших слідчих, слідчих СУ ГУМВС, УМВС, які закріплені за розслідуванням злочинів у сфері кіберзлочинності.

На виконання рішень керівництва МВС щодо можливості підготовки фахівців, проведення підвищення кваліфікації та спеціалізації фахівців по боротьбі з кіберзлочинністю з початку 2012 року університетом були впроваджені наступні заходи:

1. Розроблено проект Концепції створення і розвитку в ХНУВС факультету з підготовки фахівців для підрозділів, задіяних у боротьбі з кіберзлочинністю та інформаційної безпеки.

2. Розроблено Робочу навчальну програму підвищення кваліфікації оперативних працівників ОВС з питань протидії кіберзлочинності.

3. Проведено анкетування по вивченню професійної здатності курсантів 3 та 4 курсів щодо використання сучасних технологій у боротьбі з кіберзлочинністю. За результатами анкетування сформовано 4 групи спеціалізації «боротьба з кіберзлочинністю» у навчально-науковому інституті підготовки фахівців кримінальної міліції та на факультеті підготовки слідчих.

4. Проведено курси підвищення кваліфікації з працівниками Управління боротьби з кіберзлочинністю ГУМВС України в Харківській області.

5. Науково-педагогічні працівники кафедри взяли участь у підготовці таких наукових розробок:

– науково-методичних рекомендацій щодо документування наркозлочинів, що вчиняються з використанням комп'ютерних мереж;

– пропозицій до проекту закону України «Про внесення змін до Кримінального кодексу України (щодо посилення відповідальності за кіберзлочини)»;

– пропозицій щодо надання органам розслідування повноважень, необхідних і достатніх для ефективної боротьби з кіберзлочинністю (з метою їх внесення до Кримінального процесуального кодексу України);

– пропозицій до проекту Закону України «Про внесення змін до деяких законів України (щодо вдосконалення порядку надання телекомунікаційних послуг абонентам та отримання правоохоронними органами інформації про них)»;

– пропозицій до проекту Порядку використання підрозділами МВС України програмного забезпечення для провадження окремих слідчих дій та оперативно-розшукових.

6. Розроблено навчальні плани для підготовки слідчих та оперуповноважених працівників за спеціалізацією «боротьба з кіберзлочинністю», навчально-методичне забезпечення та проводяться поточні заняття з дисциплін спеціалізації «Оперативно-технічні засоби», «Попередження та розкриття кіберзлочинів», «Основи боротьби з кіберзлочинністю», «Основи обробки та передачі інформації», «Безпека інформаційних та комунікаційних систем», «Основи програмування та алгоритмічні мови», «Основи web-технології баз та банків даних».

7. Видано навчальний посібник «Використання комп'ютерних технологій в оперативно-розшуковій діяльності».

8. Підготовлено низку наукових статей, зокрема, «Про необхідність підготовки кадрів для підрозділів боротьби з кіберзлочинністю МВС України на базі напряму «системи технічного

захисту інформації»», «Procedure Analysis of the Special Investigative Actions Through Cyberspace in Countries of Common and Continental Law», «Використання програмного забезпечення для провадження окремих слідчих дій та оперативно-розшукових заходів», «Проблеми нормативно-правового забезпечення боротьби з кіберзлочинністю в Україні», «Аналіз нормативно-методичної урегульованості питання протидії несанкціонованому проникненню на об'єкти інформаційної діяльності», «Актуальні проблеми в підготовці фахівців з комп'ютерно-технічних експертиз».

9. На кафедрі інформаційної безпеки оновлено комп'ютерний парк спеціалізованого комп'ютерного полігону з інформаційної безпеки та навчальні стенди.

10. Складено розклад проведення лекційних та практичних занять науково-педагогічними працівниками Харківського національного університету внутрішніх справ з працівниками Управління боротьбі з кіберзлочинністю ГУМВС України в Харківській області.

11. На основі «Програми підготовки працівників експертної служби МВС України за експертною спеціальністю 10.9 «дослідження комп'ютерної техніки та програмних продуктів»», що була розроблена ДНДЕКЦ МВС України, було підготовлено навчальний план підвищення кваліфікації працівників НДЕКЦ МВС, ГУМВС, УМВС, які спеціалізуються на проведенні комп'ютерно-технічної експертизи.

Незважаючи на проведену роботу та досвід підготовки фахівців за спеціалізацією «Боротьба з кіберзлочинністю» для досягнення мети вважається необхідним вирешення наступних завдань:

1) з метою закріплення теоретичних знань слід активніше залучати курсантів до практики в УБК та СУ ГУМВС в Харківській області, яку проводити шляхом направлення один день на тиждень по два курсанти відповідно до спеціалізації із розробленням карток контролю проходження такого виду практики та графіків виходу в практичні підрозділи, результатом якої є зібрання зразків процесуальних та службових документів, а за слідчою спеціальністю – макет кримінальної справи;

2) забезпечити проходження стажування в кінці курсу навчання саме на посадах за спеціалізаціями що передбачають протидію кіберзлочинності з обов'язковим контролем за направленням на такі посади з боку УБК та ГСУ Міністерства;

3) враховуючи положення Кримінального процесуального кодексу України, щодо створення у всіх практичних підрозділах відеозв'язку – облаштування навчальних аудиторій таким зв'язком для

проведення занять з практичними працівниками без виїзду до навчального закладу;

4) на базі існуючого в ХНУВС спеціалізованого комп'ютерного полігону з інформаційної безпеки розробити закриту систему (навчальний кіберпростір) в якому курсанти можуть навчатися вистежувати осіб, які вчиняють злочини, встановлення їх місцезнаходження, проводити документування та фіксацію обставин вчинення злочину.

Підсумовуючи слід наголосити, що в умовах глибокого латентного проникнення кіберзлочинності у суспільне та державне життя організація такої підготовки є складним завданням, виконанню якого сприятиме створення консолідованими зусиллями системи цільової підготовки та перепідготовки фахівців у сфері протидії кіберзлочинності.

Список використаних джерел:

1. Положення про Управління боротьби з кіберзлочинністю Міністерства внутрішніх справ України [Електронний ресурс] : затв. наказом МВС України від 31.05.2012 № 494 / Ліга: Закон Еліт : Мережна версія.

2. Манжай О. В. Про необхідність підготовки кадрів для підрозділів боротьби з кіберзлочинністю МВС України на базі напряму «Системи технічного захисту інформації» / О. В. Манжай, В. В. Тулупов // Актуальні проблеми забезпечення практичної спрямованості підготовки кадрів для органів внутрішніх справ України : матеріали наук.-практ. конф. (м. Харків, 5 трав. 2012 р.) / МВС України, Харк. нац. ун-т внутр. справ. –Х. : ХНУВС, 2012. – С. 74–78.

3. Невидимый, но зоркий глаз милиции [Електронний ресурс]. – Режим доступу: http://www.simech.ru/index.php?id=445.

4. МВД создаст новые IT подразделения [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/420008.php.

Отримано 01.11.2012

УДК 343.9

Дмитро Юрійович УЗЛОВ
начальник Управління інформаційно-аналітичного забезпечення
ГУМВС України в Харківській області

ВИКОРИСТАННЯ ПОВЕДІНКОВОГО ПРОФІЛЮ ДЛЯ ВИЯВЛЕННЯ ОЗНАК КІБЕРЗЛОЧИННОСТІ

Розглянуто ознаки кіберзлочинності та принципи побудови поведінкового профілю скорингових систем щодо їх виявлення.

пристрої, програми які забезпечують їх
йним середовищем, призначеним для
і життєдіяльності людини, організацій, держави, суспільства. Всі функції регулюються відповідними нормами права, а інформаційні системи та пристрої - правилами експлуатації.

Сукупність інформаційних систем, пристроїв, програмного забезпечення довкола функцій життєдіяльності людини (суспільства) можна вважати кіберпростором. Неправомірна поведінка в кіберпросторі, яка спричинила настання негативних наслідків для людини (суспільства) є кіберзлочинністю. Кіберскладова у складі злочинного діяння за своєю суттю є інструментом і відноситься до об'єктивної сторони його складу.

1. Типи кіберзлочинності.

1.1. За направленістю.

Протиправні дії в кіберпросторі спрямовані на зміни нормального функціонування пристроїв і інформаційних систем по цілі злочинного наміру можна поділити на наступні види:

– спрямовані проти особистості;

– спрямовані проти організацій і установ комерційного та некомерційного типу усіх форм власності;

– спрямовані проти державних установ і безпосередньо управлінських функцій держави.

1.2. За механізмом здійснення.

1.2.1. Не спрямовані безпосередньо на інформаційні системи і пристрої, але використовують їх для здійснення протиправних дій у всіх сферах життєдіяльності. До таких видів можна віднести: фінансові крадіжки; поширення порнографії; нелегальний продаж; азартні ігри; порушення прав інтелектуальної власності; підміна електронної адреси; підробка державних цінних паперів; поширення наклепу; кіберпереслідування.

1.2.2. Спрямовані безпосередньо на інформаційні системи та пристрої (комп'ютери, локальні мережі, сховища та інше). Дані протиправні дії в міжнародній класифікації визначаються як Хакінг (HACKING). До них відносяться: крадіжка інформації в електронній формі; атака на поштовий сервіс (E-mail bombing); підміна даних (Data diddling); приховані комісії (Salami attacks); DDoS-атака, руйнування ресурсів (Distributed Denial of Service); поширення вірусів; логічні бомби (Logic bomb); троянська програма (Trojan Horse); Крадіжка інтернет трафіку (Internet Time Theft); Фізичне руйнування комп'ютерних систем (Physically damaging a computer system).

2. Методи виявлення. Використання технологій Data Mining і Text Minig.

