W. По-видимому, структура модели $\sigma_{z1}(g_1, g_2)$ является более адекватной задаче исследования погрешности оценивания разборчивости W речевого сообщения, позволяя более наглядно отобразить механизм и степень влияния факторов x_1 и x_2 (порождающих соответственно ошибки g_1 и g_2) на формирование погрешности оценивания.

V Выводы

Предложена описательная модель процесса возникновения ошибок аудитора при распознавании им искаженных маскирующей помехой слов артикуляционных таблиц, позволяющая на качественном уровне интерпретировать особенности и характеристики ошибок аудитора, объяснить форму закона распределения погрешностей оценок разборчивости. Построены аппроксимативные математические модели зависимостей словесной разборчивости W и среднеквадратической погрешности ее оценивания σ_z от определяемых из данных артикуляционных испытаний значений выходных индикаторных переменных g_1, g_2, интегрально учитывающих профессиональные характеристики бригады аудиторов.

Литература: ***1.*** *Архипова О. О., Журавльов В. М., Кумейко В. М. Артикуляційні таблиці слів української мови / О. О. Архипова, В. М. Журавльов, В. М. Кумейко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К., 2009. – № 2/19. – С. 13-17.* ***2.*** *Архипова О. О., Журавльов В. М., Доровських А. В. Таблиці слів української мови для артикуляційних випробувань розбірливості інформації, що передається трактами зв'язку / О. О. Архипова, В. М. Журавльов, А. В. Доровських // Зв'язок. – К., 2010. – № 1 (89). – С. 9-11.* ***3.*** *Архипов А. Е. Анализ и обработка данных артикуляционных испытаний / А. Е. Архипов, Е. А. Архипова // Захист інформації. – 2012. – №4 (57), – С.34 – 42.* ***4.*** *Мудров В. И. Методы обработки ошибок измерений / В. И. Мудров, В. Л. Кушко – М., Советское радио, 1976. – 192 с.* ***5.*** *Архипов А. Е. О моделировании некоторых типов случайных последовательностей / А. Е. Архипов // Вестник Киев. политехн. ин-та – Вып. 12. – К.:1988 – С. 39-44.* ***6.*** *Архипов О. Є. Модель ошибок экспертных оценок / О. Є. Архипов, С. А. Архипова // "Сучасні проблеми управління", Матеріали IV Міжнародної наук.-практичної конференції (28-30 листопада 2007р., м.Київ). – ІВЦ Видавництво "Політехніка"– К.: 2007. – С. 65-66.* ***7.*** *Вентцель Е. С., Овчаров Л. А. Теория вероятностей и её инженерные приложения / Е. С. Вентцель, Л. А. Овчаров – М.: Наука, 1988. – 480 с.* ***8.*** *Пугачев В.С. Теория вероятностей и математическая статистика / В. С. Пугачев – М.: Наука, 1979. – 496 с.* ***9.*** *Градштейн И. С. Таблицы интегралов, сумм, рядов и произведений / И. С. Градштейн, И. М. Рыжик – М.: ГИФМЛ, 1971.*

УДК 343.974

СТРУКТУРА КРИМІНАЛЬНИХ ВІДНОСИН У КІБЕРПРОСТОРІ

Ігор Гриненко, Дарія Прокоф'єва-Янчиленко*, Михайло Прокофьєв**

*Національна академія Служби безпеки України, *Служба безпеки України, **НДЦ "ТЕЗІС" НТУУ "КПІ"*

Анотація: **Розглянуто специфічні аспекти впливу сучасних телекомунікаційних технологій на структурні зміни угрупувань організованої злочинності та визначено можливі тенденції у формуванні такого роду утворень, що діють у сфері комп'ютерної злочинності.**

Summary: **The article examines the impact that modern telecommunication technologies have on the structural evolution of organized crime and offers an assessment trends in criminal enterprises, involved in cybercrime.**

Ключові слова: **Організована злочинність, кіберпростір, кіберзлочинність, правоохоронна діяльність**.

Вступ

Організована злочинність є одним із найбільш небезпечних суспільних явищ, що становить безпосередню загрозу національній безпеці окремих країн та міжнародному правопорядку в цілому. Особливо гострою ця проблема є для нашої країни, де процеси становлення демократичного державного управління, громадянського суспільства та ринкової економіки залишаються значною мірою не завершеними. За таких умов злочинність стає одним із ключових чинників, що перешкоджають реалізації державної політики як у внутрішній, так і в зовнішній сферах.

