ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

В. Є. Ткаліч

ОРГАНІЗАЦІЙНО-ТАКТИЧНІ ЗАХОДИ ЩОДО ПРОТИДІЇ ОРГАНІЗОВАНИМ ЗЛОЧИННИМ УГРУПОВАННЯМ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ

Монографія

Одеса
ОДУВС
2009

УДК 343.85:343.97.000.347.83
ББК 67.518.4я9
Т48

Рекондовано до видання рішеннім Вченої ради Одеського державного університету внутрішніх справ
Протокол № 2 від 23 жовтня 2009 року.

Автор: В.Є. Ткаліч – кандидат юридичних наук, доцент кафедри криміналістики факультету з підготовки фахівців для підрозділів слідства та дізнання Одеського державного університету внутрішніх справ

Рецензенти:

- В.Д. Берназ – доктор юридичних наук, професор професор кафедри криміналістики факультету з підготовки фахівців для підрозділів слідства та дізнання Одеського державного університету внутрішніх справ;
- Ю.П. Аленін - доктор юридичних наук, професор завідувач кафедри кримінального процесу Одеської національної юридичної академії

Ткаліч, Віталій Євгенович

Т48 Організаційно-тактичні заходи щодо протидії організованим злочинним угрупованням з використанням інформаційних технологій і засобів масової інформації : монографія – Одеса : ОДУВС, 2009. - 196 с.

Монографія присвячена комплексному аналізу теоретичних та практичних засад використання інформаційних технологій і ЗМІ при розкритті і розслідуванні злочинів, вчинених ОЗУ у діяльності оперативних та слідчих підрозділів ОВС. Розроблені рекомендації щодо удосконалення правового забезпечення тактики використання інформаційних технологій органами дізнання та досудового слідства; покращення забезпечення конфіденційності даних досудового слідства; особливостей виявлення ознак злочинної діяльності з використання інформаційних технологій та ЗМІ; положень тактики протидії злочинній діяльності ОЗУ в умовах адаптації правоохоронних органів до нових соціальних відносин, що змінюються під впливом сучасних науково-технічних досягнень у інформаційній сфері.

УДК 343.85:343.97.000.347.83
ББК 67.518.4я9

©В.Є. Ткаліч, 2009

Наукове видання

Ткаліч Віталій Євгенович

ОРГАНІЗАЦІЙНО-ТАКТИЧНІ ЗАХОДИ ЩОДО ПРОТИДІЇ ОРГАНІЗОВАНИМ ЗЛОЧИННИМ УГРУПОВАННЯМ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ

Монографія

Підписано до друку 22.12.2009.Формат 60х84/16. Папір офсетний.
Гарнітура «Times New Roman» Друк цифровий. Ум. друк .арк. 10,98.
Наклад 300 прим. Зам. № 126
Видавець і виготовлювач ОДУВС
м. Одеса, вул. Успенська, 1
Свідоцтво суб'єкта видавничої справи ДК № 3507 від 25.06.2009 р.
тел. 0487024884; 0949547884 email – *ndrvv1@gmail.com*

МВС України, 1993. – 120 с.

450 Стеценко Ю.В. Особливості порушення кримінальної справи за повідомленнями засобів масової інформації /Ю.В. Стеценко // Держава і право. – 2003. - Випуск 20. – с. 404-411

451. Судебная дигитология - современный взгляд на содержание криминалистической техники / Михаил Алексеевич Романенко // Вестник Омского университета. - Омск : Изд-во ОмГУ, 2007г. № 1

452 Інформатизація, право, управління (організаційно-правові питання): [Монографія] / Р. А. Калюжний, О. Д. Крупчан, В. Д. Гавловський та інші. - К.: Ін-Юре, 2002. - с. 11.

453 Овчинский С.С. Оперативно-розыскная информация / С.С. Овчинский [Под ред. А.С. Овчинского и В.С. Овчинского]. – М.: ИНФРА-М, 2000. – 367 с.

454 Денісова О. О. Інформаційні системи і технології в юридичній діяльності: Навч. посібник. /О. О. Денісова - К.: КНЕУ, 2003. - 315 с.

455 Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві Закон України від 23 грудня 1993 року / Відомості Верховної Ради України. – 1994. - №11.

456 Васильев В.Л. Юридическая психология. / В.Л Васильев. - С.Пб.: ПитерКом, 1998. - с. 387-388.

457 Самонов А.П. Психология преступных групп. /А.П. Самонов - Пермь, 1991. - с. 17.

458 Васильев В.Л. Юридическая психология. /В.Л. Васильев - С.Пб.: ПитерКом, 1998. - с. 386.

459 Овчинский С.С. Оперативно-розыскная информация / С.С. Овчинский [Под ред. А.С. Овчинского]. - М.: ИНФРА, 2000. - с. 59.

460 Основы борьбы с организованной преступностью. - М.: ИНФРА, 1996. - с. 334.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АБД – автоматизований банк даних
АВН - автоматичний визначник номера
АДІС - автоматизовані дактилоскопічні ідентифікаційні системи
АІПС - автоматизовані інформаційно-пошукові системи
АРМ –автоматизоване робоче місце
ГІС - геоінформаційні системи
ГУМВСТ – Головне управління міністерства внутрішніх справ на транспорті
ДАІ – державна автомобільна інспекція
Держкомстат – Державний комітет статистики
ДПА – Державна податкова адміністрація
ДСБЕЗ – Державна служба боротьби з економічними злочинами
ЕОМ – електронно-обчислювальна машина
ЕЦП – електронний цифровий підпис
ЄС – Європейський союз
ЗЗТМ — засоби захищеної телекомунікаційної мережі
ЗІП — комплект запасних інструментів та приладів
ЗМІ – засоби масової інформації
ЗМК – засоби масової комунікації
ЗУСП — засоби управління системою перехоплення телекомунікації
ІБД - інтегрований банк даних
КК – кримінальний кодекс
КМУ – Кабінет Міністрів України
КПК – кримінально-процесуальний кодекс
КРІС – криміналістична регістраційно-інформаційна система
МЗС - Міністерство закордонних справ
МІІАС - міжвідомча інтегрована інформаційно-аналітична система
МК - мережний комплект
НБУ – Національний банк України
НТР – науково-технічна революція
ОВС – органи внутрішніх справ
ОЗГ –організована злочинна група
ОЗУ – організоване злочинне угруповання;
ООН – Організація Об'єднаних Націй
ОРД – оперативно-розшукова діяльність
ПЕОМ – персональна електронно-обчислювальна машина
ПЗ — програмне забезпечення

р. № 5030/Бч – К., 1997. – 3 с.

436 Закон України від 4 лютого 1998 р. «Про концепцію Національної програми інформатизації» // Юрид. вісн. України. – 1998. - №18

437 Організаційно-тактичні основи діяльності оперативних підрозділів у сфері високих технологій / [Методичні рекомендації. Донецький юридичний інститут МВС України] – Донецьк., 2004. - 28с.

438 Корнієнко М.В. Сучасні засади протидії спеціалізованих підрозділів ОВС організованій злочинності: [Монографія]. /М.В.Корнієнко– К.: Національна академія внутрішніх справ України, 2003.- 676 с.

439 Стояновский М.В.. Классификация способов сокрытия преступной деятельности /Стояновский М.В., Трухачев В.В. // Криминалистические средства и методы исследования преступлений / [Под ред. О.Я. Баева]. – Воронеж, 1999. – Вып. 10. – с. 25–38.

440 Бахин В.П. Особенности расследования заказных убийств: [Лекция]. /В.П. Бахин – Симферополь, 1999. – 48 с.

441 Лапин Е. Все – на дактилоскопирование? /Е.Лапин // Юстиция. – 1996. – № 9.

442 Айдинян Р. Функциональная теория организации и организованная преступность /Р.Айдинян, Я.Глинский / Изучение организованной преступности: российско-американский диалог. – М., 1997. - с. 112

443 Вехов В.Б. Криминалистические значимые сведения о компьютерных сетях и образующихся в них дорожках электронно-цифровых следов / [Информационное обеспечение раскрытия и расследования преступлений. Специальный выпуск №5.] [В 3-х частях. Часть 1] / В.Б.Вехов. Луганск, 2008. С. 78-85.

444 Федеральная программа по усилению борьбы с преступностью на 1994–1995 гг. / Собрание законодательства РФ. – 1994. – № 5. – ст. 403.

445 Стратегія і тактика боротьби з організованою злочинністю та корупцією / [Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при Координаційному комітеті по боротьбі з корупцією і організованою злочинністю при Президентові України]. – Київ, 1998. – Вип. 3. – 45 с.

446 Снігерьов О.П.. Попередження та розкриття умисних убивств. /Снігерьов О.П., Колошко І.М., Матвійчук В.В., Васеха Т.Е. – К., 1998.- с.32

447 Соціально-правовые аспекты терроризма: [Монография], [Под ред.. С.В. Кивалова, В.Н. Дремина]. - Одеса: Фенікс, 2003 – 232 с.

448 Правове регулювання інформаційної діяльності в Україні : станом на 1 січня 2001 р.: [упоряд. С.Е. Демський; відп. ред. С.П. Павлюк.]. – К.: Юрінком Інтер, 2001. – 688 с.

449 Про оперативно-розшукову діяльність Закон України [Наук.-практ. комент.] / Я.Ю.Кондратьєв, І.В.Козаченко, І.Ф. Обушевський та ін.: РВВ

424 Лисенко В.В. Проблеми виявлення злочинів, пов'язаних з несплатою податків /В.В. Лисенко, О.С.Задорожний // Науковий вісник Національної академії державної податкової служби України. – 2007. – № 2(37). – с. 212-219.

425 Щербаковський М.Г. Криміналістична тактика. Навчальний посібник з підготовки до практичних занять з криміналістики. / М.Г.Щербаковський, Е.О. Разумов , А.Е. Волкова. – Суми: Видавничо-виробниче підприємство „Мрія-1" ТОВ, 2008. – 256 с.