Негативні наслідки шкідливих діянь, розглянутих вище, можуть проявлятися відразу, або через деякий час, або явно не проявлятися. Фінансові крадіжки необхідно виявляти на ранніх етапах скоєння, а не після зникнення великих сум і нанесення істотного збитку. Відновлювати зруйновані DDoS-атакою ресурси важко, а втрата управління ресурсами може мати тяжкі наслідки. Універсального засобу, який дозволить виявляти кіберзлочині прояви на етапі підготовки або на ранній стадії реалізації не існує, вважаючи велику різноманітність діянь. Однак, ряд кіберзлочинів можна виявляти за допомогою технологій Data mining і Text mining.

Можливість використання технології Data Mining випливає з наступного твердження: нормальне функціонування будь-якої інформаційної системи регламентується суворо певною моделлю поведінки – виконанням певних операцій по заздалегідь закладеному авторському алгоритмом. В результаті функціонування будь-якої системи виробляється її поведінковий профіль - зовнішнє відображення результатів роботи у вигляді наборів даних що мають закономірний розподіл, відповідний авторському алгоритму.

Технологія Data Mining дозволяє нам створити поведінковий профіль будь-якої інформаційної системи.

Розглянемо створення поведінкового профілю на основі системи функціонування електронних платіжних карток. Електронні платіжні картки є частиною системи електронних платежів. В результаті функціонування платіжної системи виробляються наступні масиви даних:

– множина користувачів системи: власники карток, торгові компанії, банківські термінали та інші заклади, які приймають картки як засіб платежу;

– множина даних отримуваних в результаті використання карток: транзакції по платежах;

– множина точок підключення до системи – фізичне місцезнаходження терміналу, час роботи, інше.

Кожен користувач з моменту підключення до системи, отримання картки та нарахування коштів на неї починає здійснювати певні дії – користуватися карткою як засобом платежу. При цьому всі транзакції фіксуються та з'являється динамічний ряд даних на часовій шкалі тих чи інших транзакцій. Аналіз транзакцій дозволяє виявляти приховані закономірності користувача – його поведінковий профіль. Наприклад: нарахування заробітної плати здійснюється у певний день місяця і заноситься на картки (у разі зарплатної картки), далі користувач на протязі певного часу знімає частину грошей у певних терміналах (сама частина і місця знімання вже формують поведінковий профіль). Користувач, як правило, розраховується за товари та послуги з певною систематичністю і в певних місцях. В даному випадку авторське правило використання користувачем своєї картки – буде його індивідуальним поведінковим профілем. Чим більше буде проміжок часу користування карткою – тим точніше буде профіль.

Безумовно можливі відхилення (девіації) від звичайної поведінки – наприклад поїздки у відпустку, відрядження тощо. Однак, при значно тривалим проміжку часу і девіаційної відхилення можуть утворювати свій певний профіль поведінки, характерний для певних обставин: відпустка, відрядження та інше.

Також може бути сформований поведінковий профіль самої платіжної системи, який буде характеризуватися: кількістю користувачів, розподілом навантаження на систему за зверненням за певний часовий тренд, концентрація користувачів за певними терміналам, кількість операцій за видами, залежність від часу доби, року та інше.

Таким чином, можна говорити про побудову системи поведінкового скорингу (behaviour scoring) для платіжної системи кредитних карток.

Поведінковий скоринг для кредитних карт (behaviour scoring for credit card) – динамічна система оцінки легітимності використання кредитної картки (транзакції) заснована на історії транзакцій по картковому рахунку.

Для побудови скорингової моделі за основу береться логіко-імовірнісний підхід. В якості параметрів моделі будуть виступати імовірність настання не легітимною транзакції на основі

ретроспективного аналізу попередніх транзакцій і побудови поведінкової функції легітимних транзакцій.

Використання даної моделі можливо для виявлення ознак практично для всіх видів кіберзлочинів, розглянутих у першій частині цієї роботи.

Отримано 10.11.2012

—

УДК 351.74:57.087.1

Дмитро Юрійович УЗЛОВ
начальник Управління інформаційно-аналітичного забезпечення ГУМВС України в Харківській області

МОДЕЛЬ МЕТАПОШУКОВОЇ МАШИНИ ДЛЯ ДОБУВАННЯ КРИМІНАЛЬНО ЗНАЧУЩИХ ДАНИХ З НЕСТРУКТУРОВАНИХ МАСИВІВ ТА ЇХ ІНТЕГРАЦІЯ В БАЗИ ДАНИХ ОВС

Представлено модель метапошукової машини, яка дозволяє проводити пошук і структурування кримінально значущої інформації з різних текстових масивів, у тому числі з мережі Internet. Може також використовуватися як локальна пошукова машина на будь-яких відкритих і закритих ресурсах за наявності технічної можливості індексації великих масивів даних.

Масиви даних, що формуються в процесі оперативно-службової діяльності органів внутрішніх справ, складаються як з фактографічних баз даних структурованої інформації, так і неструктурованих текстів. У пропонованій системі витяг кримінально значимих даних з неструктурованих масивів відбувається за спеціальною методикою на основі використання даних існуючих фактографічних систем. При цьому не передбачається зміна структур баз даних, зміна існуючого програмного забезпечення. Система вилучення припускає автономну роботу з будь-якими ресурсами, до яких буде доступ. Методика реалізована в лінгвістичному процесорі [2], який виділяє метадані з вже існуючих масивів, формує нові, додає відсутні або коригує існуючі.

Формування метаданих здійснюється за трьома основними напрямками: особа, об'єкт, подія. Дані напрями містять повний обсяг інформації, достатній для ідентифікації складу злочину. У всіх випадках використовуються структуровані дані, наявні в СУБД, ранжирування за сукупністю деякого набору критеріїв (актуальність, зустрічальність, важливість, зв'язаність і т.д.), і проіндексовані документи, пов'язані з ними. Аналіз взаємозв'язків особи, об'єкта і події здійснюється методами LSA і статистичної обробки. На рис.1 представлена схема метапошукової машини, яка використовує як базу знань існуючу фактографічну СУБД (кілька СУБД) з інтегрованою в неї базою текстів та URL Server, що містить URL адреси, за якими здійснюється пошук.

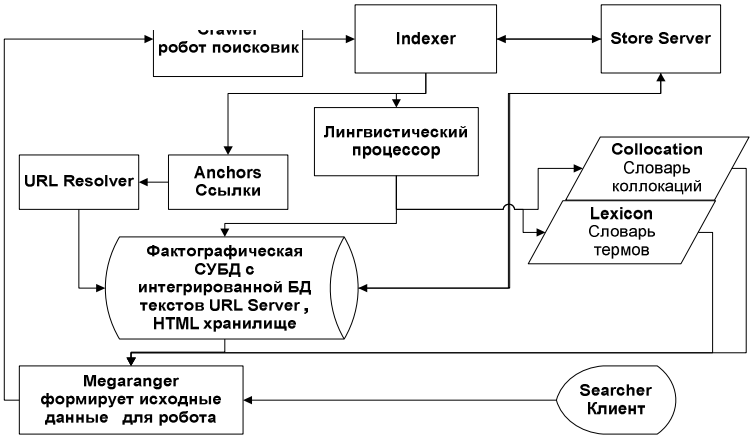

Рис. 1. Структура метапошукової машини

Особливість даної пошукової машини полягає в тому, що вона використовує можливості зовнішніх пошукових систем, отже, позбавлена необхідності у використанні потужних обчислювальних ресурсів для індексування величезного числа WEB ресурсів (XML, HTML сторінок). У пропонованому варіанті модуль Crawler формує пошукові запити для існуючих пошукових машин (Google, Яндекс, Meta, Rambler і ін). Отриманий масив результатів розбирається в модулі Indexer на окремі сторінки і виділяються вагомі теги, що

містять основний текст, URL адреси і посилання на інші сторінки. При цьому не обробляються сторінки, що містяться в чорному списку, дані про які зберігаються на URL Server і аналізуються в модулі Store Server. Подальше семантичне розбирання отриманих текстів здійснюється в лінгвістичному процесорі з використанням методів статистичної обробки і логічного висновку. Результатом роботи процесора є:

– класифіковані за рубриками тексти, які прив'язані до даних (особа, об'єкт, подія) з фактографічної СУБД;

– безліч нових термів – слова з вектором ознак, які поміщаються у відповідний словник Lexicon;

– безліч виявлених колокацій – пов'язаних семантично слів (2-х і більше), які поміщаються в словник колокацій Collocation.

Другою особливістю є модуль Mega ranger. Він виконує функцію ранжирування інформації, що зберігається в Базі Даних за деякими критеріями (актуальність, важливість, повнота) і побудови пошукових запитів пошукачеві Crawler у фоновому (автоматичному) режимі або видачі для аналізу користувачеві Searcher в ручному режимі. Mega ranger в даній пошуковій системі частково виконує ту ж функцію, що і Page rank в системі Google, але використовує інші принципи. Mega ranger має набір логічних правил, побудованих на основі онтологічної моделі формування запитів, які дозволяють йому самостійно робити зважування наявної в базі знань інформації та формувати запити, витягуючи необхідні дані та метадані з баз даних і словників.

Список використаних джерел:

1. Особливості виділення кримінально значимої інформації в текстових масивах / О. М. Бандурка, М. М. Зацеркляний, Д. В. Лазарєв, Д. Ю. Узлов // Наше право. – 2011. – № 2, ч. 1.– С. 79–83.

2. Зацеркляний Н. М. Лингвистический процессор для поиска и обработки криминально значимой информации в неструктурированных массивах / Н. М. Зацеркляний, Д. Ю. Узлов // Вестник НТУ «ХПИ». Тематический выпуск: Информатика и моделирование. – № 36. – 2011. – С. 87–94.