Найбільшої небезпеки організована злочинність набуває у формі транснаціональної протиправної діяльності, не обмеженої державними кордонами та географічними відстанями. Транснаціоналізації злочинності, набуттю нею якісно нових рис сприяє використання організованими злочинними угрупуваннями новітніх телекомунікаційних технологій як для забезпечення вчинення «традиційних» злочинів, наприклад, у сфері наркобізнесу, торгівлі людьми та зброєю, нелегальної міграції тощо, так і здійснення принципово нових видів протиправної діяльності, безпосередньо пов'язаних із функціонуванням кіберпростору.

Як зазначено у Концепції державної політики у сфері боротьби з організованою злочинністю «організовані злочинні угруповання дедалі частіше прагнуть використовувати Інтернет і новітні інформаційно-комп'ютерні технології для досягнення своїх кримінальних цілей». З огляду на це, Концепція ставить перед правоохоронними органами нові завдання щодо «визначення стратегічних напрямів їх діяльності, пошуку нових підходів до боротьби з організованою злочинністю, які б відповідали сучасним реаліям та враховували тенденції розвитку суспільства і держави» [1].

Результати досліджень

Сучасні дослідження протидії злочинності, пов’язаної із використанням телекомунікаційних технологій, стосуються, передусім, застосування норм кримінального права щодо осіб, причетних до цієї протиправної діяльності, а також технічних аспектів забезпечення інформаційної безпеки. Однак у таких дослідженнях питанням структурного розвитку організованих злочинних угрупувань, обумовленого впливом сучасних телекомунікаційних технологій, як правило суттєва увага не приділялася.

З огляду на це, **метою** статті є розкриття специфіки впливу сучасних технологій на структурні зміни організованої злочинності. Досягненню цієї мети сприятиме виконання таких завдань:

- дослідити структурні зміни в організованій злочинності в історичному контексті;
- визначити характер впливу телекомунікаційних технологій на структуру сучасних злочинних угрупувань;
- з'ясувати можливі тенденції створення та функціонування злочинних угруповань, що діють у кіберпросторі.

Незважаючи на те, що злочинність як діяльність певного роду організованих структур існувала впродовж усієї історії людства, формування феномену організованої злочинності у його сучасному стані сталося у XX столітті і найчастіше асоціюється із мафіозними структурами Італії та США, латиноамериканськими наркокартелями, а також виходом на транснаціональний рівень традиційних азійських «тріад» та «якудзи». При цьому до другої половини минулого століття організована злочинність як окремий феномен практично не привертала уваги науковців та юристів-практиків, і навіть традиційні мафіозні утворення часто взагалі розглядалися не як форма злочинності, а як своєрідний культурний феномен, прояв місцевої самоорганізації, що за своєю сутністю мало відрізнявся від тогочасних державних інституцій.

Усвідомлення феномену організованої злочинності почало відбуватися лише у 1950-1960-ті роки, у першу чергу в США, і дещо пізніше в Італії. Ключовою рисою цього феномену був його виражений антисоціальний характер, спрямований проти суспільства в цілому, а не лише проти окремих державних інститутів чи суспільних прошарків.

Подальша еволюція організованої злочинності відбувалася у напрямі транснаціоналізації – на відміну від традиційних мафіозних структур, орієнтованих на встановлення територіального контролю над визначеними видами злочинної діяльності, такими як наркоторгівля, торгівля людьми, незаконні азартні ігри та лихварство. Нові структури орієнтувалися виключно на максимізацію прибутку за рахунок розширення ринків збуту незаконних товарів та послуг, тож притаманна традиційній мафії система патронажу, обмеженого членства та чіткого ролевого розподілу виявилася не лише непотрібним анахронізмом, а й перешкодою для подальшого розвитку. Таким чином, місце мафіозних структур зайняли транснаціональні кримінальні мережі нового типу, побудовані на принципах самоорганізації та комерційного інтересу.