426 Григорьев В.Н. Проблемы развития средств обнаружения признаков преступления // Пути совершенствования деятельности следственных аппаратов органов внутренних дел: [Сборник науч. трудов]. – Ташкент, Ташк. высш. школа МВД СССР, 1987. – с. 40-52.

427 Выявление преступлений как элемент криминалистики: Межвузовский науч. сб. [Проблемы программирования, организации и информационного обеспечения предварительного следствия] Башк. ун-т. – Уфа, 1989. – с. 146-150.

428 Джинчарадзе Н.Г. Інформаційна культура. [Навч. посібник]. /Н.Г. Джинчарадзе – К., 1999. – 147 с.

429 Овчинский С.С. Оперативно-розыскная информация / С.С. Овчинский – М.: [Под ред. Овчинского А.С. и Овчинского В.С]. ИНФРА – М., 2000. – 367 с.

430 Карпов Н.С. Злочинна діяльність: [Монографія]. /Н.С. Карпов – К.: вид-во Семенко Сергія. 2004. – 310 с.

431 Євдокіменко С.В. Злочинна діяльність: сутність та криміналістичні аспекти боротьби з нею: автореферат дис. ... канд. юрид. наук 12.00.09 / С.В. Євдокіменко НАВСУ. - Київ, 2002. – 17 с.

432 Леженіна О.І. Концептуальні засади інформаційного забезпечення міжнародної діяльності органів внутрішніх справ України в боротьбі з торгівлею людьми / О.І. Леженіна // Вісник ЛАВС МВС ім. 10-річчя незалежності України. – Вип. 2. – Луганськ, 2003. – с. 228-233.

433 Обертинський О. Комп'ютер як засіб та об'єкт злочину / Іменем закону. – 2005. – 21-27 січня.

434 Біленчук П. Д., Кофанов А. В., Кобилянський О. Л.. Антитерористичні сили, засоби, технології безпеки: концептуальні основи запобігання та протидії тероризму: навчальний посібник / Біленчук П. Д., Кофанов А. В., Кобилянський О. Л.. // Київський національний ун-т внутрішніх справ. Навчально-науковий ін-т підготовки слідчих і криміналістів; Європейський ун-т управління, безпеки та інформаційно-правових технологій.— К. : ННІПСК КНУВС, 2009. — 46с.

435 Щодо узгодження проекту Тимчасового Положення про створення першої черги міжвідомчої інтегрованої інформаційно-аналітичної системи правоохоронних органів / Вказівка МВС України від 25 вересня 1997

РФ – Російська федерація
СБУ – Служба безпеки України
СПТ - Система перехоплення телекомунікацій
СУ ОМУ ГУМВС – Слідче управління Одеського міського управління Головного управління Міністерства внутрішніх справ
США – Сполучені Штати Америки
ТІАД - технологія інтелектуального аналізу даних
УБНОН – Управління боротьби з незаконним обігом наркотиків
УБОЗ ГУМВС – Управління боротьби з організованою злочинністю Головного управління Міністерства внутрішніх справ
ФБР – Федеральне бюро розслідування
ФРН – Федеративна Республіка Німеччина
ЦК – цивільний кодекс

ВСТУП

Розбудова в Україні інформаційного суспільства породила широкомасштабне застосування високих технологій не тільки у корисних для суспільства цілях, а й використання їх у злочинній діяльності, що призвело до збільшення кількості злочинів, які вчиняються організованими злочинними угрупованнями з використанням інформаційних технологій та засобів масової інформації. Зазначене викликає потребу адаптації правоохоронних органів до нових соціальних відносин, що змінюються під впливом сучасних науково-технічних досягнень в інформаційній сфері та спрямування їх у бажаному для нашої держави напрямку – гармонізації співвідношення інтересів людини, суспільства, держави.

Аналіз досліджуваної проблеми свідчить про те, що працівники слідчих та оперативних підрозділів не завжди готові адекватно реагувати на технологічно високо оснащену групову злочинність. Аналіз стану і динаміки злочинності в нашій державі у сфері високих інформаційних технологій, свідчить про негативну тенденцію збільшення кількості цієї категорії кримінальних діянь. Використовуючи екстраполяцію та враховуючи високий рівень латентності, можливо спрогнозувати подальше зростання кількості даних видів злочинів. Одним зі шляхів оптимізації розкриття та розслідування злочинів, які вчиняються з використанням інформаційних технологій, є провадження досліджень у цьому напрямку з метою озброєння оперативних уповноважених та слідчих новітніми рекомендаціями, підвищення ефективності системи інформаційно-аналітичного забезпечення діяльності правоохоронних органів України при розкритті та розслідуванні злочинів.

Актуальність дослідження проблем використання можливостей інформаційних технологій і засобів масової інформації при розкритті і розслідуванні злочинів, учинених ОЗУ, полягає й у тому, що окремі криміналістичні аспекти розроблені недостатньо.

Про необхідність та можливості використання інформаційних технологій при розслідуванні злочинів відзначається в роботах багатьох учених-криміналістів: Авер'янової Т.В., Бахіна В.П., Бєлкіна Р.С., Берназа В.Д., Гори І.В., Долженкова О.Ф., Дулова А.В., Іщенка А.В., Ієрусалімова І.О., Карпова Н.С., Коновалової В.Е., Кузьмичова В.С., Лисогора В.Г., Лисенка В.В., Лук'янчикова Є.Д., Матусовського Г.А., Овчинського С.С., Ортинського В.Л., Почепцова Г.Г., Салтевського М.В., Стеценка Ю.В., Цимбала П.В., Шепитька В.Ю., Щербаковського М.Г., Яблокова М.П. та інших.

Однак аналіз наукових робіт показує, що в цілому деякі аспекти дослі-

праць. Юридичні і політичні науки. Випуск 8]. /О.О. Пунда - К.: Ін-т держави і права ім. В.М. Корецького НАН України, Спілка юристів України, 2000. - 524 с.

414 Корнелюк В.С. Криминалистическая характеристика автомототранспортных средств и ее использование в следственной практике: автореф. дис.... канд. юрид. наук. / В.С Корнелюк.- Волгоград, 1997. - с. 27.

415 Корнієнко М.В. Сучасні засади протидії спеціалізованих підрозділів ОВС організованій злочинності: [Монографія]. /М.В. Корнієнко – К.: Національна академія внутрішніх справ України, 2003.- 676 с.; Корнієнко М. В. Суспільство і правопорядок: [вид. у 6 т.] [Т. 3 : Протидія організованій злочинності в країнах ЄС та США.] / Корнієнко М. В.— К. : Фонд юрнауки АПС, 2007 — 312 с.

416 Выявление преступлений — начальный этап борьбы с преступностью: [Проблемы оптимизации первоначального этапа расследования преступлений]. - Свердловск, 1988. – с. 25-32.

417 Своевременное обнаружение преступления: понятие, методы и профилактическое значение: [Правовые и организационные вопросы предварительного расследования]. Высшая следственная школа МВД СССР, Вып. 17. - Волгоград, 1977. – с. 19-24.

418 Криминалистика: [Учебник для вузов] / А.Ф. Волынский, Т.В. Аверьянова, И.Л. Александрова и др.; [Под ред. проф. А.Ф. Волынского]. – М.: Закон и право, ЮНИТИ-ДАНА, 1999. – 615 с.

419 Васильев В.Л. Психологические аспекты раскрытия убийств, совершенных в условиях неочевидности / Проблемы раскрытия и расследования преступлений, совершенных в условиях неочевидности/ В.Л. Васильев – Волгоград: ВСШ МВД СССР, 1989. – с. 87-95.

420 Галаган В.І. Проблеми вдосконалення кримінально-процесуальної діяльності органів внутрішніх справ України: [Монографія]. /В.І. Галаган – К.: Національна академія внутрішніх справ України, 2002. – 300 с.

421 Про оперативно-розшукову діяльність Закон України: [Наук.-практ. комент.] / Я.Ю.Кондратьєв, І.В.Козаченко, І.Ф. Обушевський та ін.: РВВ МВС України, 1993. – 120 с.

422 Сущность и понятие оперативно-розыскной деятельности, её основные задачи / А.Н. Гущин, В.А.Колдин, В.В.Лисоволенко, Н.А. Громов // Следователь. – 2004. - № 7 (75). – с. 50-55.

423 Сулейманов Д.И. Концептуальные основы использования информации при раскрытии преступлений: автореф. дис. ... доктора юрид. наук: 12.00.09 / Д.И. Сулейманов КГУ им. Т.Г. Шевченко. – К., 1997. – 45 с.

402 Криминалистика: [Учебник для вузов], [Под ред., проф. Р.С.Белкина]. - М., 2001.- с. 495.

403 Путивка С.Н. Криминалистическое моделирование для реконструкции неочевидных обстоятельств при расследовании дорожно-транспортных происшествий: дис. ... канд.юрид.наук: 12.00.09. /С.Н.Путивка.- Волгоград, 2002. – 188 с.

404 Орлов Ю.Ю. застосування оперативної техніки в оперативно-розшуковій діяльності міліції (теоретичні, правові та організаційно-тактичні проблеми) : автореф. дис. ... канд. юрид. наук: 21.07.04 / Ю.Ю. Орлов. – Київ, КНУВС. 2008. – 35 с.

405 Технічні засоби для здійснення уповноваженими органами оперативно-розшукових заходів у телекомунікаційних мережах загального користування України. Загальні технічні вимоги / Наказ Мінтрансзвязку та СБУ від 11 грудня 2007 року N 1140/882

406 «Про електронні документи та електронний документообіг» Закон України від 22.05.2003 № 851-IV / Відомості Верховної Ради (ВВР), 2003, N 36, ст.275) (Із змінами, внесеними згідно із Законом N 2599-IV (2599-15) від 31.05.2005, ВВР, 2005, N 26, ст.349)

407 Винберг А.И. Криминалистика и доказывание. / А.И.Винберг, Р.С. Белкин - М., 1969. - с.178,181

408.Криминалистика: [Учеб. для вузов], [Под ред. Р.С. Белкина]. М.,- 1999. - 945 с.; Криминалистика: [Учебник], [Под ред. Т.А.Седовой, А.А. Эксархопуло]. СПб., - 2001. - 368 с.