Отримано 21.11.2012

УДК 004.75:[004.65:004.89]

Валентин Олександрович ФІЛАТОВ
доктор технічних наук, професор,
професор кафедри штучного інтелекту
Харківського національного університету радіоелектроніки
Зоя Леонідівна КОСТІНА
аспірант Харківського національного університету радіоелектроніки

МУЛЬТИАГЕНТНИЙ ПІДХІД ДО ВИДОБУВАННЯ ЗНАНЬ В РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Розглянуто питання використання мультиагентних систем в задачах оперативної підтримки прийняття рішень. Запопоновано використовувати технологію згортки графа рішень до дерева, що дозволяє скоротити час реакції на запит.

Інформаційно-аналітична робота при розслідуванні злочинів – це збирання, зберігання, систематизація та аналіз доказової інформації з метою прийняття оптимальних кримінально-правових, кримінально-процесуальних і тактичних рішень, а також в цілях забезпечення діяльності взаємодіючих експертних підрозділів й органів дізнання.

Актуальність використання в процесі розкриття і розслідування методів інформаційно-аналітичної роботи визначається процесом інтенсивного впровадження в діяльність правоохоронних органів засобів обчислювальної техніки, що різко підвищує ефективність розслідування.

Застосування засобів обчислювальної техніки, найчастіше використовує методи штучного інтелекту, заснованих на моделюванні різних типів слідчих ситуацій з використанням багатоагентних (або мультиагентних) систем.

Архітектури таких систем штучно інтелекту, можуть бути найрізноманітнішими. Для реалізації подібних систем розробляються спеціальні інструментальні програмні засоби. Ці засоби передбачають певну технологію створення мультиагентних систем. Подібна технологія включає ряд етапів, типовими з яких є наступні [1]:

– вибір архітектури мультиагентної системи;

– вивчення властивостей і поведінки середовища і подання знань у вигляді неформальної онтології;

– представлення глобальних і локальних знань на формальній мові;

– вибір стратегії виведення для кожного з агентів;

– розробка програмних засобів для реалізації мультиагентної системи.

Архітектура мультиагентної системи показана на рис. 1. Агент отримує повідомлення від системи збору інформації, при цьому завданням агента є аналіз різних ситуацій та на основі цих повідомлень пропонувати оператору результат цього аналізу.

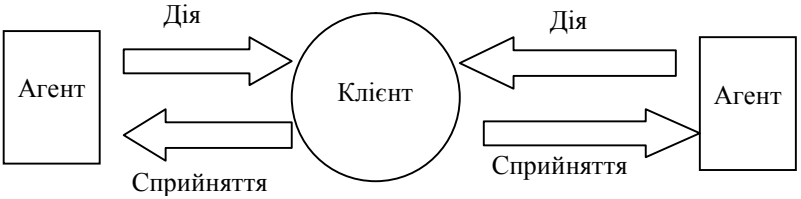

Рис. 1. Архітектура системи з двома агентами

Одна з проблем, пов'язаних з отриманням знань полягає в неточності, приблизності, а іноді і помилковості знань, що добуваються. Інша проблема, пов'язана з процесом добування знань, складається в суб'єктивності аналітика.

На жаль, перераховані проблеми не дозволені повністю, оскільки процес вилучення знань сильно залежить від специфічних особливостей середовища.

Будемо вважати, що дані формується на природної мові, а формалізацію результатів представляє у вигляді схем ситуацій. Схемою ситуацій називатиме орієнтований граф з трьома типами вершин: ситуації, сприйняття, реакції. Вершини останнього типу дозволяють утворювати деяку ієрархію схем і розбивати процес вилучення знань по частинам [2].

Будь шлях, що веде від вершини ситуації S_i через вершину виразом (*а дія* (*d*)) в вершину з дією *d* до вершини ситуації S_j, представляється складовим виразом (*ситуація Si* $\wedge$ *а* $\supset$ *дія* (*d*), *f*(*перехід* (*d*, S_i)) = *ситуація* S_j), де *f* – функція переходу.

Таким чином, схема ситуацій є деякою формою представлення формул. Тут схема ситуацій використовується для витягання знань шляхом поступового її побудови в процесі аналізу предметної області, починаючи від початкової вершини. Вилучення знань в цьому випадку полягає в отриманні відповідей на питання і побудові за результатами відповіді відповідної схеми ситуацій.

З іншого боку схема ситуацій може бути дуже великою і надлишкової, схем може бути декілька. глубіна схеми може залежати від початкової ситуації, з якої починається процес її побудови. Число вершин і дуг схеми характеризує складність процесу видобування знань. Але ця складність може бути зменшена об'єднанням вершин, для яких всі можливі шляхи однакові, таким чином можливо перейти від дерева до графу.

Очевидно, що ця стратегія є стратегією прямого виводу в ширину на основі узагальнено правила Modus Ponens з наступними відмінностями: частина значень змінних беруться з сприйняття агента, а не є аксіомами, які формуються заздалегідь; процес виведення може бути нескінченним.

Такий напрям визначено тим, що в даний час вже з'явився сучасний інструментарій і технології, що використовують мови логічних числень для розробки мультиагентних систем. Розглянутий матеріал є введенням у теоретичну основу таких технологій в діяльність правоохоронних органів.

Список використаних джерел:

1. Филатов В. А. Мультиагентный подход к интеграции и управлению информацией в гетерогенных вычислительных средах / В. А. Филатов // Искусственный интеллект. – 2004. – № 4. – С. 748–755.

2. Девятков В. В. Системы искусственного интеллекта / В.В. Девятков. – М. : Изд-во МГУ им. Н. Э. Баумана, 2001. – 352 с.

Отримано 07.11.2012

УДК 004.75

Лариса Ернестівна ЧАЛА
кандидат технічних наук, старший науковий співробітник,
доцент кафедри штучного інтелекту
Харківського національного університету радіоелектроніки
Сергій Григорович УДОВЕНКО
доктор технічних наук, професор,
професор кафедри електронних обчислювальних машин
Харківського національного університету радіоелектроніки

МУЛЬТИАГЕНТНА МОДЕЛЬ БІОМЕТРИЧНОГО КОНТРОЛЯ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ КОМП'ЮТЕРНИХ СИСТЕМ

Запропоновано модель біометричної ідентифікації користувачів розподілених інформаційних систем на основі агентних технологій. Розроблено рекомендації до застосування цієї моделі в системах з обмеженим доступом до інформаційних ресурсів.

Перспективним напрямком забезпечення обмеженого доступу до деяких інформаційних ресурсів є розробка і впровадження методів біометричної ідентифікації користувачів розподілених інформаційних систем (РІС) на основі множини факторів, характерних для об'єкта ідентифікації (користувача РІС). До цих факторів слід віднести використання характерних дій при вирішенні деяких задач у програмних оболонках, а також часові характеристики та послідовності виконання цих дій. Використання такого підходу дозволяє вирішувати цілий ряд важливих практичних задач, характерних для експлуатації РІС різного призначення, зокрема: обмеження доступу до певних інформаційних ресурсів для деяких класів користувачів; моніторинг звертання користувачів до різних типів ресурсів РІС. При ідентифікації індивідуального клавіатурного почерку користувача РІС його первинний образ формується на основі індивідуальних параметрів-характеристик: часу утримання кожної клавіші, часу між натисканнями клавіше), швидкості набору, ритмічності тощо. Важливим напрямком формування біометричного профілю є використання поряд з параметрами клавіатурного почерку і стилю роботи, що є характерним для користувача РІС. Формалізовану модель поведінки n-го користувача під час сеансу роботи можна представити таким кортежем:

$$B_n = < U_n, t_0, t_1, S_l, \{d_j\}, \{a_{ij}\}, \{x_m^k\} >, \quad (1)$$

де U_n – ідентифікатор n-го користувача; t_0, t_1 – час початку та завершення сеансу роботи; S_l, $l = \overline{1, L}$ – програмні оболонки; $\{d_j\}$, $j = \overline{1, J}$ – множина вирішуваних задач; $\{a_{ij}\}$, $i = \overline{1, I}$ – сукупність атомарних дій, необхідних для вирішення j-ї задачі; $\{x_m^k\}$, $m = \overline{1, M}$ – сукупність значень біометричних параметрів, що визначають клавіатурний почерк n-го користувача.

Біометричний профіль користувача за клавіатурним почерком формується на основі математичних очікувань та дисперсій параметрів, що контролюються. Динамічна ідентифікація користувачів за стилем роботи є єдино можливим методом у разі, якщо користувач під час поточного сеансу не використовує клавіатуру. Для практичної реалізації задачі ідентифікації користувачів запропоновано модель ідентифікації користувачів РІС на основі дворівневої мультиагентної системи, що складається з агентів-моніторів та агента-менеджера. Запропоновані методи формування та корекції баз біометричних еталонів, динамічної ідентифікації та моніторингу дій користувачів РІС реалізовано за допомогою програмних агентів «Etalon», «Idenus» та «Monit». Програмний агент «Etalon» реалізує функції формування та корекції баз біометричних еталонів користувачів, а також для виділення компактних класів користувачів. Програмний агент «Idenus» реалізує поточну ідентифікацію користувачів за клавіатурним почерком і стилем роботи. Програмний агент «Monit» виконує моніторинг дій користувачів під час поточного сеансу. Під час аутентифікації користувача формується його біометричний профіль, який порівнюється з відповідним еталоном, що зберігається агентом-менеджером. Потім згідно з матрицею повноважень визначаються ім'я користувача, можливість доступу, дані для журналу-протоколу. В разі негативного результату аутентифікації або відсутності ідентифікатора здійснюється процес ідентифікації користувача, що увійшов до системи. При цьому біометричний профіль порівнюється з усіма еталонами бази згідно з методом біометричної ідентифікації. Моделі програмних агентів запропонованої дворівневої мультиагентної системи ідентифікації подано як фреймову структуру такого вигляду:

$$FR = [(R_1, A_1), (R_2, A_2), ..., (R_n, A_n)], \quad (2)$$

де FR – ім'я фрейма; R – ім'я слота; A – значення слота.