Передусім доцільно визначити сутність феномену організованої злочинності. Якщо розпочати з національного законодавства, слід звернути увагу на те, що поняття організованої злочинності міститься у ст. 1 Закону України «Про організаційно-правові основи боротьби з організованою злочинністю»: під організованою злочинністю розуміється сукупність злочинів, що вчиняються у зв'язку зі створенням та діяльністю організованих злочинних угруповань. Види та ознаки цих злочинів, а також кримінально-правові заходи щодо осіб, які вчинили такі злочини, встановлюються Кримінальним кодексом України [2]. При цьому Ст. 28 Кримінального кодексу України, присвячена питанням співучасті у вчиненні злочину, розглядає особливості вчинення злочину групою осіб, групою осіб за попередньою змовою, організованою групою або злочинною організацією [3].

Конвенція ООН проти транснаціональної організованої злочинності 2000 р. визначає організовану злочинність як структурно оформлену групу у складі трьох або більше осіб, існуючу протягом певного часу і діючу узгоджено для вчинення одного чи кількох серйозних злочинів, визнаних такими відповідно до цієї Конвенції, з тим щоб безпосередньо отримати фінансову або іншу матеріальну вигоду. Тобто, з точки зору Конвенції, організованою злочинністю є злочинна діяльність як злочинних організацій, так і організованих груп [4].

Інтерпол визначає організовану злочинну групу як «групу будь-яким чином асоційованих між собою осіб, що здійснює злочинну діяльність задля отримання прибутку, не зважаючи на національні кордони» [5]. Злочинні організації, як правило, вчиняють злочини і з іншою метою, наприклад для забезпечення власної безпеки, для чого вони встановлюють та фінансують корупційні зв'язки, здійснюють насильство щодо конкурентів чи представників правоохоронних органів тощо. Але такі дії не є самостійними і підпорядковані основній меті – отриманню прибутку. Таким чином, організована злочинна діяльність є формою підприємництва, що відрізняє її від «індивідуальної» злочинності, що часто має ірраціональний та емоційний характер. Організована злочинність являє собою раціональну цілеспрямовану діяльність з метою збагачення її учасників за рахунок жертв.

Отже, основними ознаками злочинної організації є:

а) ієрархічність;

б) розподіл ролей і функцій;

в) наявність "нормативних приписів";

г) самофінансування;

д) систематична злочинна діяльність.

Останню характеризують: протиправні засоби досягнення мети; професіоналізм і спеціалізація; конспірація; розвідувальні та контррозвідувальні заходи; прагнення нейтралізувати працівників державних органів влади і управління (корупція); зовнішня видимість законності дій.

Як і легальні організації, злочинні структури мають здатність до розширення, залучаючи до свого складу нових осіб. З іншого боку, усунення будь-якого члена організації, як правило, не призводить до її колапсу, що вірно як для легального, так і для нелегального бізнесу.

Найпростішою моделлю злочинної організації є «банда», що складається із лідера та підлеглих, із яких може бути (але не обов'язково) виділена певна група, що користується особливими правами. Такі структури існують впродовж тисячоліть і відомі з часів Стародавнього світу. Сила банди полягає у її чисельності. Вона функціонує, передусім, завдяки лідеру, що віддає обов'язкові для виконання накази, влада якого ґрунтується на певних організаційних принципах, як правило, на залякуванні інших. Групи, побудовані за моделлю банди, продовжують існувати, але складніші кримінальні оборудки потребують і більш складної організаційної моделі. Мафіозні структури, що раніше будувалися за такою простою моделлю, вже досить давно набули інших, більш складних, організаційних властивостей. Передусім це було пов'язано із виходом на значно більший, аніж традиційний італійський, ринок Сполучених Штатів. Впровадження «сухого закону» створило у цій країні величезний нелегальний ринок, що став сферою операційної діяльності злочинних організацій та приносив небачені до цього прибутки. Задоволення потреб на цьому ринку вимагало організацію поставок та продажу великих партій товару, його закупок або виробництва. Це, у свою чергу, перетворило злочинців із типових «бандитів» на бізнесменів. Успішні банди, такі як група Капоне у Чикаго, перекваліфікувалися із крадіжок та пограбувань на поставки заборонених товарів, що вимагало більш складної структури із відповідною ієрархією та розподілом ролей, як це має місце у легальних корпораціях. Таким чином, «банди» є ефективними, коли їх діяльність обмежена тим, аби лише відняти майно, що належить іншим, тоді як для отримання сталого прибутку потрібні організації, побудовані за корпоративним принципом. Для функціонування «банди» необхідно, аби майно, що вона збирається привласнити, вже було б кимось створене. Корпорація (у тому числі кримінальна) сама має можливості створювати майно, яке вона пропонує для продажу на ринку.