409 Дулов А.В. Судебная психология. /А.В. Дулов – Минск: Вышэйшая шк., 1975. – 462 с.

410 Лукашевич В.Г. Тактика общения следователя с участниками отдельных следственных действий: [Учеб. пособие]. / В.Г. Лукашевич – К.: НИиРИО КВШ МВД СССР, 1989. – 88 с.

411 Тимошенко П.Ю.. Теория и практика использования следов памяти (идеальных отображений) в расследовании преступлений. / П.Ю.Тимошенко, М.В.Салтевский, Ю.Ф.Жариков – К., Типография МВД Украины, 1991. – 88 с.

412 Гуляев П.И. Исследование эмоционального состояния человека в процессе производства следственного действия / П.И.Гуляев, И.Е. Быховский / Криминалистика и судебная экспертиза.– К., 1972. – Вып. 9. – с. 103–109.

413 Пунда О.О. Проблеми застосування науково-технічних засобів захисником у кримінальному процесі: [Держава і право: Збірник наукових

джувалися фрагментарно. Це стосується, насамперед, тенденцій щодо активного використання інформаційних технологій і ЗМІ організованими злочинними угрупованнями для вчинення злочинів; напрямів використання інформаційних технологій при розслідуванні злочинів; розуміння тенденцій впливу сучасних інформаційних технологій на діяльність правоохоронних органів загалом і досудового слідства зокрема; необхідності постійного вдосконалення нормативно-правової бази щодо суб'єктів інформаційної діяльності, змісту тактико-криміналістичних аспектів інформаційного супроводження розслідування злочинів. Низка питань зазначеної наукової проблеми залишається дискусійною.

Необхідність поглиблення наукових досліджень проблем використання можливостей інформаційних технологій при розслідуванні злочинів набуває актуальності також у зв'язку з постійним оновленням технічних можливостей інформаційного забезпечення життєдіяльності суспільства та виникненням нових інформаційних технологій. На жаль, організовані злочинні угруповання нерідко випереджають правоохоронні органи щодо впровадження новітніх науково-технічних досягнень у злочину діяльність, із протидії розкриттю та розслідуванню злочинів. Аналіз спеціальної літератури та практики розкриття й розслідування злочинів, які вчиняються ОЗУ, свідчить, що існує низка проблем, пов'язаних із використанням інформаційних технологій і засобів масової інформації в оптимізації тактики боротьби із цим видом кримінальних проявів.

Зазначені тенденції поширення новітніх досягнень науки, запізнення як теорії, так і практики з теоретичними та прикладними розробками проблеми, позначається на якості розкриття та розслідування цих злочинів. Необхідність постійного поглибленого вивчення питань використання інформаційних технологій і засобів масової інформації при розкритті та розслідуванні злочинів, учинених організованими злочинними угрупованнями, а також потреба в удосконаленні правоохоронної діяльності і зумовили вибір теми дослідження.

РОЗДІЛ 1
ЗАГАЛЬНІ ПОЛОЖЕННЯ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ ПРИ РОЗКРИТТІ І РОЗСЛІДУВАННІ ЗЛОЧИНІВ, УЧИНЕНИХ ОРГАНІЗОВАНИМИ ЗЛОЧИННИМИ УГРУПОВАННЯМИ

1.1. Поняття, види, значення інформаційних технологій, стан та тенденції використання при розкритті та розслідуванні злочинів, учинених організованими злочинними угрупованнями

Технологія набула значення могутнього символу принаймні із часів Ф. Бекона. У XVIII й частково в XIX століттях технологія обов'язково пов'язувалася з вірою в прогрес. Саме про їхній тісний зв'язок із розквітаючим капіталізмом, який зростаючими темпами вимагав нових технологій як засобу для підтримки й підвищення рівня прибутку, йшлося головним чином у вченнях Бекона, Макіавеллі [1, с.362-380].

У звичайному розумінні технологія — це комплекс наукових і інженерних знань, реалізованих у прийомах праці, наборах матеріальних, технічних, енергетичних, трудових факторів виробництва, способах їх з'єднання для створення продукту або послуги, що відповідають певним вимогам. Тому технологія нерозривно пов'язана з машинізацією виробничого або невиробничого, насамперед управлінського процесу. Управлінські технології ґрунтуються на застосуванні комп'ютерів і телекомунікаційної техніки [2, с.5].

Під технологією в англосаксонській термінології розуміється «прикладне знання». За слов'янською інженерною традицією технологія розглядається як сукупність методів обробки, виготовлення, зміни стану чи властивості, форми сировини, матеріалів у процесі виробництва. У сучасній інтерпретації технологія — це сукупність виробничих процесів, науково-технічних і професійних знань, методів, засобів виробництва, нової техніки, які забезпечують перетворення природної речовини в продукти промислового і побутового використання. Існують і інші підходи до тлумачення технології [83]. У радянському енциклопедичному словнику технологія - це «сукупність методів обробки, виготовлення, зміни стану, властивостей, форми сировини, матеріалу або напівфабрикату, здійснюваних у процесі виробництва продукції» [3, с. 1338]. У словнику російської мови

університет внутрішніх справ, - 2008.- 44 с.

393 Денісова О. О. Інформаційні системи і технології в юридичній діяльності: [Навч. посібник]. /О. О. Денісова - К.: КНЕУ, 2003. — 315 с.

394 Деятельность экспертно-криминалистических подразделений органов внутренних дел по применению экспертно-криминалистических методов и средств в раскрытии и расследовании преступлений: [Учеб. пособие] / В.А. Ивашков, М.И. Овсянников, Л.И. Слепнева, В.А. Снетков. – М.: ЭКЦ МВД РФ, 1996. – 104 с.

395 Про авторське право і суміжні права: Закон України від 23 грудня 1993 р. / Відомості Верховної Ради України. – 1994. – № 13. – Ст. 64.

396 Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних: Постанова Кабінету Міністрів України № 121 від 4 лютого 1998 р. / Офіційний вісник України. – 1998. – № 5. – С. 52.

397 Про організаційні заходи щодо функціонування системи державних закупівель: Постанова Кабінету Міністрів України № 1469 від 27 вересня 2000 р. / Офіційний вісник України. – 2000. – № 39. – С. 57.

398 «Коллекция компромата» [Електронний ресурс] Режим доступу: Compromat.ru; Интернет издания lenta.ru; gazeta.ru та інш.

399 Лисенко В.В. Взаємодія окремих підрозділів податкової служби при проведенні перевірок діяльності суб'єктів підприємництва /В.В. Лисенко // Науковий вісник Академії державної податкової служби України. – 2001. – № 1 (11). – С. 152–158.

400. Выявление и пресечение незаконного оборота наркотиков: справочник сотрудника органов наркоконтроля / С.Д. Демчук, И.С. Поликарпов, С.Г. Терещенко, В.А. Фадеев; [Под общей ред. С.Г. Терещенко]. - СПб.: Специальная Литература, 2006. с. 256.

401.См. детальніше: Мироненко В.А., Штаб Т.А. Перспективы использования дистанционной макрофотографии в криминалистической технике // Актуальные проблемы борьбы с преступностью в Дальневосточном федеральном округе: Сб. мат. Всерос. науч.-практ. конф. В 2-х ч. / Под ред. Е.П. Кима. - Хабаровск: Дальневосточный юрид. институт МВД России, 2008. Ч. 2. С. 519-524; Шошин СВ. Некоторые проблемы использования возможностей мониторинга земной поверхности и окружающей среды в целях раскрытия и расследования тяжких преступлений // Современные проблемы применения новых технологий в раскрытии и расследовании преступлений: Мат. Всероссийск. науч.-практ. конф. - Калининград, 2006. С. 188-192.

блеми протидії нелегальній економіці засобами оперативно-розшукової діяльності: Автореф. дис. ...докт. юрид. наук:12.00.09 / В.Л. Ортинський, НУВС. – Харків, 2004. – 36 с.

384 Ткаліч В.Є. Інформаційне забезпечення діяльності щодо розкриття і розслідування злочинів /В.Є.Ткаліч // Південноукраїнський правничий часопис. – 2008, - №.2 (т). – с. 145-150

385 Кондратьєв Я.Ю. Теоретичні, правові та оперативно-тактичні щасади запобігання злочинам оперативними підрозділами кримінальної міліції: [Монографія]. /Я.Ю. Кондратьєв – К.: Нац. Акад.. внутр. Справ України, 2004. – 444 с.

386 Ієрусалімов І.О. Інформаційне забезпечення використання науково-технічних досягнень в слідчій діяльності: авч. посіб./ І.О.Ієрусалімов, О.О.Алексєєв - К.: світ, 2001.- с. 33.

387 Журавльов В.Ю. Інформаційне забезпечення оперативно-розшукової діяльності спеціальних підрозділів по боротьбі з організованою злочинністю: автореф. дис. ...канд. юрид. наук :21.07.04 / В.Ю. Журавльов– Харків, НУВС. 2002. – 17 с.

388 Про затвердження інструкції з організації роботи, взаємодії органів внутрішніх справ та галузеви служб у виявленні, постановці на облік, документуванні та знешкодженні організованих злочинних груп та злочинних організацій, їх лідерів, активних учасників та оперативного супроводження порушених відносно них кримінальних справ / Наказ МВС України від 14.07.2002 р. № 703

389 Кондратьєв Я.Ю. Теоретичні, правові та оперативно-тактичні щасади запобігання злочинам оперативними підрозділами кримінальної міліції: [Монографія]. / Я.Ю. Кондратьєв– К.: Нац. Акад.. внутр. Справ України, 2004. – 444 с.

390 Ортинський В.Л. Протидія нелегальній економіці засобами оперативно-розшукової діяльності: [Монографія]. / В.Л.Ортинський. – Львів: ЛЮІ, 2004. - 436 с.

391 Долженков О.Ф. Інновації – чинник оптимізації оперативно-розшукової діяльності. Актуальні проблем ОРД / О.Ф. Долженков // Вісник ЛАВС МВС. Спеціальний випуск №2 - 2003. – Луганськ: РВВ ЛАВС, 2003, - 74 с.