На підставі концептуальної моделі (2) формується сукупність значень слотів: <об'єкт>, <умова>, <дія>, <пріоритет>. Кожен слот

містить чотири атрибути базових типів та реалізує процеси моніторингу дій користувача, формування бази еталонів, поточної ідентифікації користувача.

Результати тестування мультиагентної моделі свідчать про працездатність запропонованих процедур формування баз біометричних образів за поведінковими характеристиками та прийняття рішень щодо ідентичності поточного профілю користувача і елементів цих баз. Значення помилок ідентифікації за клавіатурним почерком і стилем роботи для різних класів користувачів знаходяться в діапазоні 0,04–0,18. Наведену модель може бути застосовано для попередження та виявлення правопорушень, що є пов'язаними з несанкціонованим доступом до деяких інформаційних ресурсів комп'ютерних систем.

Отримано 05.11.2012

УДК 343.983

Володимир Олександрович ЧЕРКОВ
кандидат юридичних наук, доцент,
начальник факультету кримінальної міліції
Луганського державного університету внутрішніх справ імені
Е. О. Дідоренка

ПРО НАПРЯМИ НОРМАТИВНО-ПРАВОВОГО ВРЕГУЛЮВАННЯ ЗАСТОСУВАННЯ ПОЛІГРАФА У ПРОТИДІЇ ЗЛОЧИННОСТІ

Розглянуто питання щодо напрямів нормативно-правового врегулювання застосування поліграфа в оперативно-розшуковій та слідчій практиці органів внутрішніх справ України.

Однією з основних умов розбудови правової держави в Україні, для якої людина, її життя і здоров'я, честь і гідність, недоторканність і безпека є найвищою соціальною цінністю, ми вбачаємо гарантування забезпечення конституційних прав і свобод людини. Нажаль, цей процес в нашій державі супроводжується досить високим рівнем злочинності, що розповсюджується серед усіх верств населення, стає більш організованою, оснащеною новітніми технічними засобами,

іншими матеріальними ресурсами тощо. У зв'язку з цим правоохоронні органи, що створені для протидії такому негативному соціальному явищу як злочинність, повинні постійно вдосконалювати форми, методи, засоби подолання її росту та, відповідно, спрямовувати свої зусилля на зниження кількості вчинених нерозкритих злочинів, поновлення порушених конституційних прав і свобод людини, встановлення й притягнення до кримінальної відповідальності винних осіб тощо.

На наш погляд, сьогодні одним із перспективних новітніх засобів отримання й перевірки інформації, що становить оперативний інтерес під час виявлення, розкриття та розслідування злочинів, є використання поліграфа. Сучасний поліграф є різновидом психофізіологічної апаратури і представляє собою комплексну багатоканальну комп'ютерну апаратну методику реєстрації змін психофізіологічних реакцій людини у відповідь на пред'явлення за спеціальною методикою певних психологічних стимулів [1]. В свою чергу, використання поліграфа здійснюється шляхом проведення за спеціальною методикою опитування людини з одночасною реєстрацією змін її психофізіологічних реакцій у відповідь на психологічні стимули, що задаються у вигляді варіантів відповідей, предметів, схем, фото та ін. У процесі такого інтерв'ю використовуються поліграфні пристрої, що не завдають шкоди здоров'ю, життю людини, навколишньому середовищу та мають відповідні сертифікати.

Не дивлячись на те, що використання можливостей поліграфа в практиці правоохоронних органів України, особливо їх оперативних підрозділів, має досить широке розповсюдження, сьогодні в нашій державі, нажаль, відсутнє спеціальне нормативно-правове регулювання такої діяльності.

Якщо звернутися до світового досвіду застосування поліграфа при виявленні, розкритті й розслідуванні злочинів, то його можливості використовуються в таких країнах, як Бельгія, Білорусь, Великобританія, Естонія, Індія, Іспанія, Канада, Китай, Польща, Росія, Туреччина, Фінляндія та інших. Крим цього є такі країни, де поліграф застосовується для відбору персоналу або проведення службових розслідувань у правоохоронних органах або в приватному секторі.

У цьому контексті звернемо увагу на нормативно-правове регулювання застосування поліграфу в інших країнах світу, які за цим критерієм умовно можна розділити на чотири основні групи:

– країни, в яких застосування поліграфа при розкритті та розслідуванні злочинів урегульоване окремими законами (Литва,

Закон «Про використання поліграфу» 2000 року; Молдова, Закон «Про застосування тестування на детекторі симуляції (поліграфі)» 2009 року – у цих законах згадується можливість застосування поліграфу під час реалізації завдань оперативно-розшукової діяльності);

– країни, в яких застосування поліграфа при розкритті та розслідуванні злочинів урегульоване окремими правовими нормами законів, що регламентують більш широке коло суспільних відносин (Польща, параграф 2 ст. 192 Кримінально-процесуального кодексу (1997 року) дозволяє експертам застосовувати технічні засоби контролю мимовільних реакцій особи; Угорщина, ст. 180, 182^2, 435 Кримінально-процесуального кодексу (1998 року) передбачено можливість застосування поліграфу в кримінальному процесі; Словенія, п. 6 ст. 54 Закону «Про поліцію» 1994 року передбачено можливість застосування поліграфа для отримання інформації при розкритті та розслідуванні злочинів);

– країни, в яких застосування поліграфа при розкритті та розслідуванні злочинів урегульоване підзаконними нормативно-правовими актами (Росія, наказ МВС від 28.12.1994 № 437 «Про затвердження Інструкції про порядок використання поліграфа при опитуванні громадян», наказ МВС від 12.09.1995 № 353 «Про забезпечення впровадження поліграфа в діяльність органів внутрішніх справ»; Білорусь, постанова МВС від 31.10.2001 № 206 «Про затвердження Інструкції про порядок проведення органами внутрішніх справ Республіки Білорусь опитування громадян з використанням поліграфу», наказ МВС від 16.04.2004 № 87 «Про забезпечення впровадження поліграфа в діяльність органів внутрішніх справ»);

– країни, в яких застосування поліграфа при розкритті та розслідуванні злочинів нормативно не врегульовано (Японія, Казахстан, Сінгапур, Латвія – поліграф може застосовуватися в загальному порядку, встановленому для проведення оперативно-розшукових заходів та слідчих дій, а також застосування технічних засобів).

Таким чином, як ми бачимо, найбільш поширеним способом правового врегулювання застосування поліграфу в протидії злочинності в інших країнах є прийняття відповідного підзаконного нормативно-правового акту, а також передбачення застосування поліграфа окремими нормами відповідних законів. Узагальнюючи світовий досвід застосування поліграфу, та враховуючи погляди практикуючих поліграфологів, вважаємо за доцільне закріпити правові підстави використання поліграфа в протидії злочинності шляхом внесення відповідних доповнень до Кримінального процесуального

кодексу України та Закону України «Про оперативно-розшукову діяльність», а також, на основі цих доповнень, розробити відповідну Інструкцію щодо застосування поліграфа в оперативно-розшуковій та слідчій практиці органів внутрішніх справ України.

Список використаних джерел:

1. Інструкція щодо застосування комп'ютерних поліграфів у роботі з персоналом органів внутрішніх справ України : затв. наказом МВС від 28.07.2004 № 842.

Отримано 05.11.2012

УДК 004.932.2:681.3.06

Юрій Якович ЧІЖЕНКОВ
викладач кафедри електронних обчислювальних машин
Харківського національного університету радіоелектроніки
Олександр Іванович БИРКА
студент Харківського національного університету радіоелектроніки

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ НА ОСНОВІ ВЕЛИКОМАСШТАБНИХ БАЗ ДАНИХ

Розглянуто основні передумови широкого використання інформаційних технологій в діяльності органів внутрішніх справ. Визначено основні напрямки розвитку інформаційних технологій, зокрема системи прийняття рішень в структурах правоохоронної діяльності. Запропоновано підхід до вирішення задачі прийняття рішень з використанням великомасштабних баз даних.

Однієї з головних особливостей діяльності органів внутрішніх справ, є програмно-технічна потужність інформаційних і комунікаційних технологій. Відбувається перехід до інформаційного простору, що має гігантський потенціал. У такій складній структурі якої є сучасне суспільство, без інформаційних технологій (ІТ) попросту неможливо налагодити ефективну взаємодію між численними владними структурами, не можна належним чином підвищити ефективність і якість вироблення й прийняття рішень, знизити ймовірність прояву управлінських помилок.

Освоєння можливостей сучасних ІТ пов'язане з освоєнням нових практичних прийомів, методів і засобів, що розширюють межі можливостей користувачів ІТ. Однієї з причин неефективності підготовки й прийняття рішень – недостатнє методичне забезпечення, розробка, впровадження й використання ІТ в органах внутрішніх справ, починаючи з постановки задачі підтримки аналітичної діяльності, до застосування математичних методів і засобів інформаційно-аналітичній підтримці управлінських рішень.

У тім або іншому ступені системи підтримки прийняття рішень (СППР) присутні в будь-якій ІТ. Одним з підходів до створення таких систем стало використання великомасштабних баз даних (БД). СППР можна, залежно від даних, с якими вони працюють, розділити на оперативні, призначені для негайного реагування на поточну ситуацію, і стратегічні – засновані на аналізі великої кількості інформації з різних джерел.

СППР першого типу називаються інформаційні системи керівництва (ІСК). По суті, вони являють собою кінцеві набори звітів, побудовані на підставі даних з інформаційної системи організації. СППР другого типу припускають досить глибоке пророблення даних, спеціально перетворених так, щоб їх було зручно використовувати в ході процесу прийняття рішень. Такого роду системи створюються тільки в тому випадку, якщо є підстави для узагальнення та аналізу не тільки даних, але й процесів їхньої обробки.

Чим більше інформації бере участь у процес прийняття рішень, тим більше обгрунтоване рішення може бути прийнято. Інформація, на основі якої приймається рішення, повинна бути достовірної, повної, несуперечливої та адекватної. Тому при проектуванні СППР виникає питання про те, на основі яких даних ці системи будуть працювати. В ІСК якість оперативних рішень забезпечується тим, що дані вибираються безпосередньо із БД організації, що повинна адекватно відбиває стан справ на даний момент часу.