Здійснення тривалої діяльності, спрямованої на отримання максимального прибутку на мінливих ринках, неминуче призводить до конкурентного відбору та самоудосконалення організації. Інтенсивність цього процесу посилюється і відсутністю будь-яких правових обмежень як для здійснення конкурентної боротьби, так і для операцій із поставками товарів на ринок. З іншого боку, правова заборона діяльності таких організацій, вимушених оперувати всупереч зусиллям держави, змушує останніх швидше пристосовуватися до такого середовища, що також прискорює їх розвиток. Ці процеси є тим більш швидкими, чим більшим є прибуток від діяльності таких організацій.

Завершення епохи «сухого закону» призвело до змін мафіозного середовища. Значна частина угрупувань бутлегерів просто припинила своє існування. Серед тих, що вижили, найбільш помітною була італійська мафія «Коза-Ностра», що існувала задовго до введення «сухого закону» і продовжила діяти після його

відміни. Значні прибутки від незаконної торгівлі алкоголем призвели і до зміни способу життя мафіозі, що вже не бажали повертатися до моделі «банди». У 1930-ті роки мафія створила «Національну комісію», до складу якої входили лідери «родин», що розподілили між собою територію США, тобто, фактично була утворена ієрархічна корпорація національного рівня, що проіснувала впродовж десятиліть і дозволила усунути конфлікти між окремими структурами [6].

Регіональні підрозділи поставили під свій контроль злочинну діяльність на певних територіях, що включала, як правило, торгівлю людьми, наркобізнес, рекет, незаконні азартні ігри та лихварство. Подібні, але значно менші за масштабом діяльності структури сформували банди байкерів, що спеціалізувалися на торгівлі метамфетамінами та рекеті, та деякі інші формування. Окрім цього, певні ніши зайняли і інші етнічні структури, такі як японська «якудза», китайські «тонги» та «тріади», певною мірою представництва колумбійських та мексиканських картелів у США. З кінця 1990-х ці групи почали співробітничати між собою, зокрема, щодо розподілу праці, що, у свою чергу, дозволило їм ще більше максимізувати прибутки. Так, наркобізнес набув статусу глобального явища передусім через співпрацю кримінальних структур із різних регіонів світу [7-8].

Глобалізація злочинності розглядається як тенденція, що у майбутньому може лише посилюватися. Це, в свою чергу, сприятиме подальшому збільшенню могутності кримінальних угрупувань [9, С. 6 – 7]. Найбільш вагомим чинником, що визначає цю динаміку, є вплив інформаційних технологій, адже використання глобальних комп‘ютерних мереж у сучасному суспільстві призводить не лише до позитивних результатів, але й до зростання кількості джерел соціальних небезпек, в тому числі кримінального характеру [10, С. 318].

Ознакою останніх десятиліть стало використання кримінальними угрупуваннями телекомунікаційних технологій, їх вихід у кіберпростір, що призводить до подальших структурних змін організованої злочинності. Зокрема, соціальне середовище, що виникає у зв‘язку з використанням глобальних інформаційних мереж, викликає до життя специфічні форми соціальної взаємодії, в тому числі складні процеси детермінації злочинності та, відповідно, невідомі раніше види кримінальних формувань з якісно новою структурою.

Слід враховувати, що кіберпростір, з одного боку, пов‘язаний з існуючою географією світу фізичними мережевими об‘єктами (серверами, мережевим обладнанням, каналами зв‘язку, комп‘ютерами або іншими пристроями користувачів тощо), а з іншого – має особливі «над географічні» та транскордонні властивості, а також постійно змінюється, розширюється та модернізується. У разі вчинення злочину у такому просторі, як правило, встановлення фізичного місця знаходження злочинця та жертви (або предмета злочину) є можливим, а також є можливим визначення місця збереження слідів в апаратних пристроях мережевої інфраструктури, однак спроби просторової локалізації певних інформаційних об‘єктів може лишитися безрезультатною. Так, у кіберпросторі злочинець здатний одночасно виконувати низку різнопланових операцій у декількох обчислювальних системах, причому можливе також вчинення дистанційних діянь, за яких впливові піддається інформаційний об‘єкт, що перебуває на віддаленій відстані та не має фізичної прив‘язки до конкретного місця. Певні операції можуть виконуватися з мобільних пристроїв (ноутбуки, планшети тощо) в той час, коли оператор переміщується у фізичному просторі. Тобто, в певному сенсі можливо вести мову про «розмивання» фізичного місця вчинення злочину та порушення його просторової реалізації.