392 Використання в діяльності чергових частин ОВС новітніх технологій, спрямованих на захист прав і законних інтересів громадян: [Методичні рекомендації] [За заг. ред.. канд.. юрид. наук, доц.. Калаянова Д.П.] / Д.П. Калаянов В.Є. Ткаліч - Одеса: Одеській державний

технологія трактується, як сукупність виробничих процесів у певній галузі виробництва, а також науковий опис способів виробництва [4, с.169]. У новому тлумачному словнику української мови „технологія” визначається, як „сукупність знань, відомостей про послідовність окремих виробничих операцій...” [5, с.529]. Можна виділити кілька різних підходів до визначення поняття «технологія»: операційний – набір послідовно розташованих операцій для одержання відповідного результату; продуктовий – спосіб перекладу вихідної сировини (продукту) з одного стану в інший й комплексний підхід - єдність науково-технічних ідей і матеріальних форм їхнього втілення [6 , с.137]. В.А. Образцов один із перших запровадив термін «технологія» у криміналістиці – «наука про технологію й засоби практичного слідознавства (пошуково-пізнавальної діяльності) у кримінальному судочинстві» [7]. У широкому розумінні технологія визначається як система наукових положень заснованих на них практичних рекомендацій з використання певних засобів за допомогою конкретних методів у процесі цілеспрямованої діяльності для підвищення її ефективності. Поняття технології у вузькому змісті можна сформулювати як систему наукових положень і заснованих на них рекомендацій із практичного використання технічних засобів у процесі цілеспрямованої діяльності для підвищення її ефективності. Під інформаційними технологіями розуміють систему наукових положень і заснованих на них рекомендацій із практичного використання технічних засобів у процесі цілеспрямованої діяльності по пошуку, збору, зберіганню, обробці, поданню й поширенню інформації для підвищення ефективності даної діяльності [8 , с. 136-146]. У російському законодавстві інформаційні технології визначені як процеси, методи пошуку, збору, зберігання, обробки, подання, поширення інформації й способи здійснення таких процесів і методів [9]. Закон України «Про Національну програму інформатизації» від 4 лютого 1998 р. визначає інформаційну технологію як цілеспрямовану організовану сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування [10].

В останні роки термін «технологія» широко застосовується в криміналістиці й не тільки в тих випадках, коли мова йде про виробничі технологічні процеси, технологічні експертизи або технологію планування. У науковий оборот увійшли такі поняття, як «технологія одержання хабара», «технологічний рівень здійснення злочинів», «технології злочинної діяльності» [11, с. 858, 897].

У підручниках криміналістики окремі параграфи присвячені технології слідчих дій, розглядаються питання технології розслідування злочинів окремих видів. Тобто має місце використання аналогії з переносом змісту поняття з виробничих процесів, на інші види діяльності і зокрема на діяльність посадових осіб з розкриття та розслідування злочинів. Термін технологія може не рівнозначно застосовуватися як у технічній сфері, так і в інших нематеріальних галузях людської діяльності, у тому числі і в ОРД. Таку позицію підтримує більшість вчених юристів і під технологією оперативно-розшукової діяльності – сукупність прийомів та операцій, певним чином здійснюваних у певній послідовності, з яких складається оперативно-розшуковий процес за конкретною справою (матеріалом) оперативного обліку [12, с.256, 549].

Для цих видів діяльності характерно автоматизація документообігу, що також охоплюються терміном «інформаційні технології», це комплекс методів і процедур, за допомогою яких реалізуються функції збирання, передавання, оброблення, зберігання та доведення до користувача інформації в організаційно-управлінських системах з використанням обраного комплексу технічних засобів [13, с.5]. Як справедливо відзначає В.Ю.Федорович, інформаційні технології — це не тільки сукупність технічних засобів автоматизації, обчислювальної техніки, засобів зв'язку [14, с. 48], а як правильно вказував А.Ф.Волинський, - певна система організації, правового регулювання науково-методичного забезпечення їхнього функціонування в специфічних умовах розкриття й розслідування злочинів, що стосовно до криміналістичних завдань охоплюється поняттям — криміналістичного забезпечення [15, с. 291]. Зараз для фіксації й обробки криміналістично значущої інформації усе ширше використовуються сучасні комп'ютерні технології. За визначенням В.В. Бірюкова, "комп'ютерні технології – це сукупність методів і програмно-технічних засобів на базі комп'ютера (ЕОМ), об'єднаних у єдиний технологічний ланцюжок, що забезпечує збирання, обробку, збереження і передачу інформації з метою зниження трудомісткості інформаційних процесів, а також підвищення їх надійності й оперативності" [16, с. 54]. Т.В. Авер'янова і співавтори зазначають: "Інтеграція в криміналістику досягнень природничих і технічних наук, ускладнення технічних засобів, удосконалення і розвиток методик їх застосування нерідко пов'язано зі складними технологічними операціями, тому необхідно говорити вже не тільки про криміналістичну техніку, а й про технологію" [17, с. 131]. "Сучасна технологія – невід'ємний елемент НТР, революціонізуюча сила суспільного виробництва" [18, с. 13, 139-147], - зазначають М.Я. Сегай і В.К.

Феміна, 1996. - 696 с.

373 Правова інформатика: система інформатизація законотворчої, правозастосовчої, правоохоронної, судочинної та право освітньої діяльності в Україні. [Монографія] / В.М Брижко., І.А.Вознюк, В.Д. Гавловський, та інші. [За ред. М.Я. Швеця, Р.А. Калюжного]. – Ужгород: ІВА, 2003. – 168 с.

374 Лисенко В.В. Поняття та зміст криміналістичного забезпечення діяльності податкової міліції / В.В. Лисенко // Науковий вісник Національної академії державної податкової служби України. – 2004. –№2 (24). – с.181-187.

375 Ищенко А.В. Криминалистическая рекомендация как средство обеспечения следственной практики достижениями науки и техники: дис. канд.. юрид. наук.: 12.00.09 / А.В. Ищенко – Киев, 1983. – 260 с.

376 Беляков К.И. Совершенствование информационного обеспечения расследования преступлений на базе АИЛС: автореф. дис.. канд..юрид.. наук. /К.И.Беляков - К. 1993.- 23 с.

377 Галаган В.І. Использование следователем информации на первоначальном этапе расследования : дис.. канд.. юрид.. наук. /В.І. Галаган - К., 1992.- 21с.

378 Карпов Н.С. Использование передового опыта органов внутренних дел по раскрытию и расследованию преступлений в целях совершенствования криминалистической тактики и методики: автореф.. дис.. канд.. юрид.. наук. /Н.С. Карпов - К. 1989.- 22 с.

379 Лукашенко В.Я. Криминалистические средства и методы представления инфомации на предварительном следствии: автореф. дисс… канд.. юрид.. наук. В.Я. Лукашенко – К. 1992.- 20с.

380 Попов Ю.В. Совершенствование информационного обеспечения следственной деятельности органов внутренних дел на основе использования методов информатики: автореф. дис.. канд.. юрид.. наук. /Ю.В.Попов – К. 1989. – 21с.

381 Цымбал П.В. Совершенствование использования научно-технических достижений в расследовании преступлений: дис… канд.. юрид.. наук. /П.В. Цымбал - К., 1992.- 243с.

382 Сулейманов Д.И. Концептуальные основы использования информации при раскрытии преступлений: Дис... доктора юрид. наук: 12.00.09 / Д.И. Сулейманов: Азербайджанский НИИ проблем криминологии, криминалистики и судебных экспертиз. - Баку, 1994. - 343 с.

383 Ортинський В.Л. Теоретичні основи, правові та організаційні про-

тореф. дис. … канд. юрид. наук: 12.00.09. / Н.М. Ахтирська – Харків, 1998. – 16 с.

360 Криміналістика: [Курс лекцій (ч.1)]. / В.П.Бахін, І.В Гора, П.В.Цимбал – Ірпінь: Академія ДПС України, 2002. – 356 с.

361 Криминалистика: [Учебник для вузов] / А.Ф. Волынский, Т.В. Аверьянова, И.Л. Александрова и др.; [Под ред. проф. А.Ф. Волынского]. – М.: Закон и право, ЮНИТИ-ДАНА, 1999. – 615 с.

362 Ткаліч В.Є. Тіньова економіка-актуальна проблема сьогодення / В.Є. Ткаліч // Вісник Одеського інституту внутрішніх справ. - 2002. - №1. - с. 149-155

363 Ткаліч В.Є. Деякі напрями використання інформаційних технологій при розкритті і розслідуванні злочинів / В.Є. Ткаліч // Південноукраїнський правничий часопис. – 2006, №4 (т). - с. 140-144

364 Ларин А.М. Расследование по уголовному делу. Планирование, организация. /А.М Ларин – М.: Юрид. лит., 1970. – 223 с.

365 Яблоков Н.П. Расследование организованной преступной деятельности. /Н.П. Яблоков. – М.: Юристъ, 2002. – 172 с.

366 Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. /Р.С. Белкин – М.: Издательство НОРМА (Издательская группа НОРМА – ИНФРА-М), 2001. – 240 с.

367 Криминалистика: [Учебник для вузов] / А.Ф. Волынский, Т.В. Аверьянова, И.Л. Александрова и др.; [Под ред. проф. А.Ф. Волынского]. – М.: Закон и право, ЮНИТИ-ДАНА, 1999. – 615 с.

368 Бакштановский В.И. Принципы морального выбора. /В.И. Бакштановский. – М., 1974. – 64 с.

369 Хайдуков Н.П. Тактико-психологические основы воздействия следователя на участвующих в деле лиц / Н.П. Хайдуков [Науч. ред. В.В. Козлов]. – Саратов: Изд-во Сарат. ун-та, 1984. – 124 с.

370 Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. /Р.С.Белкин – М.: Издательство НОРМА (Издательская группа НОРМА – ИНФРА-М), 2001. – 240 с.

371 Лисенко В. Використання податковою міліцією автоматизованих інформаційних систем при виявленні і розслідуванні злочинів / В. Лисенко // Науковий вісник Національної академії державної податкової служби України. – 2004. – №1 (23). – с. 223–228.