У найпростішому варіанті для БД використовується та модель даних, що лежить в основі транзакційної системи. Якщо, як це часто буває, така система функціонує на базі реляційної системи керування базою даних (СКБД), то самою складною задачею стає виконання запитів, оскільки неможливо заздалегідь оптимізувати структуру БД.

Основною функцією оптимізації запиту є вироблення плану виконання запиту, тобто вибір порядку виконання з'єднання відношень, що перебувають у різних вузлах комп'ютерної мережі, а також способу виконання з'єднання цих відношень. При цьому в оцінних формулах з'являється новий компонент – оцінка мережевих

накладних витрат, що виникають при виконанні запиту, що є складним і включає число повідомлень, які приблизно будуть передаватися в мережі, і сумарне число байтів, які ці повідомлення будуть містити [1].

При традиційній організації структур зберігання й керування структурою реляційною базою даних найбільше ефективно виконуються операції, що відповідають обмеженню й проекції одного збереженого відношення. Двумістні операції – об'єднання, перетинання, з'єднання відносин спеціально не підтримуються структурами даних і операціями нижнього рівня.

Для ефективного використання таких операцій використовується алгоритм, що використовує попереднє сортування відношень у відповідності зі значеннями атрибутів з'єднання. Після цього з'єднання виконується з використанням процедури злиття, застосовувану в алгоритмах зовнішнього сортування файлів. Якщо відношення проіндексоване по полях з'єднання, то вихідне сортування цього відношення не потрібно, для цього в циклі злиття використовуються сканування відношення по цьому індексі.

У розглянутому методі впроваджені засоби, що дозволяють кількісно оцінити ефекти, досягнуті в ході оптимізації запиту, і зрівняти їх з можливими альтернативними варіантами. При такому підході операції обмеження й з'єднання виконуються над частковими відношеннями, а значення інших атрибутів вибираються при формуванні остаточного результату по наявних посиланнях. Слід також зазначити, що в ряді випадків, обумовлених ступенем селективності предикатів обмеження, алгоритми з'єднання на основі часткових відношень виявляються ефективніше традиційних.

Список використаних джерел:

1. Чаудхари С. Методы оптимизации запросов в реляционных системах / С. Чаудхари // Системы управления базами даннях. – 1998. – № 3. – С. 22.

Отримано 19.11.2012

УДК 343.97

Світлана Валентинівна ЯКИМОВА
кандидат юридичних наук, доцент,
доцент кафедри кримінального права та кримінології
Львівського державного університету внутрішніх справ

КРИМІНОЛОГІЧНА ЕКСПЕРТИЗА ЯК ІННОВАЦІЙНИЙ ЗАСІБ ПОПЕРЕДЖЕННЯ ЗЛОЧИННОСТІ

Розглянуто доцільність розроблення нормативно-правового та організаційного забезпечення кримінологічної експертизи, доведена важливість кримінологічної експертизи для подальшого розвитку можливостей загальносоціального попередження злочинності.

Термін «інновація» вперше було досліджено австрійським економістом Й. Шумпетером як «непостійний процес впровадження нових комбінацій у галузі технології виробництва чи управління певною господарською системою [1, с. 159]. Однак, згодом, у тлумачному словнику Колінза, під інновацією розуміється «… здійснення змін шляхом впровадження чогось нового» [2]. О. М. Фолом'єв визначає інновацію «як форму прояву науково-технічного прогресу, результат творчої інтелектуальної праці людини, пов'язаної із поновленням усіх сфер діяльності людини» [3, с. 15]. Вважаємо, що таке тлумачення найбільш повно відповідає реаліям сьогодення, адже даний термін все частіше використовується для означення особливого виду соціальної діяльності – попередження злочинності. Отже, інновація – це процес, під час якого відбувається науковий пошук та впровадження нових засобів, методів, форм і врешті-решт більш досконалих технологій попередження злочинності в Україні. Попередження злочинності – це діяльність, яка спрямована на зниження рівня злочинності, зменшення її суспільної небезпеки шляхом усунення, послаблення дії криміногенних факторів. Однак чимало криміногенних факторів може були закладено ще на рівні нормативно-правого регулювання суспільних відносин, коли нормативно-правова конструкція (окремого нормативного припису чи їх сукупності) самостійно чи у взаємодії з іншими нормами, створюють ризик вчинення злочинів й, зокрема, окремими категоріями осіб. У зв'язку з цим одним з таких нових перспективних засобів попередження злочинності можна вважати кримінологічну експертизу. Разом з тим на даний час кримінологічна експертиза не одержала свого всебічного практичного використання як засіб попередження злочинності. Натомість в Україні вже започатковано механізми

реалізації антикорупційної експертизи, яка за змістом є окремим видом кримінологічної. Так, у ст. 15 Закону України «Про засади запобігання та протидії корупції» зазначається, що антикорупційна експертиза проводиться з метою виявлення у проектах нормативно-правових актів норм, що можуть сприяти вчиненню корупційних правопорушень і розроблення рекомендацій стосовно їх усунення.

Загалом кримінологічна експертиза полягає у визначенні відповідності нормативно-правових актів соціальним потребам суспільства шляхом виявлення та усунення можливих криміногенних наслідків в результаті прийняття чи правозастосування нормативно-правових актів [4, с. 44]. Кримінологічна експертиза, як вид наукової експертизи та складова частина правової експертизи, має проводитися, передусім, експертами в галузі попередження злочинності. Однак в залежності від змісту нормативного акту і характеру поставлених питань до проведення кримінологічної експертизи необхідно залучати соціологів, економістів, інших фахівців конкретних галузей знань. Таким чином, кримінологічна експертиза за характером учасників є комплексною, однак керівна роль має відводитися експертам у галузі попередження злочинності. Кримінологічна експертиза також може бути доручена науково-дослідним установам або учбовим закладам чи професійним асоціаціям (організаціям) кримінологів [5].

Попередження злочинності включає здійснення широкого комплексу засобів не лише спеціально-кримінологічних, але й загальносоціальних. У зв'язку з цим виникає чимало дискусій з приводу того чи доцільно загальносоціальне попередження вважати кримінологічною категорією. Адже, по-перше це діяльність, що не має на меті боротьбу зі злочинністю, а покращення якості життя у суспільстві в цілому; по-друге, загальносоціальні заходи розробляються без урахування кримінологічної інформації про злочинність; по-третє такі заходи містяться у планах соціально-економічного розвитку, законах, інших нормативно-правових актах, що не стосуються регулювання суспільних відносин у сфері боротьби зі злочинністю. Разом з тим загальносоціальне попередження злочинності створює сприятливе підґрунтя для подальшої реалізації спеціально-кримінологічних заходів. Відтак, запровадження кримінологічної експертизи проектів нормативно-правових актів, у тому числі тих, які розробляються не у галузі правоохоронної діяльності, певною мірою усуне можливі суперечності з приводу недоцільності відносити загальносоціальне попередження до сфери кримінологічних інтересів. Отже, запровадження кримінологічної експертизи має не лише важливе практичне значення для

удосконалення попередження злочинності, але й важливе загальнотеоретичне значення для подальшого розвитку кримінологічної науки.

Список використаних джерел:

1. Шумпетер Й. Теория экономического развития/ Й. Шумпетер. – М. : Прогресс, 1982. – 456 с.

2. Collins National Dictionary. – London and Glasgow, 1966.

3. Фоломьев А. Н. Национальная промышленность и научно-техническая политика России, их влияние на решение экологических проблем / А. Н. Фоломьев // Морозовский проект «Экологический менеджмент». – М. : РАГС, 1995. – 120 с.

4. Бородин С. В. О криминологической экспертизе законов и иных нормативных актов / С. В. Бородин, В. В. Лунеев // Государство и право. – 2002. – № 6. – С. 44–45.

5. Проект Закону України «Про кримінологічну експертизу проектів нормативно-правових актів» [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb_n/webproc4_2?id=&pf3516=7755&skl=5.

Отримано 07.11.2012

УДК 681.3

Ірина Олександрівна ЯКОВЛЕВА
кандидат технічних наук, доцент,
доцент кафедри математичного моделювання
та інформаційних технологій навчально-наукового інституту
права та масових комунікацій
Харківського національного університету внутрішніх справ
Сергій Олександрович ПОЛОНИЦЬКИЙ
курсант групи ФПТ-09-2 факультету психології, менеджменту,
соціальних та інформаційних технологій
Харківського національного університету внутрішніх справ

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП'ЮТЕРА НА РІВНІ ФІЗИЧНОГО ДОСТУПУ

Розглянуто питання захисту комп'ютера на рівні фізичного доступу. Запропоновано використовувати комплексний підхід для захисту від несанкціонованого копіювання інформації, що складається з декількох етапів

Безпека конкретного об'єкта є складовою частиною загальної системи інформаційної безпеки. Захистити себе від злому і викрадення цінної інформації в два кліка вирішити не вийде. Вирішувати проблему мережевої безпеки потрібно поетапно.

Основними напрямками робіт із захисту інформації є: захист на рівні фізичного доступу до комп'ютера; організація безпечної роботи в локальній мережі і захист при підключенні до глобальних мереж.

У разі виникнення потенційної можливості несанкціонованого фізичного доступу до комп'ютера інші заходи безпеки марні. Це одна з найважливіших заповідей. Необхідно застосувати комплексний підхід щодо захисту від несанкціонованого проникнення. Одним з типових прикладів є розміщення серверів компанії в спеціальних приміщеннях, доступ до яких суворо обмежений, однак не треба забувати про ситуації грубого вторгнення в організацію, а також про те, що найбільш вразливі з точки зору фізичного доступу комп'ютери мобільних користувачів.