У кіберпросторі, так само як і у «реальному» просторі, корисним є об’єднання ресурсів задля досягнення певної, у тому числі злочинної мети, але тут таке об’єднання вимагає не стільки утворення групи осіб, скільки поєднання обчислювальних можливостей та навичок. Найбільш характерним прикладом такого використання ресурсів є організація DDoS-атак, що передбачає встановлення контролю над іншими комп’ютерами, які використовуються без відома їх власників. Створення угрупування чи, тим більше, збільшення числа його членів, для цього не є потрібним.

З іншого боку, об’єднання ресурсів може бути корисним, якщо злочинці забажають здійснити злочин проти декількох об’єктів або реалізувати серію злочинів. Вчинення злочинів проти низки об’єктів створюватиме середовище, у якому злочинцям буде легше досягти своєї мети. Окрім цього, розширення кола суб’єктів може слугувати приховуванню слідів злочинів, введенню в оману правоохоронних органів.

У тому разі, якщо злочинці переходитимуть від експропріації прибутків на їх генерування, цілком ймовірною є поява кримінальних структур типу корпорацій. Основною перевагою таких структур є об’єднання спеціалізованих елементів задля здійснення масштабних кримінальних акцій або одночасної реалізації декількох операцій. Такого роду структура є доцільною у разі організації торгівлі певним товаром або послугами. На сьогодні основним видом нелегальних товарів, представленим у кіберпросторі, є предмети інтелектуальної власності, розповсюдження яких є відносно простим процесом, що не потребує додаткових організаційних зусиль, подібних до забезпечення поставок наркотиків чи налагодження каналів торгівлі людьми. Відсутність фізичних обмежень у кіберпросторі робить недоцільною формування структур

ієрархічного типу. За самою своєю природою кіберпростір є несумісним із ієрархією – він є мережею, елементами якої є інші мережі, основною рисою яких є гнучкість, текучість, відкритість та здатність еволюціонувати. З огляду на це, діяльність у цьому просторі – як легальна, так і нелегальна – не потребує ієрархій.

Організація передбачає наявність відносин, що ґрунтуються на певних принципах. Такі принципи – це, передусім, спільні інтереси, якими для злочинності є отримання прибутку шляхом вчинення злочинів. У випадку кіберзлочинності такі організації можуть бути віртуальними майданчиками взаємодії осіб, зацікавлених у вчиненні певних дій, навіть якщо відносини між ними не є усталеними. Ця взаємодія може включати у себе обмін досвідом, певними навичками, програмними ресурсами та іншою інформацією, а також надання взаємної підтримки.

Слід враховувати, що кіберпростір формує особливе соціальне середовище, яке можливо розглядати як стійку сукупність особистостей, що беруть участь у мережевих процесах, та суспільних відносин, що між ними виникають. Соціальне середовище кіберпростору є вкрай різноплановим, і певна його частина, що поділяє соціально-небезпечні погляди та поширює відповідну субкультуру, може розглядатися як криміногенне середовище [10, С. 321], яке структурується також відповідно до специфіки кіберпростору.

У цьому зв'язку доцільним буде згадати дослідження, проведене Національним науково-дослідним інститутом корпорації РАНД щодо впливу інформаційних технологій на військові операції [11-12]. У дослідженні зроблено висновок про те, що інформаційні технології змінюють обличчя сучасної війни – найбільш ефективним стає використання невеликих підрозділів, що діють відносно автономно. Така стратегія отримала назву «роїння» і розглядається як напрям використання збройних сил, більш перспективний, аніж їх традиційне об'єднання у масивний ударний кулак. «Роїння» характеризується як «структуроване та скоординоване завдання ударів на усіх можливих напрямах та з різних відстаней із використанням множини невеликих розосереджених підрозділів із високим ступенем маневрування». Дослідники РАНД вважають, що сучасні організації у цілому прямують до мережевої моделі, підґрунтям якої є використання можливостей інформаційних технологій координувати діяльність різних об'єктів, не пов'язаних між собою формальними стосунками. Оволодіння цією формою організації дає небачені до цього часу конкурентні переваги. Важливою є і надана дослідниками характеристика сучасних бойових дій як «нелінійних», де сторонами конфлікту є розосереджені перемішані між собою одиниці. Організаційна структура стає скоріше горизонтальною, аніж вертикально-ієрархічною.