372 Юридичний словник-довідник. [За ред. Ю.С.Шемшученка]. - К.:

Стринжа. Таким чином, посилання на технології, на нашу думку, так само має знайти закріплення у визначенні науково-технічних засобів.

У спеціальній літературі в останні роки часто вживається поняття нові інформаційні технології як сукупність засобів і методів реалізації інформаційних процесів у різних галузях людської діяльності, тобто способів реалізації інформаційної діяльності людини, що розглядається як інформаційна система. Розділяють традиційні і нові інформаційні технології. Нові інформаційні технології, на відміну від традиційних, передбачають надання не тільки інформаційного продукту, але й і - засобів доступу до нього (засобів пошуку, обробки, подання й т.п.). Ці засоби дозволяють користувачеві не тільки візуально знайомитися зі змістом комп'ютерних файлів, у яких втілений інформаційний продукт, але й оперативно одержувати інформацію в обсязі й форматі, які адекватні (релевантні) саме його потребам.

Подібні можливості зв'язуються з поняттям інформаційної послуги. У широкому змісті інформаційна послуга складається в наданні користувачеві інформаційних продуктів. У вузькому змісті під інформаційними послугами розуміють послуги, одержувані за допомогою нових інформаційних технологій. Інформаційні технології на основі використання засобів комп'ютерної техніки називають не тільки новими [19, с.7], а і сучасними [20], високими [21], хоча спочатку в юридичній і спеціальній літературі їх називали комп'ютерними технологіями. Нові інформаційні технології - це узагальнене поняття, що стосується не тільки комп'ютерних технологій, але й технологій в галузі кіно, радіо, телебачення, зв'язку й т.ін., де комп'ютерна техніка має не головне, а допоміжне значення. Інформаційні технології тісно пов'язані з інформаційними системами, які є для неї основним середовищем.

Основна мета інформаційної технології - у результаті цілеспрямованих дій по переробці первинної інформації одержати необхідну для користувача інформацію, а основна мета інформаційної системи - організація зберігання й передачі інформації.

Таким чином, інформаційна технологія є більше ємним поняттям, що відображає сучасне уявлення про процеси перетворення інформації в інформаційному суспільстві. Інформаційні технології сьогодні мають винятково важливу роль у забезпеченні інформаційної взаємодії між людьми, а також у системах підготовки й поширення масової інформації. Ці засоби швидко асимілюються культурою нашого суспільства, тому що вони не тільки створюють більші зручності, але знімають багато виробничих, соціальних і побутових проблем, які викликані процесами глобалізації й інтеграції світового співтовариства, розширенням внутрішніх і міжнарод-

них економічних і культурних зв'язків.

На нашу думку, під інформаційними технологіями слід розуміти сукупність знань, засобів і методів послідовної реалізації інформаційних процесів за допомогою яких здійснюються за певними правилами функції пошуку, збирання, передавання, оброблення, зберігання інформації та доведення, як до користувача, так і від нього.

Інформаційні технології можуть бути різних видів до найбільш типових можливо віднести: Internet-технології (мережеві); комп'ютерні технології (апаратні засоби, програмне забезпечення); мультімедіамережеві технології, телеконференція, телебачення, системи підтримання прийняття рішень (СППР), виконавчі інформаційні системи (ВІС), видобуток даних - ВД (Data mining), штучний інтелект (ШІ), експертні системи (ЕС), нейронні мережі, генетичні алгоритми, віртуальна реальність, системи підтримки роботи групи, географічні інформаційні системи, імітаційні системи та інші.

Інформаційні технології можна класифікувати:

- за способом реалізації в ІС: традиційні; нові інформаційні технології;
- за ступенем охоплення завдань управління: електронна обробка; автоматизація функцій управління; підтримка прийняття рішень; електронний офіс, експертна підтримка;
- за класом реалізованих технологічних операцій: робота з текстовим редактором; робота з табличним процесором; робота із СКБД (системами керування базами даних); робота з графічними об'єктами; мультимедійні системи; гіпертекстові системи;
- за типом інтерфейсу користувача: пакетні; діалогові; мережні; реального масштабу часу, поділу часу, регламентний, «запит-відповідь» інтерактивний, однопрограмний і багатопрограмний, телеобробки;
- за способом побудови мережі: локальні; багаторівневі; розподілені;
- за предметними сферами, що обслуговуються: бухгалтерський облік; банківська діяльність; податкова діяльність; страхова діяльність; слідча діяльність; оперативно-розшукова діяльність; інші.

Об'єктивні фактори зростання ролі інформації, інформаційних технологій та відносин сприяли тому, що в юриспруденції останніх десятиріч XX ст. з'явилась нова теорія кримінальної інформатики, яка базується на концепціях інформаційного права та права інформаційної технології. Відповідно до понять сучасної кібернетики та інформатики інформаційне право зараз визнає інформацію третім основоположним фактором після матерії та енергії [22, с. 50]. Ця концепція розглядає інформацію і інформаційну сферу як новий економічний, культурний і політичний капітал, який особливо піддається новим формам злочинності, які потребують

– М.: Закон и право, ЮНИТИ-ДАНА, 1999. – 615 с.

346 Український радянський енциклопедичний словник: У 3-х т. [Відп. ред. А.В. Кудрицький.], Т. 1. – К.: Голов. ред. УРЕ, 1986. – 752 с.

347 Бєляков К.І. Інформатизація в Україні: проблеми організаційного, правового та наукового забезпечення. [Монографія]. – К.: КВІЦ. 2008 .- 576 с.:іл.

348 Овчинский С.С. Оперативно-розыскная информация / С.С. Овчинский – М. [Под ред. Овчинского А.С. и Овчинского В.С.]: ИНФРА – М., 2000. – 367 с.

349 Почепцов Г.Г. Теория коммуникации. /Г.Г. Почепцов – М.: "Рефл-бук", К.: "Ваклер" – 2001. – 656 с.

350 Криміналістика: [Курс лекцій (ч.1)]. / В.П.Бахін, І.В Гора, П.В.Цимбал – Ірпінь: Академія ДПС України, 2002. – 356 с.

351 Строков І.В. Правові та моральні засади застосування криміналістичних засобів. [Монографія] / Строков І.В. – К.: Редак.-видавн. центр НАВСУ, 2003. – 325 с.

352 Допустимость тактических приёмов при допросе: [Учебное пособие] / И.Е.Быховский, Ф.В.Глазырин, С.К. Питерцев. – Волгоград, МВД СССР; Высш. следств. Школа. -1989. – 48 с.

353 Возможность использования провокации (побуждения к действиям) как средство выявления и изобличения преступников: материалы международной дистанционной конференции. [Научные труды Академии финансовой полиции Выпуск 2].. – Алматы: Жеты жаргы, 2001. – с. 121-128.

354 Белкин Р.С. Очерки криминалистической тактики: [Учебное пособие]. /Р.С. Белкин – Волгоград: ВСШ МВД РФ, 1993. – 200 с.

355 Криминалистика: [Учеб. для вузов] / И.Ф. Герасимов, Л.Я. Драпкин, Е.П. Ищенко и др.; Под ред. И.Ф. Герасимова, Л.Я. Драпкина. – 2-е изд., перераб. и доп. – М.: Высш. шк., 2000. – 672 с.

356 Ларин А.М. Я – Следователь. /А.М.Ларин – М.: Юрид. лит-ра, 1991. – 192 с.

357 Судебная этика. Некоторые проблемы нравственных начал советского уголовного процесса / Г.Ф.Горский, Л.Д.Кокорев, Д.П..Котов. – Воронеж: Изд-во Воронежского ун-та, 1973. – 271 с.

358 Тактика слідчої діяль-ності: поняття, сутність, зміст / В.П. Бахін, В.С.Кузьмічов, В.К. Весельський / Науковий вісник НАВСУ. – К., 1998. – № 2. – с. 217–225.

359 Ахтирська Н.М. Криміналістична тактика: принципи і функції: ав-

332 Богинский В.Е. Рефлексивное управление при допросе: [Учеб. Пособие]. В.Е. Богинский – Харьков: Харьковский юрид. инст., 1983. – 41 с.

333 Шепитько В.Ю. Теория криминалистической тактики: [Монография]. /В.Ю. Шепитько – Харьков: "Гриф", 2002. – 349 с.

334 Орлов Ю.Ю. Застосування оперативної техніки в оперативно-розшуковій діяльності міліції (теоретичні, правові та організаційно-тактичні проблеми) : автореф. дис. ... канд. юрид. наук 21.07.04 / Ю.Ю. Орлов – Київ, КНУВС. 2008. – 35 с.

335 Порфімович О. Оригінальні методи співпраці правоохоронних органів та ЗМІ в контексті "кримської війни" із криміналітетом /О.Порфімович // Інформаційна сфера як духовне явище: [Збірник]. – К., 1999. – с. 99-104.

336 Сергушев М. Супруги из Винницкой области убивали киевлян, дававших в газету объявления о продаже шуб из натурального меха / М.Сергушев // Факты и комментарии. – 2002. - 2 марта.

337 Криминалистика: Краткая энциклопедия: [Авт. сост. Р.С. Белкин]. [Большая Российская энциклопедия], - М.: 1993. – 111 с.

338 Пацера Н. Сводни пойдут в суд /Н.Пацера // Киевские ведомости. – 2002. - 15 августа.

339 Драпкин Л.Я. Тактические приёмы в структуре следственных действий и тактических операций /Л.Я. Драпкин // Научная информация по вопросам борьбы с преступностью. № 76 (Вопросы криминалистики). – М., 1989. – с. 22-24.

340 Яблоков Н.П. Расследование организованной преступной деятельности. /Н.П. Яблоков – М.: Юристъ, 2002. – 172 с.

341 Бояров В.И. Убийства, совершенные в процессе противостояния организованных преступных группировок (особенности расследования). [Методическое пособие]. /В.И.Бояров – Харьков: Изд-во "Крим Арт", 1997. – 132 с.