Процес входу в систему потрібен для ідентифікації користувача. Отримавши ці відомості, операційна система дозволяє або забороняє доступ до відповідних системних ресурсів. Якщо зловмисник дізнається пароль користувача, він зможе входити в систему під ім'ям цього користувача. Тому одним з головних завдань забезпечення безпеки комп'ютера є організація зберігання паролів. Алгоритми

шифрування типу AES і Bloufish, використовувані в менеджерах паролів дуже надійні та не відкриваючі. Асиметричні, з так званим відкритим або публічним ключем, алгоритми шифрують файли одним ключем, а розшифровуються – іншим, отриманим з першого. Менеджер сам придумає паролі, необхідно запам'ятати лише один пароль до самого менеджеру. Паролі у вигляді слів елементарно підбираються за словником. Прикладом парольного менеджера може служити KeePass. База паролів в цьому менеджері шифрується AES-256 і зберігається у файлі, який можна синхронізувати будь-якими зручними способами.

Наступним етапом захисту особистої інформації повинно стати приховування будь-яких документів і папок від сторонніх осіб. Для цього існують програми, подібні TrueCrypt, які дозволяють створювати віртуальні зашифровані диски, які потім можуть використовуватися як звичайні логічні диски системи. Допустимі алгоритми шифрування: AES (256-бітний ключ), Serpent (256-бітний ключ), Twofish (256-бітний ключ). Шифруються повністю всі дані, включаючи назви файлів і папок. Способом гарантованого знищення даних з комп'ютера є спеціальні програми, наприклад Eraser – інструмент для безпечного стирання файлів, який дозволяє повністю видаляти дані з жорсткого диска, записуючи поверх них кілька разів складні зразки, щоб неможливо було відновити стерті дані. У інструмента Eraser є ще одна чудова функція – ця програма чистить вільне місце жорстких дисків від шматків колись давно видалених файлів, роблячи тим самим неможливість їх відновлення.

Грамотно реалізований комплекс заходів із захисту інформації на комп'ютері дозволяє навіть при отриманні зловмисником фізичного доступу максимально знизити можливість викрадення інформації.

Отримано 20.11.2012

УДК 343.163;34.06;343.985

Александр Петрович Бабиков
начальник управления надзора
за соблюдением законов специальными подразделениями и иными
органами, ведущими борьбу с организованной преступностью
и коррупцией прокуратуры Харьковской области,
старший советник юстиции, соискатель кафедры уголовного права № 1
Национального университета «Юридическая академия Украины
имени Ярослава Мудрого»

ПОНЯТИЕ И ОСОБЕННОСТИ НЕГЛАСНЫХ СЛЕДСТВЕННЫХ (РОЗЫСКНЫХ) ДЕЙСТВИЙ В НОВОМ УПК УКРАИНЫ

Проанализирован Уголовный процессуальный кодекс Украины 2012 года, соотношение негласных следственных (розыскных) действий и оперативно-розыскной деятельности, особенности назначения, проведения и фиксации негласных следственных (розыскных) действий.

С принятием нового Уголовного процессуального кодекса Украины функции, цели и задачи уголовного процесса остались, фактически неизменными, несколько изменились требования к порядку проведения и фиксации следственных действий.

Однако если говорить о негласных следственных действиях, это абсолютно новая для уголовного процесса форма сбора и фиксации доказательств. Можно говорить о том, что негласные следственные действия имеют много общего с оперативно-розыскной деятельностью, и это так, но главная проблема в том, что надзор за ОРД осуществляют и соответственно специфику этого направления прокурорской деятельности знают единицы, что усложняет процесс понимания и применения указанных новаций.

При этом в открытом (несекретном) информационном пространстве Украины (да и стран СНГ) по данной теме изданы считанные учебники по теории ОРД, а темы прокурорского надзора за ОРД фрагментарно освещены в отдельных учебниках, монографиях и научных статьях. В частности, указанные вопросы изучались Михайловым В. А., Самоделкиным С. М. [1], Курочкой М. И. [2–4], Середой Г. П. [5], Козьяковым И. Н. [6; 8–10].

Безусловно, неверно ставить знак равенства между негласными следственными (розыскными) действиями и оперативно-розыскной деятельностью. Но тем не менее, они имеют много общего. Факт и методы (формы) их проведения являются секретными, однако если

ОРМ проводятся инициативно оперативными подразделениями, то негласные следственные (розыскные) действия (далее – НС(Р)Д) – исключительно по инициативе следователя и прокурора, которые самостоятельно определяют как вид мероприятия, порядок его проведения, так и подразделение, которому оно будет поручено. Кроме того, если ОРД могут заниматься только уполномоченные оперативные подразделения, то НС(Р)Д проводятся в первую очередь следователем, или же оперативным подразделением по его поручению. При этом оперативное подразделение, в соответствии с ч. 2 ст. 41 УПК пользуются полномочиями следователя. Соответственно можно сделать вывод, что выполняя поручение следователя, сотрудники оперативных подразделений, руководствуются не Законом Украины «Об оперативно-розыскной деятельности» [11], а УПК Украины [12].

Негласные следственные (розыскные) действия (далее – НС(Р)Д) регламентированы главой 21 УПК Украины, в которой законодатель выделил три раздела:

1. Общие положения о негласных следственных действиях.
2. Вмешательство в частное общение.
3. Другие виды негласных следственных действий.

НС(Р)Д могут проводиться, если:

1. Сведения о преступлении и лице, его совершившем, нельзя получить иным способом.

2. Проводятся, как правило, по тяжким и особо тяжким преступлениям.

Возникает вопрос, могут ли НС(Р)Д проводиться по нетяжким преступлениям?

В зависимости от тяжести преступления нет никаких ограничений при проведении такого НС(Р)Д как установление местонахождения радиоэлектронного устройства (ст. 268 УПК Украины) и снятие информации с электронных информационных систем, доступ к которым не ограничивается их собственником, пользователем или владельцем или системой логической защиты (ч. 2 ст. 264 УПК Украины). Это исключения из общих правил. Все остальные НС(Р)Д – только по тяжким и особо тяжким пр.

Могут ли *НС(Р)Д, связанные с вмешательством в частное общение, проводиться без решения следственного судьи?* Следует отметить, что действительно в ч. 2 ст. 258 УПК Украины указанно, что никто не может быть подвергнутым вмешательству в частное общение без определения следственного судьи. Это общее правило, но ч. 2 ст. 264 УПК Украины установлено исключение, если нет запрета собственника, пользователя или владельца, или снятие такой

информации не связано с преодолением системы логической защиты, то получение информации с такого устройства или системы, без решения следственного судьи возможно.

Рассмотрим эти два действия:

Установление радиоэлектронного устройства (ст. 268 УПК Украины) может заключаться в:

1. Установлении по базовым станциям местонахождения, интервала времени, перемещения радиоэлектронного устройства (телефон, смартфон, планшетник и т. д.) принадлежащего или пребывающего в пользовании подозреваемых, потерпевших, свидетелей и т. д.

2. Определении местонахождения в конкретное время радиоэлектронного устройства, активированного в сетях мобильной связи.

Снятие информации с электронной информационной системы (ст. 264 УПК Украины) может заключаться в:

1) исследовании информации в электронном устройстве (телефоне, смартфоне, планшетнике, компьютере и т. д.), заключающейся в списке абонентов, входящих и исходящих вызовах, сообщениях, текстовых, аудио и видео файлах и иных записях на самих устройствах или их частях (карта памяти и т.д.);

2) получении информации с сайтов с открытым доступом, в том числе («Одноклассники», «В контакте», на форумах и т. д.) не защищенной, и доступ к которой не ограничен пользователем.

Такие мероприятия сейчас активно используются оперативными и следственными подразделениями при расследовании уголовных дел и, с учетом распространенности радиоэлектронных устройств, это негласное следственное действие будет применятся очень широко.

Поэтому законодатель и выделил эти мероприятия как такие, которые могут проводиться по преступлениям любой тяжести, а также в некоторых случаях без разрешения следственного судьи.

Все остальные негласные следственные действия могут проводиться только по тяжким и особо тяжким преступлениям, и это требование законодателем обусловлено тем, что помимо взятия под стражу, проведения обыска у лица, назначения приговором наказания, связанного с лишением свободы, конфискации имущества, ничто так не ограничивает права и свободы человека, как проведение НС(Р)Д.

Решение о проведении НСРД принимают: следователь; следователь с согласия руководителя следственного подразделения; прокурор; следственный судья по представлению следователя, согласованного с прокурором или прокурора.

Общий механизм получения согласия у уполномоченного лица сложностей не представляет, в ходатайстве, к которому приобщается извлечение из Единого реестра, указываются установленные ст. 248 УПК Украины обстоятельства, при этом на орган досудебного следствия не возложена обязанность предоставлять какие-либо еще документы. Однако, на следователя и прокурора возлагается обязанность доказать два обстоятельства:

1. Совершенное преступление относится к категории тяжких или особо тяжких.

2. Во время проведения НС(Р)Д могут быть получены доказательства, имеющие существенное значение по делу.

Соответственно можно предположить, что аргументируя свою позицию, следователь и прокурор должны предоставить суду для ознакомления собранные ими документы или иные носители, которые могут быть использованы как доказательства.

Законодателем также предусмотрены случаи проведения негласных следственных действий до вынесения определения следственным судьей.

В дискуссиях по поводу применения этой нормы часто звучит мнение, что это не что иное, как уже существующая норма в ЗУ «Об оперативно-розыскной деятельности», согласно которой в неотложных случаях по рапорту, согласованному с руководителем подразделения, возможно проведение оперативно-технических мероприятий с целью фиксации противоправных действий по тяжким и особо тяжким преступлениям, и соответственно ничего принципиального не поменялось.

Действительно, ст. 250 УПК Украины установлено, что в исключительных случаях, связанных со спасением людей и пресечением тяжкого или особо тяжкого преступления, могут проводиться такие мероприятия с последующей, так называемой, «легитимизацией» через следственного судью.