Подібна до «роїння» стратегія вже відносно тривалий час (щонайменше з кінця 1990-х років) застосовується транснаціональними організованими злочинними угрупуваннями, що діють у сфері наркобізнесу і є одним із можливих напрямів розвитку кіберзлочинності. З одного боку, її використання дозволяє одночасну організацію численних атак проти одного, що суттєво підвищуватиме їх ефективність. З іншого боку, діяльність правоохоронців із виявлення зловмисників буде значно ускладнена. Окрім цього, можливим є і завдання шкоди фактично необмеженому колу об'єктів. У випадку кіберзлочинності елементами «рою» виступатимуть як індивідууми, так і невеликі за чисельністю групи. Мережа надає їм необмежені можливості координувати свою діяльність незалежно від географічної віддаленості, національних кордонів або правових обмежень.

Виокремлення лідерів таких угрупувань є малоймовірним, оскільки їх члени, як правило, матимуть подібні один до одного ресурси, основним із яких є технічні знання. Наявність відповідних знань дозволяє будь-кому виступати у ролі ініціатора певної злочинної акції, а отже, відігравати роль лідера. Участь у певній групі не є у цьому разі настільки важливою для «кримінальної кар'єри», як це має місце у «традиційній» злочинності. З огляду на це, самі «організації» у такому випадку мають ситуативний характер і створюватимуться під конкретну акцію задля тимчасового об'єднання ресурсів, при цьому одні й ті самі індивідууми та групи входитимуть до декількох більш широких структур. Відповідно, спільна протиправна діяльність у таких групах може істотно відрізнятися від звичайних форм співучасті при вчиненні злочину.

Горизонтальна побудова є природною для кіберпростору, як це видно на прикладі групи «Anonymous». Зрозуміло, що встановлення територіального контролю або монопольного домінування над частиною ринку у такому випадку не є актуальним. Так само мінімальним є вплив на діяльність таких структур і національних кордонів та правових систем або культурних відмінностей, у тому числі і через формування у цьому середовищі власної космополітичної культури. При цьому межа між кримінальними групами та утвореннями «хактивістів» й іншими квазі-соціальними об'єднаннями часто є досить розпливчастою.

Отже, організовані злочинні угруповання, побудовані за мережевим принципом, набувають високої адаптивності до змін у середовищі існування та є стійкими до зовнішніх впливів, що зумовлене низкою чинників:

-мережева структура має гнучке управління (керівні впливи можуть передаватися різними маршрутами, що є оптимальними для почтової ситуації), що забезпечує підвищену швидкість реакції на дії правоохоронних органів;

-відсутність чітко локалізованої структури; функціональна динамічність ускладнює власне правоохоронну діяльність та створення в таких групах оперативних позицій;

-здатність до швидкої зміни складу та перерозподілу ролей робить такі угруповання більш ефективними порівняно з угрупованнями з традиційною ієрархічною структурою в аспекті виживання, оскільки угруповання не припиняє існування внаслідок затримання окремих учасників;

-угруповання з мережевою структурою для вирішення одного й того ж завдання обирають кожного разу різні способи, які є оптимальними в контексті поточної ситуації, що ускладнює викриття протиправних дій правоохоронними органами, оскільки унеможливлює використання стандартних алгоритмів типових оперативних ситуацій та криміналістичних методик [10, С. 323].