342 Криміналістика: [Курс лекцій (ч.1)]. / В.П.Бахін, І.В Гора, П.В. Цимбал – Ірпінь: Академія ДПС України, 2002. – 356 с.

343 Криминалистика: [Учебник для вузов] / А.Ф. Волынский, Т.В. Аверьянова, И.Л. Александрова и др.; [Под ред. проф. А.Ф. Волынского]. – М.: Закон и право, ЮНИТИ-ДАНА, 1999. – 615 с.

344 Яблоков Н.П. Расследование организованной преступной деятельности. /Н.П. Яблоков – М.: Юристъ, 2002. – 172 с.

345 Криминалистика: [Учебник для вузов] / А.Ф. Волынский, Т.В. Аверьянова, И.Л. Александрова и др.; [Под ред. проф. А.Ф. Волынского].

адекватної протидії з боку правоохоронних органів і вимагають від них використання найсучасніших досягнень науки та техніки [23, с. 4-7].

Різноманітність та стабільність видів діяльності людини визначається соціально-економічними потребами суспільства. Вона існувала та розвивалась за законами, що відповідали певному історичному періоду. При цьому на зміст і методи конкретної діяльності впливає декілька факторів, серед яких зумовленість останньої соціально-економічними. Це також і ті матеріально-технічні можливості, які відповідно до досягнутого рівня розвитку використовуються для її здійснення.

Сьогодні у світі визначається тенденція до зростання значимості інформації в суспільних відносинах. Це об'єктивно пов'язано з таким соціальним явищем, як інформатизація – впровадження електронних засобів комунікації на основі комп'ютерних технологій у різні сфери суспільного буття. Інформатизація – сукупність взаємозв'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що мають на меті створити умови для задоволення інформаційних потреб громадян і суспільства завдяки розробці, розвитку й використанню інформаційних систем, мереж, ресурсів та технологій, які базуються на застосуванні сучасної обчислювальної та комунікаційної техніки. Часто термін «інформатизація» вживається разом із терміном «комп'ютеризація», який позначає процес розвитку та впровадження комп'ютерів, що забезпечують автоматизацію інформаційних процесів і технологій у різних сферах людської діяльності [24, с.3, 25].

Інформатизація належить до процесів, що постійно та динамічно розвиваються. Можна констатувати той факт, що інформація стала першоосновою життя сучасного постіндустріального суспільства, предметом і продуктом його діяльності, а процеси її створення, накопичення, обробки, зберігання, пошуку і передачі – інформаційні процеси, у свою чергу, стимулювали прогрес в галузі знарядь її виробництва: електронно-обчислюваної техніки, засобів телекомунікацій і зв'язку. Усе це в цілому входить у поняття визначення нової інформаційної технології, яка є сукупністю методів і засобів реалізації інформаційних процесів у різних галузях людської діяльності, тобто способами реалізації інформаційної діяльності людини, якого так же можна розглядати як інформаційну систему. [26]

Проблемами злочинності у сфері нових інформаційних технологій займались такі вчені, як П.Д. Біленчук, М.С.Вертузаєв, Б.В. Вехов, О.Г. Волеводз, Ю.В. Гаврилін, В.О. Голубєв, О.Ф. Долженков, В.В. Крилов, А.В. Касаткін, В.Є. Козлов, С.С. Овчинський, М.В. Лісогор, В.В. Лисенко, Л. П. Паламарчук, О.І. Мотлях, М.Г. Щербаковський та інші. В різні роки

загальним проблемам застосування засобів спеціальної техніки в ОРД присвячені праці П.П. Артеменка, О.М. Бандурки, Р.С. Бєлкіна, Д.І. Біднякова, Г.М. Бірюкова, О.В. Вишні, В.І. Декшне, І.П. Козаченка та інших.

Окремим напрямам інформаційного забезпечення розслідування злочинів на дисертаційному рівні досліджувалися: теоретичні основи одержання інформації про злочинця з матеріальних джерел на досудовому слідстві (К.В.Скибицький); удосконалення інформаційного забезпечення слідчої діяльності органів внутрішніх справ на основі використання методів інформатики (Ю.В.Попов); криміналістичні методи та засоби подання інформації на досудовому слідстві (В.Я.Лукашенко); використання слідчим інформації на початковому етапі розслідування (В.І. Галаган); удосконалення інформаційного забезпечення розслідування злочинів на базі АІПС (К.І. Бєляков); інформаційне забезпечення використання науково-технічних досягнень у розслідуванні злочинів (І.О. Ієрусалимов 1996); концептуальні основи використання інформації при розкритті злочинів (Д.І. Сулейманов); аналіз методологічних і правових проблем інформаційного забезпечення розслідування злочинів (Є.Д. Лук'янчиков); аналіз науково-методичних засад використання засобів масової інформації при розслідуванні злочинів (Ю.В. Стеценко). Кримінально-правовому аспекту злочинів у сфері інформаційних комп'ютерних технологій присвячено роботи Д.С. Азарова, М.В. Карчевського, Н.А. Розенфельда та ін.

В останні роки в Україні в роботах П.А. Єрмакова, Ю.Ю. Орлова, В.П. Сапальова розглянуто питання використання технічних засобів оперативно-технічними підрозділами та можливості використання отриманих фактичних даних як джерел доказів. Дослідженнями інформаційного забезпечення діяльності органів внутрішніх справа з використанням сучасних інформаційно-технічних засобів займались науковці В.Л. Ортинський, П.І. Орлов, І.Р. Шинкаренко.

Комплексних робіт на монографічному рівні присвячених тактиці використання інформаційних технологій і засобів масової інформації при розкритті і розслідуванні злочинів, учинених ОЗУ, не виявлено серед масиву захищених вітчизняних досліджень.

Разом із тим, проблема вдосконалення розкриття і розслідування злочинів багатоаспектна. Розкриття злочину в криміналістичному аспекті розуміється як завдання кримінального судочинства, слідча (пізнавальна) діяльність, результат розслідування. Розкрити це значить здійснити пізнавальну діяльність, зібрати й оцінити інформацію, щоб невідоме стало відомим, таємне-явним, особа, що вчинила злочин, - була розшукана і викрита, встановлені всі інші обставини події злочину. А розслідування зло-

зисы выступл. к обл. конф.] – Харьков, 1990. – с.127-129.

320 Коновалова В.Е. Убийство: искусство расследования: [Монография]. /В.Е. Коновалова – Харьков: Факт, 2001. – с. 284.

321 Россинский С.Б. Осуществление специальных операций при производстве следственных действий / С.Б.Россинский //Воронежские криминалистические чтения. [Под ред. О.Я.Баева]. – Воронеж: Изд-во Воронежского гос. ун-та, 2002. – Вып. 3. – с. 187.

322 Лагутин А.В. Тактические операции при расследовании преступлений /А.В. Лагутин //Криминалистика и судебная экспертиза. – Вып. 20. – К.: Вища школа, 1980. – с.16

323 Матусовський Г.А. Основи взаємодії та інформаційного забезпечення в методиці розслідування злочинів /Г.А. Матусовський /Криміналістика. Криміналістична тактика і методика розслідування злочинів: [Підручник], [За ред. В.Ю.Шепітька]. – Харків: Право, 1998. – с.177-179

324 Матусовский Г.А. Экономические преступления: криминалистический анализ. /Г.А. Матусовский – Харьков: Консум, 1999. – с.149-156.

325 Белкин Р.С. Курс криминалистики: В 3 т. – Т.1: Общая теория криминалистики. / Р.С.Белкин – М.: Юрид. лит., 1991 – 204 с..

326 Криминалистика: [Учеб. для вузов] / И.Ф. Герасимов, Л.Я. Драпкин, Е.П. Ищенко и др.; [Под ред. И.Ф. Герасимова, Л.Я. Драпкина]. – 2-е изд., перераб. и доп. – М.: Высш. шк., 2000. – 672 с.

327 Яблоков Н.П. Есть ли необходимость в коренном изменении системы криминалистики и ее учебного курса? /Н.П. Яблоков // Вестник криминалистики / [Отв. ред. А.Г. Филиппов]. Вып. 1(9). – М.: Спарк, 2004. – с. 4-9.

328 Драпкин Л.Я. О возможностях использования современных информационных технологий в расследовании преступлений / Л.Я.Драпкин, Я.М.Злоченко, А.Е. Шуклин // Вестник криминалистики [Отв. ред. А.Г. Филиппов]. Вып. 3(7). – М.: Спарк, 2003. – с. 23-27.

329 Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. / Р.С. Белкин – М.: Издательство НОРМА (Издательская группа НОРМА – ИНФРА-М), 2001. – 240 с.

330 Криминалистическая тактика: состояние и тенденции: Межвуз. сб. науч. тр. / Актуальные проблемы уголовного процесса и криминалистики на современном этапе – Одесса: Одесский ун-т, 1993. – с. 147-152.

331 Шепитько В.Ю. Теория криминалистической тактики: [Монография]. /В.Ю. Шепитько – Харьков: "Гриф", 2002. – 349 с.

доказательств" //Воронежские криминалистические чтения. Вып. 2 / Ш.М. Хаутиев [Под ред. О.Я.Баева]. – Изд-во Воронежского ун-та, 2001. – с.86-93

305 Шиканов В.И. Информация к тактической операции "Атрибуция трупа". /В.И.Шиканов – Иркутск, 1975

306 Шиканов В.И. Теоретические основы тактических операций в расследовании преступлений. /В.И.Шиканов– Иркутск, 1983

307 Яблоков Н.П. Криминалистика. /Н.П. Яблоков – М.: Изд. группа НОРМА-ИНФРА-М, 2000. – с.193-195.

308 Булулуков О.Ю. Тактическая операция "Личность преступника" в расследовании убийств при отсутствии трупа /О.Ю. Булулуков //Проблеми законності: Респ. міжвідом. наук. зб. [Відп. ред. В.Я.Тацій]. – Харків: Нац. юрид. акад. України, 2001. – Вип. 49. – с. 166.

309 Дулов А.В. Тактические операции при расследовании преступлений. /А.В. Дулов – Минск, 1979. – с.44.