Вместе с тем, не все так просто. Есть ряд существенных обстоятельств, которые могут повлиять на допустимость собранных таким способом доказательств. Следует отметить:

1. Этот случай исключение из правил, то есть его применять можно очень редко при исключительных обстоятельствах, когда отсутствует возможность получить санкцию следственного судьи. Это связано со спасением человеческих жизней и пресечением тяжкого или особо тяжкого преступления. Если в суде адвокат докажет, что у прокурора было время получить согласие следственного судьи или это

не было никак связано со спасением жизней людей, – полученные доказательства могут быть признаны не допустимы.

2. При этом преступления, которые пресекаются, должны быть не только тяжкими и особо тяжкими, а и находиться в определенных разделах УК Украины. Вместе с тем, незаконное похищение человека (ч. 3 ст. 146 УПК Украины) или организация массовых беспорядков (ст. 294 УПК Украины) находятся в разделах 3 и 12 УК Украины, и соответственно без санкции судьи, несмотря на то, что они являются тяжкими, проводить НС(Р)Д запрещено. Статья 250 УПК Украины на них не распространяется.

3. Из всего перечня НС(Р)Д до вынесения следственным судьей определения можно провести только два вида НС(Р)Д установление радиоэлектронного устройства (ст. 268 УПК Украины) и наблюдение за лицом, вещью или местом (ст. 269 УПК Украины), проведение иных НС(Р)Д не предусмотрено. При этом, как поиск радиоэлектронного устройства, так и наблюдение за лицом исключает возможность вмешательства в общение. Полученная информацию об общении не может быть использована как доказательство.

4. Процедура реализации: решение принимает следователь с согласия прокурора, безотлагательно с момента начала ее проведения прокурором уведомляется следственный судья, который может не признать законным проведение таких мероприятий, и полученные доказательства подлежат уничтожению.

Указанные обстоятельства и алгоритм реализации ст. 250 УПК Украины позволяют сделать вывод, что ее использование в практической деятельности не будет эффективно, и нужно ориентироваться на то, что бы во всех случаях, предусмотренных законом, получать санкцию следственного судьи.

Сроки и фиксация.

Общий срок действия определения следователя судьи – 2 месяца, может продлеваться в установленном порядке, но не должен превышать максимальных сроков расследования.

При проведении НС(Р)Д производится фиксация по общим правилам, с составлением протокола и дополнений к ним (фото, аудио, видео фиксация, образцы и т. д.) Однако в отдельных случаях могут быть засекречены сведения о лицах проводивших такие действия либо участвовавших в них в случае применения мер безопасности.

В соответствии со ст. 252 УПК Украины, протокол о проведении НС(Р)Д с приложениями на протяжении 24 часов передается прокурору, на которого и возлагается обязанность обеспечить их сохранность.

Вместе с тем, есть и определенные особенности. Так арест на корреспонденцию (ст. 261, 262 УПК Украины) заключается в возможности следователя или уполномоченного им подразделения осмотреть, при наличии необходимости изъять, отобрать образцы, сделать копии, нанести специальные отметки, оборудовать техническими средствами контроля, заменить на аналог. При этом по каждому факту осмотра, изъятия и т. д. составляется отдельный протокол (это исключение из общего правила), а не в конце срока действия определения следственного судьи, что дает возможность постоянно фиксировать и использовать такие протоколы как аргументацию для проведения иных следственных действий или продления срока ареста корреспонденции.

Нередко возникает вопрос, какие документы и материалы, их копии, могут предоставляться суду для рассмотрения вопросов как то: о даче разрешения на обыск, о применении мер обеспечения уголовного производства, о проведение НС(Р)Д, принятии иных решений. И хотя прямо в законе не указано на необходимость направлять материалы уголовного дела или их копии для принятия решения судье, многие, по аналогии с действующим процессом, высказывают мысль, что суду необходимо дать какие-то документы, чтобы он обосновал свое решение и мотивировал его, а также приобщил такие материалы к делу, находящемуся в суде.

Следует указать, что ч. 3 ст. 254 УПК Украины прямо запрещено делать копии протоколов и приложений к ним по НС(Р)Д. Исключений нет. Указанные протоколы могут быть изготовлены лишь в одном экземпляре и никому, ни судье, ни адвокату, ни прокурору в надзорное производство в копиях не предоставляются независимо от присвоения им грифа секретности.

Список литературы

1. Михайлов В. А. Прокурорский надзор за исполнением законов органами, осуществляющими оперативно-розыскную деятельность : учеб. пособие / В. А. Михайлов, С. М. Самоделкин. – Волгоград : ВСШ МВД России, 1995. – 180 с.

2. Курочка М. Й. Прокурорський нагляд за додержанням законів органами, які здійснюють оперативно-розшукову діяльність : навч. посіб. / М. Й. Курочка. – 2-ге вид., переробл. і доповн. / за ред. Е. О. Дідоренка ; МВС України, Луган. акад. внутр. справ ім. 10-річчя незалежності України. – Луганськ : РВВ ЛАВС, 2005. – 176 с.

3. Курочка М. Й. Прокурорський нагляд в Україні : підручник / М. Й. Курочка, П. М. Каркач ; за ред. Е. О. Дідоренка. – К. : Центр навч. л-ри, 2005. – 424 с.

4. Курочка М. Й. Законність в оперативно-розшуковій діяльності та прокурорський нагляд за її дотриманням : автореф. дис. ... канд. юрид. наук : спец. 21.07.04 «Оперативно-розшукова діяльність». – К., 2000.

5. Середа Г. П. Законність оперативно-розшукової діяльності як мета та завдання прокурорського нагляду / Г. П. Середа // Вісник національної академії прокуратури України. – 2009. – № 4. – С. 11–17.

6. Козьяков І. М. Прокурорський нагляд за законністю оперативно-розшукової діяльності: його проблеми / І. М. Козьяков // Право України. – 2000. – № 1. – С. 82–85.

7. Соколкін В. Л. Щодо характеристики стану правового регулювання прокурорського нагляду за додержанням законів в оперативно-розшуковій діяльності ОВС / В. Л. Соколкін // Сучасні проблеми правового, економічного та соціального розвитку держави : матеріали наук.-практ. конф. (Харків, 10 квіт. 2012 р.) / МВС України, Харк. нац. ун-т внутр. справ. – Х. : ХНУВС, 2012. – 432 с.

8. Козьяков І. М. Прокурорський нагляд та судовий контроль за оперативно-розшуковою діяльністю при розслідуванні злочинів: проблеми та реальність / І. М. Козьяков // Право України. – 1999. – № 3. – С. 21–26.

9. Козьяков И. Н. Соотношение судебного контроля и прокурорского надзора за соблюдением законов органами, осуществляющими оперативно-розыскную деятельность / И. Н. Козьяков // Вісник Луганського інституту внутрішніх справ. – 1999. – № 1.

10. Козьяков И. Н. Прокурор и оперативно-розыскная деятельность / И. Н. Козьяков // Юридический вестник. – 2000. – № 4. – С. 99–102.

11. Про оперативно-розшукову діяльність : закон України від 18 лют. 1992 р.// Відомості Верховної Ради України. – 1992. – № 22. – Ст. 303.

12. Кримінальний процесуальний кодекс України : прийн. Верховною Радою України Законом № 4651-VI від 13.04.2012. – Х. : Право, 2012. – 392 с.

Отримано 03.12.2012

Проаналізовано Кримінальний процесуальний кодекс України 2012 року, співвідношення негласних слідчих (розшукових) дій та

оперативно-розшукової діяльності, особливості призначення, проведення та фіксації негласних слідчих (розшукових) дій.

—

УДК 343.163;34.06;343.985

Олександр Олександрович Цимбалістенко
заступник начальника управління – начальник відділу нагляду за додержанням законів спецпідрозділами та іншими органами, які ведуть боротьбу з організованою злочинністю, та процесуального керівництва прокуратури Харківської області, радник юстиції, здобувач кафедри організації судових та правоохоронних органів Національного університету «Юридична академія України імені Ярослава Мудрого»

ОКРЕМІ АСПЕКТИ ПРОКУРОРСЬКОГО НАГЛЯДУ ЗА ДОДЕРЖАННЯМ ЗАКОНОДАВСТВА ПРО БОРОТЬБУ З ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ

Розглянуто законодавство України щодо протидії організованій злочинності, зокрема особливості прокурорського нагляду за додержанням закону спеціальними підрозділами, які ведуть боротьбу з організованою злочинністю та корупцією.

Тема боротьби з організованою злочинністю є актуальною у науковому та практичному відношенні, що викликає дотепер неоднозначні підходи до її проблематики з боку вчених та практиків.

Відповідно до ч. 1 ст. 4 Закону України «Про організаційно-правові основи боротьби з організованою злочинністю» законодавство про боротьбу з організованою злочинністю базується на Конституції України і включає цей Закон, Кримінальний і Кримінальний процесуальний кодекси України, закони України «Про оперативно-розшукову діяльність», «Про міліцію», «Про Службу безпеки України», «Про прокуратуру», інші закони, міжнародно-правові угоди, учасником яких є Україна [1].

Вказаним Законом визначені головні напрями загальнодержавної політики та організаційно-правові основи боротьби з організованою злочинністю. Поряд із цим законодавчо запроваджено спеціалізацію прокурорів у здійсненні повноважень саме на цьому напрямі боротьби зі злочинністю.

Згідно з ч. 1, 2 ст. 26 цього ж Закону нагляд за виконанням законів у сфері боротьби з організованою злочинністю здійснюється Генеральним прокурором України і підпорядкованими йому прокурорами. Для здійснення нагляду за виконанням законів спеціальними підрозділами по боротьбі з організованою злочинністю, здійсненням досудового розслідування відповідних злочинів, а також підтриманням державного обвинувачення в суді по цих кримінальних провадженнях у Генеральній прокуратурі України створюється управління, а в Автономній Республіці Крим, областях, містах Києві та Севастополі – його відділи.