Сприятливі умови, що їх забезпечує специфіка кіберпростору маргінальним спільнотам, призводять до появи численних зон спілкування осіб з девіантною поведінкою. Відповідно, зростає кількість інтернет-ресурсів асоціального та навіть екстремістського характеру. Зокрема, зростає число сайтів, що належать організованим злочинним угрупованням, через які вони не лише обмінюються інформацією, алей популяризують свої ідеї. У мережевому просторі формується ринок дитячої порнографії, мережеві можливості використовуються для поширення інформації про місця збуту підконтрольних речовин та рекомендацій щодо їх виготовлення, так само і рекомендацій щодо виготовлення вибухових та отруйних речовин. З використанням глобальної мережі Інтернет також здійснюється торгівля зброєю, реквізитами викрадених кредитних карток. Почастішали випадки популяризації в кіберпросторі відео зйомок реальних сцен насильства тощо. Реальну загрозу інтересам суспільства несе і розміщення в Інтернеті шкідливих програм, пристроїв «комп'ютерного зламу», методичних рекомендацій щодо використання хакерського інструментарію, а також продаж заборонених до обігу спеціальних технічних пристроїв [10, С. 321]

Окреслена вище специфіка кіберзлочинності створюватиме додаткові ускладнення для здійснення правоохоронної діяльності. Аналіз таких структур, виявлення взаємозв'язку між їх елементами вкрай ускладнений, якщо взагалі можливий. У випадку організованих злочинних угрупувань «традиційної» сфери, наприклад, наркобізнесу, трансформація у напрямі мережевих структур, значною мірою була викликана саме потребою уникати переслідування з боку правоохоронних органів, підвищення «живучості» організацій. Очевидно, що у кіберпросторі цей чинник матиме не менш важливе значення. Можливості використання людських джерел інформації також є вкрай обмеженими, оскільки учасники таких «угруповань» навряд чи володіють скільки-небудь достовірними даними щодо своїх подільників. Значною мірою індивідуальний «почерк» злочинців, та, відповідно, можливості щодо їх ідентифікації нівелюються застосуванням стандартизованих знарядь вчинення злочинів (програмного забезпечення). Крім того, сліди злочину зазвичай розпорошуються у значній кількості об'єктів (комп'ютерні системи жертви, злочинця, провайдера, проміжні мережеві вузли тощо) при відсутності чітко вираженого місця вчинення злочину.

З іншого боку, переформатування структури організованої злочинності, у тому числі у кіберпросторі, надає нових можливостей і для правоохоронних органів. Зокрема, космополітичність таких об'єднань, їх відкритість та часткова анонімність може полегшити введення до їх складу співробітників правоохоронних органів, що володіють спеціальними знаннями та навичками. Фактично ж проведення заходів з протидії та викриття злочинів у кіберпросторі ґрунтується на оперативному пошуку, в т. ч. оперативному моніторингу. При цьому важлива для протидії злочинності інформація концентрується на мережевих криміногенних об'єктах у вигляді: слідів протиправної діяльності; повідомлень осіб, що володіють інформацією про обставини підготовки та вчинення злочинів; посилань на мережеві адреси розміщення матеріалів, що заборонені для поширення. Крім того, оперативно-вагома інформація наявна у комунікаційних актах представників криміногенного середовища, що реалізуються через повідомлення електронної пошти, сеанси прямого зв'язку, умовні сигнали або зашифровані повідомлення, що розміщуються на загальновідомих мережених інформаційних ресурсах, персональних профілях у соціальних мережах тощо [10, С. 325-336]

Висновки

Узагальнюючи викладене, можна дійти висновку про те, що ані власна самоідентифікація, ані тривале членство надалі не можуть бути характерними для злочинних структур, що діятимуть у кіберпросторі. Такі структури формуватимуться під конкретну операцію і матимуть плинну, відкриту та мінливу природу. Єдиною передумовою членства у таких структурах є особисте бажання, намір на вчинення протиправних діянь, а також наявність відповідних навичок. Кіберпростір дає додаткові можливості для приховування особистості злочинців, що, відповідно, робить менш важливою особисту довіру між членами організації, однак підвищує значення збереження конфіденційності інформації та заходів її захисту від

несанкціонованого доступу. Використання телекомунікаційних технологій для забезпечення незаконних операцій «традиційними» організованими злочинними угрупуваннями також є одним із чинників їх переформатування відповідно до мережевої моделі, як це має місце і в легальних транснаціональних корпораціях.

Специфіка природи злочинних організацій, що діють у кіберпросторі, ставить додаткові вимоги перед правоохоронними органами, але й створює додаткові можливості, що можуть використовуватися і для організації протидії «традиційній» злочинності, що використовує комп'ютерні технології для здійснення протиправних акцій.