310 Белкин Р.С. Криминалистика: проблемы, тенденции, перспективы. От теории – к практике. /Р.С. Белкин – М.: Юрид. лит., 1988. – с. 139, 145.

311 Белкин Р.С. Курс криминалистики: В 3 т. – Т. 3: Криминалистические средства, приемы и рекомендации./ Р.С.Белкин – М.: Юрид. лит., 1991 – 204 с..

312 Морохин Б.Г. Элементы оперативной комбинации// Оперативно-розыская робота . / Б.Г. Морохин - М., 1979 . - № 108.

313 Оперативная комбинация. / Э.А.Дидоренко, Н.Н.Польской., В.Г. Самолов – К., 1975.- 267с.

314 Михальчук А.Е. Понятие тактических комбинаций при производстве следственных действий / А.Е.Михальчук // Теория и практика криминалистики и судебной экспертизы. – Саратов: Юрид. ин-т, 1990. – с.59.

315 Яблоков Н.П. Криминалистика. / Н.П.Яблоков – М.: Изд. группа НОРМА-ИНФРА-М, 2000. – с.189-193.

316 Салтевський М.В. Криміналістика. [Підручник]: У 2 ч. /М.В.Салтевський – Харків: Консум, 2001. – Ч. 2. – С.79.

317 Криминалистика. [Краткая энциклопедия]: [Автор-составитель Р.С.Белкин]. – М.: [Большая Российская энциклопедия], 1995. – с.82.

318 Князев В.А. О понятии тактической операции / В.А.Князев //Криминалистика и судебная экспертиза. – К.: Вища школа, 1982. – Вип. 25. – с.67

319 Князев В.А. К вопросу о понятии тактической задачи расследования / В.А.Князев, А.Д.Марушев // Реформа политико-правовой системы советского общества и укрепление социалистического правопорядка: [Те-

чинів, це пізнавальна і організаційно-тактична діяльність, сутність якої обумовлена особливостями формування доказової інформації і встановленим законом порядком її одержання.

Надзвичайно високу небезпеку для суспільства й «нові проблеми» для правоохоронних органів створює кримінальний контроль, що підсилюється, над «інформаційними сферами», що включає як криміногенні впливи засобів масової інформації, так і використання глобальних комп'ютерних мереж, телекомунікацій і радіоефіру, а також спеціальної техніки й інформаційних технологій у злочинній діяльності.

У світових масштабах технічний і технологічний прогрес не виконує однозначної соціальної функції, формування єдиного кіберпростору породжує не тільки нові комунікативні творчі можливості, але й ряд девіантних, у тому числі кримінальних явищ.

До числа найбільш важливих у теоретичному й методологічному аспектах можна віднести й той факт, що організована злочинність, виражаючи глобальні закономірності власної динаміки, стала набувати нових якостей.

Серед таких якостей варто назвати транснаціональність цього виду злочинності, її популяризацію в ЗМІ, криміналізацію економічної й політичної сфер, а також правоохоронної системи, формування віртуальних форм і розвитку злочинності в параметрах глобального комп'ютерного кіберпростору, поява тенденції не тільки професіоналізації певних форм злочинної діяльності, але перетворення її - у спосіб життя, кримінальну норму соціальної поведінки. Зазначені риси організованої злочинності формуються на ґрунті постійного оновлення інформаційних технологій, які ними використовуються, зокрема при вчиненні злочинів у сфері економіки , це не тільки потреба, а закономірність розвитку сучасної злочинності.

Як зазначає Щербаковський М.Г., існує низка проблем пов'язаних з виявленням слідів злочину, вчинених з застосуванням комп'ютерних технологій [27]. Сучасні системи комунікацій забезпечують передачу інформації в кіберпросторі, практично не залишаючи слідів (як правило „віртуальних" слідів, які можуть бути тільки скопійовані) , що дозволяє зробити її повністю закритою й доступною. Крім цього, сучасні технології й глобальні інформаційні системи створюють великі можливості для транснаціональної злочинної діяльності й дають злочинним угрупованням нові способи для більше легкого й успішного проведення незаконних операцій.

Розвиток інформаційних технологій і масштабів глобальних фінансових операцій уможливили збільшення обсягів, швидкості й закритості міжнародних фінансових розрахунків, що підвищило можливості організованої злочинності й зменшило ймовірність її виявлення й припинення,

що дозволяє легалізувати доходи від різних видів незаконної діяльності. Щодня 1 млрд. кримінальних доларів уливається в оборот світових фінансових ринків. Кількість і обсяг угод, що проходять через міжнародні міжбанківські електронні системи становить наступні величини: щодня через них здійснюється більше 465 тис. електронних переказів на суму більше 2 трильйонів дол. і 220 тис. угод [28, 29].

З огляду на це можна з упевненістю сказати, що прогноз Г. Тарда таки справдився. Цей учений-криміналіст ще наприкінці XIX ст. висунув гіпотезу про те, що майбутнє XX ст. буде століттям глобалізованої публіки, об'єднаної засобами масової комунікації, а суспільство він характеризував як продукт взаємодії індивідуальних свідомостей через спілкування, причому важливе місце займає процес наслідування [30]. Терміни "масова інформація" та "масова комунікація" стали характерними рисами нашого часу і здобули широкого вжитку на сторінках наукової літератури. Хоч ці терміни близькі за змістом і тісно пов'язані між собою, та все ж вони не рівнозначні. Масова інформація є різновидом соціальної, яка розглядається як змістовний аспект масової комунікації - це саме спілкування, передача інформації від людини людині в процесі діяльності. Термін "засоби масової комунікації" є більш широким і включає в себе як складову термін "засоби масової інформації".

За сучасних умов термін "засоби масової інформації" законодавчо закріплений у ст. 20 Закону України "Про інформацію" і під ним розуміємо: канал, спосіб передачі масової інформації; організації (газетні, журнальні редакції, радіостанції, телестудії, тощо), які займаються поширенням масової інформації; 3) кінцевий продукт діяльності зазначених організацій (випуск газети, радіо- або телепередача, сайт в Інтернеті); 4) особливий соціальний інститут (сукупність зазначених у пунктах 1–3 понять), який забезпечує існування комунікаційних процесів у суспільстві.

З одного боку, інформатизація веде до вдосконалення та інтенсифікації різних напрямів людської діяльності, з іншого, – її здобутки стають об'єктом негативних, антисоціальних проявів.

До негативних проявів належать, зокрема, правопорушення, що пов'язані з використанням інформаційних технологій; серед них особливу увагу пригортають такі, що мають ознаки злочину. Особливу тривогу викликає те, що ОЗУ активно використовують здобутки інформатики для досягнення злочинних цілей, що вже стало однією із обов'язкових ознак організованої злочинності. Термін "організоване злочинне угруповання" з'явився ще за радянських часів у зв'язку з прийняттям 18 травня 1961 р. указу Президії Верховної ради СРСР та відповідного Указу Президії Вер-

тельство НОРМА (Издательская группа НОРМА – ИНФРА-М), 2001. – 240 с.

291 Дулов А.В. Тактические операции при расследовании преступлений. / А.В. Дулов – Минск, 1979. – 128 с.

292 Шиканов В.И. Тактическая операция как важнейший структурный элемент следственной тактики и одна из форм сотрудничества органов следствия и дознания /В.И. Шиканов // Проблемы советского государства и права. Вып. 9-10. – Иркутск, 1975. – с. 33-48.

293 Михальчук А.Е. Понятие тактических комбинаций при производстве следственных действий / А.Е.Михальчук // Теория и практика криминалистики и судебной экспертизы. – Саратов: Юрид. ин-т, 1990. – с. 50-59.

294 Дулов А.В. О разработке тактических операций при расследовании преступлений / А.В.Дулов // 50 лет советской прокуратуры и проблемы совершенствования предварительного следствия. – Л., 1972. – с. 23-26.

295 Баев О.Я. Основы криминалистики: [Курс лекций]. /О.Я. Баев – М.: Экзамен, 2001. – с. 215-219

296 Белкин Р.С. Курс криминалистики: В 3 т. /Р.С. Белкин – М.: Юристъ, 1997. – Т.3: Криминалистические средства, приемы и рекомендации. – с. 202-243

297 Белкин Р.С. Криминалистическая энциклопедия. – 2-е изд., доп. /Р.С.Белкин – М.: Мегатрон XXI, 2000. – с. 219

298 Драпкин Л.Я. Первоначальные следственные действия в методике расследования преступлений и проблема повышения их эффективности /Л.Я Драпкин //Вопросы методики расследования преступлений. – Свердловск, 1976. – 68 с.

299 Дулов А.В. Тактические операции при расследовании преступлений. /А.В. Дулов – Минск, 1979.- 212 с

300 Князев В.А. Проблемы тактических операций в методике расследования хищений государственного или общественного имущества: автореф. дис... канд. юрид. наук. / В.А.Князев – Харьков, 1986 – 21с.

301 Коновалова В.Е. Убийство: искусство расследования: [Монография]. /В.Е. Коновалова – Харьков: Факт, 2001. – с.282-284

302 Лагутин А.В. Тактические операции при расследовании преступлений //Криминалистика и судебная экспертиза. – Вып. 20. /А.В. Лагутин. – К.: Вища школа, 1980. – с.16-19

303 Образцов В.А. Выявление и изобличение преступника. /В.А. Образцов. – М.: Юристъ, 1997. – с.54-60

304 Хаутиев Ш.М. Понятие и сущность тактической операции "Защита

налистика: [Учебник]/ Под ред. проф. И.Ф. Крылова. – Л.: Изд-во Ленингр. ун-та, 1976. – 591 с.

279 Комиссаров В.И. Теоретические проблемы следственной тактики / В.И. Комиссаров [Под ред. А.И. Михайлова]. – Саратов: Изд-во Саратовского ун-та, 1987. – 156 с.

280 Шепитько В.Ю. Теория криминалистической тактики: [Монография]. / В.Ю. Шепитько – Харьков: "Гриф", 2002. – 349 с.

281 Дулов А.В. Тактические операции при расследовании преступлений. /А.В. Дулов – Минск, 1979. – 128 с.