Відтак, прокурорський нагляд у вказаній сфері є окремим [illegible] **альності**, якому притаманні особливі [illegible] фіки та комплексного характеру [illegible] ся матеріальними та процесуальними нормами кількох галузей права.

Пунктом 1 наказу Генерального прокурора України від 19.09.2005 № 4/2гн «Про організацію прокурорського нагляду за додержанням законів спеціальними підрозділами та іншими установами, які ведуть боротьбу з організованою злочинністю» визначено мету цього нагляду, яка полягає у захисті конституційних прав і свобод громадян та інтересів держави, вжитті передбачених чинним законодавством заходів щодо усунення виявлених порушень закону [2, с. 311–315].

При визначенні проблематики прокурорського нагляду на вказаному напрямі слід виходити передусім із законодавчого визначення в Україні поняття «організованої злочинності».

Відповідно до ч. 1 ст. 1 Закону України «Про організаційно-правові основи боротьби з організованою злочинністю» під організованою злочинністю в цьому Законі розуміється сукупність злочинів, що вчиняються у зв'язку з створенням та діяльністю організованих злочинних угруповань. Частиною 2 цієї ж статті визначено, що види та ознаки цих злочинів, а також кримінально-правові заходи щодо осіб, які вчинили такі злочини, встановлюються Кримінальним кодексом України.

У свою чергу, ч. 3, 4 ст. 28 Кримінального кодексу України встановлюють дві форми організованої злочинності, а саме організовану групу та злочинну організацію, які відрізняються за своїми кримінологічними ознаками. При цьому злочинна організація є більш суспільно небезпечною формою організованої злочинності, ніж організована група [3].

Слід зазначити, що до різновидів організованих злочинних угруповань відносяться озброєна банда (ст. 257 КК України), терористична група чи терористична організація (ст. 258-3 КК

України), не передбачені законами України воєнізовані формування (ст. 260 КК України).

Водночас жодна норма Загальної та Особливої частин КК України не містить поняття «організоване злочинне угруповання», яке застосовано законодавцем при визначенні організованої злочинності Законом України «Про організаційно-правові основи боротьби з організованою злочинністю».

Таким чином, задля конкретизації положень Закону України «Про організаційно-правові основи боротьби з організованою злочинністю» є доцільним приведення у відповідність та деталізація його понятійного апарату з огляду на терміни, що застосовані у Кримінальному кодексі України.

Метою боротьби з організованою злочинністю згідно зі ст. 2 Закону України «Про організаційно-правові основи боротьби з організованою злочинністю» є встановлення контролю над організованою злочинністю, її локалізація, нейтралізація та ліквідація. **Проте, законодавцем не дано тлумачення термінам «встановлення контролю», «локалізація», «нейтралізація» та «ліквідація».**

Вбачається, що під терміном «встановлення контролю над організованою злочинністю» слід розуміти не що інше як контроль за вчиненням злочину, який є різновидом негласних слідчих (розшукових) дій, передбаченим ст. 271 Кримінального процесуального кодексу України, та здійснюється відповідно до ч. 4 ст. 246 КПК України виключно за рішенням прокурора [4]. Прокурор у цьому випадку виступає як сторона обвинувачення – прокурор, який здійснює нагляд за додержанням законів під час проведення досудового розслідування у формі процесуального керівництва досудовим розслідуванням (ст. 36 КПК України).

Згідно зі ст. 272 КПК України одним з різновидів негласних слідчих (розшукових) дій є виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації, що також може розглядатися в контексті встановлення контролю над організованою злочинністю в межах досудового розслідування, порядок якого визначається лише кримінальним процесуальним законодавством України.

Крім того, ст. 275 КПК України надає слідчому право використовувати конфіденційне співробітництво.

Розділом IV Закону України «Про організаційно-правові основи боротьби з організованою злочинністю» передбачені такі заходи забезпечення боротьби з організованою злочинністю як використання негласних співробітників (ст. 13), використання учасників організованих

злочинних угруповань у боротьбі з організованою злочинністю (ст. 14), використання спеціальних технічних засобів у боротьбі з організованою злочинністю (ст. 15), останні два з яких мають проводитися у випадках та порядку, передбачених Законом України «Про оперативно-розшукову діяльність» та Кримінальним процесуальним кодексом України.

З огляду на викладене досягнення мети боротьби з організованою злочинністю, встановленої ст. 2 Закону України «Про організаційно-правові основи боротьби з організованою злочинністю», має відбуватися суворо у межах, визначених Кримінальним процесуальним кодексом України, Законом України «Про оперативно-розшукову діяльність». **Виходячи з цього, термінологія цих законів має бути приведена у відповідність, що також має важливе значення для визначення обсягу, змісту, механізму реалізації повноважень прокурора при здійсненні нагляду за виконанням вимог того чи іншого законодавчого акту про боротьбу з організованою злочинністю.**

Законом України від 13.04.2012 «Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Кримінального процесуального кодексу України» [4] внесено ряд змін до Закону України «Про організаційно-правові основи боротьби з організованою злочинністю», якими його окремі положення приведені у відповідність до нового кримінального процесуального законодавства.

Спецпідрозділам по боротьбі з організованою злочинністю залишено раніше надані законом повноваження, які реалізовуватимуться вже відповідно до нового КПК України.

Оскільки Закон України «Про організаційно-правові основи боротьби з організованою злочинністю» визначає повноваження спеціальних підрозділів, які ведуть боротьбу з організованою злочинністю, які є структурними підрозділами Міністерства внутрішніх справ (ст. 9) та Служби безпеки України (ст. 10), доцільно визначити у цьому Законі окремо та детально повноваження не лише прокурорів, які очолюють управління та відділи по нагляду за виконанням законів спеціальними підрозділами по боротьбі з організованою злочинністю (ч. 5 ст. 26), а й прокурорів цих управлінь та відділів, виходячи з вимог Кримінального процесуального кодексу України, законів України «Про прокуратуру», «Про оперативно-розшукову діяльність».

Прокурорський нагляд за додержанням законів спецпідрозділами та іншими органами, які ведуть боротьбу з організованою злочинністю, включає в себе:

1. Нагляд за додержанням законів спеціальними підрозділами при проведенні оперативно-розшукової діяльності.

2. Нагляд за додержанням законів під час проведення досудового розслідування кримінальних правопорушень, вчинених організованими злочинними угрупованнями, у формі процесуального керівництва.

3. Нагляд за додержанням ст. 17, 18 Закону України «Про організаційно-правові основи боротьби з організованою злочинністю» як спецпідрозділами по боротьбі з організованою злочинністю, так і Національним банком України, Міністерством фінансів України, Міністерством зовнішніх економічних зв'язків України, Державним митним комітетом України, Фондом державного майна України, Антимонопольним комітетом України, спеціально уповноваженим центральним органом виконавчої влади у справах охорони державного кордону України та іншими міністерствами і відомствами, що мають право контролю за дотриманням організаціями і громадянами законодавства України.

4. Нагляд за додержанням законів при здійсненні працівниками спеціальних підрозділів інших повноважень, встановлених законами України «Про міліцію», «Про Службу безпеки України», «Про організаційно-правові основи боротьби з організованою злочинністю».

Таким чином, з огляду на комплексний характер вказаного напряму прокурорського нагляду, доцільно окремо визначити повноваження прокурорів шляхом внесення відповідних змін та доповнень як до Закону України «Про організаційно-правові основи боротьби з організованою злочинністю», так і до Закону України «Про прокуратуру».

Конкретизація та уніфікація законодавчо визначених повноважень прокурорів з нагляду за додержанням законодавства по боротьбі з організованою злочинністю сприятиме ефективній реалізації державної політики у сфері протидії організованим формам злочинності в умовах запровадження нового кримінального процесуального законодавства, реформування системи правоохоронних та контролюючих органів у державі.

Список літератури:

1. Про організаційно-правові основи боротьби з організованою злочинністю : закон України // Відомості Верховної Ради України. – 1993. – № 35. – Ст. 358.

2. Про організацію прокурорського нагляду за додержанням законів спеціальними підрозділами та іншими установами, які ведуть боротьбу з організованою злочинністю : наказ Ген. прокурора України // Прокуратура України : законодавство, рішення Конституц. Суду України, накази та ін. організаційно-розпоряд. док. Ген. прокурора

України / Ген. прокуратура України ; за заг. ред. О. І. Медведька ; керівн. проекту С. М. Винокуров ; упор. Г. М. Титарчук, Є. П. Бурдоль, І. С. Зарубинська та ін. – К. : Юрінком Інтер, 2009. – 576 с.

3. Кримінальний кодекс України : закон України // Відомості Верховної Ради України. – 2001. – № 25–26. – Ст. 131.

4. Кримінальний процесуальний кодекс України : прийн. Верховною Радою України Законом № 4651-VI від 13.04.2012 р. Закон України «Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Кримінального процесуального кодексу України» № 4652-VI від 13.04.2012 р. – Х. : Право, 2012. – 392 с.

Отримано 03.12.2012

Наукове видання

Використання інноваційних технологій у попередженні злочинів

Матеріали науково-практичного семінару
(м. Харків, 6 грудня 2012 року)

Відповідальні за випуск: *В. В. Тулупов, В. В. Шендрик, О. М. Рвачов*
Коригування: *П. О. Білоус*
Комп'ютерне верстання: *П. О. Білоус, О.М. Рвачов*

Формат 60х84/16. Ум. друк. арк, 11,43. Обл.-вид. арк. 10,06.
Тираж 40 пр. Зам. № 2012-19. Підписано до друку 03.12.2012.

Видавець і виготовлювач –
Харківський національний університет внутрішніх справ,
просп. 50-річчя СРСР, 27, м. Харків, 61080.

Свідоцтво суб'єкта видавничої справи ДК № 3087 від 22.01.2008.