Стратегія «роїння» як напрям ведення військового протистояння може розповсюджуватися і на сферу протидії організованій злочинності, причому не лише у контексті діяльності кримінальних структур, але й в організації роботи правоохоронних органів. Це, у свою чергу, потребує не лише розробки нової парадигми правоохоронної діяльності, а й ставить нові вимоги до рівня підготовки співробітників компетентних органів, що повинні мати відповідні навички автономної діяльності, прийняття самостійних рішень та швидкого реагування на зміни у обстановці.

Література: ***1.*** *Про Концепцію державної політики у сфері боротьби з організованою злочинністю: Указ Президента України від 21 жовтня 2011 року №1000/2011. – Урядовий кур'єр від 29.10.2011 — № 201.* ***2.*** *Закону України «Про організаційно-правові основи боротьби з організованою злочинністю». [Електронний ресурс]. – Режим доступу: http://www.rada.com.ua* ***3.*** *Кримінальний кодекс України.[Електронний ресурс]. – Режим доступу: http://www.rada.com.ua* ***4.*** *Конвенція ООН проти транснаціональної організованої злочинності. 2000 р.[Електронний ресурс]. – Режим доступу: http://www.rada.com.ua* ***5.*** *McClure G. The Role of Interpol in Fighting Organized Crime /481 International Criminal Police Review (2000) – Interpol. [Електронний ресурс]. – Режим доступу: http://www.interpol.int/Public/Publications/ICPR/ICPR481_1.asp* ***6.*** *Family Cities, AmericanMafia.com [Електронний ресурс]. – Режим доступу: http://www.americanmafia.com/ 26_Family_Cities.html* ***7.*** *Castelli B. The Globalization of the Drug Trade. – Apr. 1999. [Електронний ресурс]. – Режим доступу: http://www.unesco.org/most/sourdren.pdf* ***8.*** *Shelley L., Director, Center for Transnational Organized Crime and Corruption, Testimony Before the House Committee on International Relations. – October 1, 1997. [Електронний ресурс]. – Режим доступу: http://www.fas.org/irp/congress/1997_hr/h971001ls.htm.* ***9.*** *Brenner S. W. Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships / North Carolina Journal of Law & Technology. –Volume 4, Issue 1: Fall 2002. – 50 p. [Електронний ресурс]. – Режим доступу: http://www.rand.org/publications/MR/MR880.* ***10.*** *Теория оперативно-розыскной деятельности: Учебник. 2-е изд., перераб. и доп./Под ред. К. К. Горяинова, В. С. Овчинского, Г. К. Синилова. – М.: ИНФРА-М, 2012. – Х., 690 с.* ***11.*** *Arquilla J. In Athena's Camp: Preparing for Conflict in the Information Age/ J.Arquilla, D. Ronfeldt. – 1997.* ***12.*** *Arquilla J. David Ronfeldt, Swarming and the Future of Conflict / J.Arquilla, D. Ronfeldt. – 2000. [Електронний ресурс]. – Режим доступу: http://www.rand.org/publications/DB/DB311.pdf*

УДК 35.078:342.738

ДЕЯКІ ПРАКТИЧНІ АСПЕКТИ РЕАЛІЗАЦІЇ ЗАХОДІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПІД ЧАС ЇХ ОБРОБКИ В ІНФОРМАЦІЙНИХ (АВТОМАТИЗОВАНИХ) СИСТЕМАХ

Олексій Мервінський, *Микола Щербак

*Державна служба захисту персональних даних, *ТОВ «Data Protection Development»*

Анотація **В статті обгрунтовуються вимоги щодо системи захисту персональних даних (ПД) в Україні такого рівня, щоб не існувало протиріччя між положеннями європейських директив і вимогами правових і нормативних документів системи ТЗІ України.**

Аннотация **В статье обосновываются требования относительно системы защиты персональных даннях (ПД) в Украине такого уровня, чтобы не существовало противоречия между положениями европейских директив и требованиями правовых и нормативных документов системы ТЗИ Украины.**

Summary **In the article requirements are studied in relation to the system of the personal data protection (PD) in Ukraine in such way that there were not be any contradiction was not between positions of europian directives and requirements of legal documents of Ukraine and native normative documents of the system TID**.

Ключові слова: кримінологічна **безпека, злочинність, причинність, управління ризиками, оцінювання ризиків.**