282 Тактические приёмы в структуре следственных действий и тактических операций / Л.Я. Драпкин // Научная информация по вопросам борьбы с преступностью. № 76 (Вопросы кр-ки). – М., 1983. – с. 22-24.

283 Тактические операции и охрана законных прав и интересов граждан при расследованиии преступлений / Проблемы правового статуса личности в уголовном процессе. – Изд-во Саратовского унив-та, 1981. – с. 140-142.

284 О теории тактических операций и её связях с другими структурными элементами науки криминалистики / [Оптимизация расследования преступлений: Сб. науч. тр]. – Иркутск: Изд-во Иркут. Ун-та, 1982. – с. 123-127.

285 Біленчук П.Д. Тактичні прийоми, тактичні комбінації та тактичні операції в розлідуванні злочинів: [Навч. посібник]. /Біленчук П.Д., Перкін В.І.– К.: Українська академія внутрішніх справ, 1996. – 32 с.

286 Цветков С.И. К вопросу о формировании частной криминалистической теории тактических операций / [Проблемы первоначального этапа расследования: Сб. науч. тр]. – Ташкент, Ташк. высшая школа МВД СССР, 1986. – с. 31-39.

287 Шиканов В.И. Теоретические основы тактической операции в расследовании преступлений. /В.И. Шиканов– Иркутск: Изд-во Иркут. ун-та, 1983. – 200 с.

288 Здоровко С.Ф. Тактичні операції при розслідуванні вбивств, що вчиняються організованими групами і злочинними організаціями: автореф. дис. ... канд. юрид. наук: 12.00.09 / С.Ф. Здоровко: Національна юридична академія ім. Я. Мудрого. – Харків, 2002. – 19 с.

289 Криминалистика: [Учебник], [Под ред. И.Ф. Крылова, А.И. Бастрыкина]. – М.: Дело, 2001. – 800 с.

290 Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. /Р.С.Белкин – М.: Изда-

ховної Ради УРСР від 27 червня 1961 р. [31, с.222; 32, с.342], про відповідальність за дії, що дезорганізують роботу виправно-трудових установ. Саме цим поняттям, поряд з іншими, почали оперувати дослідники феномену організованої злочинності.

Потребу тлумачення поняття "угруповання" підкреслював А.Ф. Зелінський, причому ним було проаналізовано деякі терміни, що вживалися в кримінальному законодавстві починаючи з Кримінального Уложення Росії до цього часу. На підставі здійсненого ним історико-етимологічного аналізу А.Ф. Зелінський дійшов висновку, що "термін "угруповання" нічого іншого окрім групи не означає, а стосовно теми, що розглядається – організованої групи чи співтовариства" [33, с.197–198].

В етимологічних джерелах угруповання визначається як "те саме, що група; об'єднання" [34, Т.1., с.353].

Таким чином, термін "угруповання" можна прийняти як умовне об'єднавче поняття для зручності дослідження та практичного використання у правоохоронній діяльності, оскільки цей термін закріплений законодавчо [35, с.38] і широко використовується практичними працівниками та науковцями. Змістом його виступатиме узагальнююче визначення різних типів об'єднань злочинців. Об'єднання може розглядатись як певний союз осіб, а термін "союз" мовознавцями тлумачиться як "взаємні узи, зв'язок, скріплення, поєднання, змикання, тісний зв'язок між людьми, дружба, товариство, умовна згода, поєднання двох або багатьох для відомої мети" [36, Т.4., с.285].

Відповідно до кримінального законодавства України (ч. 3 ст. 28 КК) злочин визнається вчиненим організованою групою, якщо в його готуванні або вчиненні брали участь декілька осіб (три і більше), які попередньо зорганізувалися у стійке об'єднання для вчинення цього та іншого (інших) злочинів, об'єднаних єдиним планом з розподілом функцій учасників групи, спрямованих на досягнення цього плану, відомого всім учасникам групи.

Характерними властивостями організованих груп є наявність єдиного плану з розподілом функцій учасників груп, спрямованих на досягнення цього плану. План повинен бути відомий учасникам групи. Така ретельна підготовка може мати місце не тільки тоді, коли злочинна група налаштована на вчинення ряду злочинів, але й тоді, коли нею вчиняється один злочин. Це свідчить про стійкий характер організованої групи [37, с. 45]. Залежно від способів та умов взаємодії злочинців спільна злочинна діяльність набуває певних рис. Зокрема, учасники організованої групи – це три особи і більше, які попередньо об'єднуються для підготовки та вчинення одного або декількох злочинів [38, с. 204].

Ще більш високий ступінь організованості й стійкості мають злочинні організації. На думку А.І.Гурова, такі організації являють собою найбільш небезпечну форму організованої групової злочинної діяльності, що має складний, багатоступеневий опосередкований характер, призводить до формування стійких організованих форм зв'язку співучасників, вироблення і засвоєння надійних способів вчинення і приховування злочинів, створення згуртованої організації, де безпосередні спілкування між членами з міркувань конспірації найчастіше замінюються інформаційними і діяльнісними зв'язками, а відносини мають суто "діловий" характер [39, с. 207]. За чинним КК України (ч.4 ст. 28) злочин визнається вчиненим злочинною організацією, якщо він скоєний стійким ієрархічним об'єднанням декількох осіб (три і більше), члени якого або структурні частини якого за попередньою змовою зорганізувалися для спільної діяльності з метою безпосереднього вчинення тяжких або особливо тяжких злочинів учасниками цієї організації, або керівництва чи координації злочинної діяльності інших осіб, або забезпечення функціонування як самої злочинної організації, так і інших злочинних груп. Організована злочинна діяльність є спільною діяльністю її учасників. Тому участь членів стійких злочинних угруповань в організованій злочинній діяльності може полягати в: 1) організації злочинного угруповання; 2) керівництві угрупованням чи окремим його підрозділом; 3) забезпеченні існування та функціонування самого угруповання без участі у вчиненні конкретних злочинців; 4) примусовому втягненні інших осіб до складу угруповання або до вчинення окремих злочинів; 5) участі у вчиненні в складі угруповання або в його інтересах конкретних злочинів [40, с. 78].

Традиційно до ознак функціонування ОЗУ відносять: ієрархічна побудова організованих угруповань; певна стійкість і тривалість існування; спеціалізація у спрямованості злочинного формування; сувора втурішньогрупова дисципліна; існування злочинних норм і правил поведінки; наявність лідера (декількох лідерів) з владними повноваженнями; розподіл функціональних обов'язків серед членів групи; корислива спрямованість (кримінальний бізнес) злочинної діяльності; наявність системи захисту від викриття; створення єдиної каси («общак»); існування власної системи «заохочення» і «покарання»; підтримка тих, кого притягують до кримінальної відповідальності; існування системи втягування до злочинної групи; використання корумпованості в органах влади і управління, а також у правоохоронних органах; наявність стосунків із корумпованими особами органів влади і управління та працівниками правоохоронних органів; підтримка стосунків та вирішення проблем між організованими злочинними

Аверьянова, И.Л. Александрова и др.; [Под ред. проф. А.Ф. Волынского]. – М.: Закон и право, ЮНИТИ-ДАНА, 1999. – 615 с.

267 Криминалистика: [Учебник] / Под ред. И.Ф. Крылова, А.И. Бастрыкина. – М.: Дело, 2001. – 800 с.

268 Лекар А.Г. Научные основы организационно-тактических мер повышения эффективности борьби органов внутренних дел с преступностью. /А.Г Лекар. – М.., 1992.

269 Лукашов В.А. К вопросу об исходных положениях теории оперативно-розыскной тактики / В.А.Лукашов, С.А. Смирнов. – М. / Оперативно-розыскная тактика органов внутренних дел: Труды академии МВД, 1988. – с.3-16.

270 Дидоренко Э.А. Правове и организационо-тактические проблемы совершенствования оперативной разработки (по материалам аппаратов уголовного розыска Увд областей Западного региона Украинской ССР): автореф. дис. ..канд.юрид. наук. /Э.А. Дидоренко - М.1979.- 41с.

271 Козаченко И.П. Основные направления совершенствования теории и практики оперативно-розыскной деятельности / И.П Козаченко – К.: Вопросы совершенствования оперативно-розыскной деятельности органов внутренных дел. УАВД, 1992.- 167 с.

272 Басецкий И.И. Теоретические основы, правовые, этические и организационно-тактические проблемы агентурной работы органов внутренних дел: автореф. дис. …доктора юрид. наук. / И.И. Басецкий. – М., 1991. - 36 с.

273 Біленчук П.Д. Тактичні прийоми, тактичні комбінації та тактичні операції в розлідуванні злочинів: [Навч. посібник]. / П.Д.Біленчук, В.І. Перкін – К.: Українська академія внутрішніх справ, 1996. – 32 с.

274 Криминалистика: [Учебник для вузов] / А.Ф. Волынский, Т.В. Аверьянова, И.Л. Александрова и др.; [Под ред. проф. А.Ф. Волынского]. – М.: Закон и право, ЮНИТИ-ДАНА, 1999. – 615 с.

275 Филющенко А.А. Предмет и содержание криминалистической тактики // Теоретические проблемы криминалистической тактики. / А.А.Филющенко – Свердловск, 1981. – с. 5-9.

276 Криминалистика: [Учебник для юрид. ис-тов и фак.]. [Отв. ред. д-р юрид. наук проф. А.Н. Васильев]. – М.: Изд-во Моск. ун-та, 1963. – 619 с.

277 Криминалистика: [Учеб. для вузов] / И.Ф. Герасимов, Л.Я. Драпкин, Е.П. Ищенко и др.; [Под ред. И.Ф. Герасимова, Л.Я. Драпкина]. – 2-е изд., перераб. и доп. – М.: Высш. шк., 2000. – 672 с.

278 Быховский И.Е. Общие положения следственной тактики / Крими-

255 Концепція технічного захисту інформації в Україні: Постанова Кабінету Міністрів України № 1126 від 8.10.1997 р. / Державний вісник України. – 1997. – № 12 (38).

256 Про заходи щодо посилення контролю за розробленням, виготовленням і реалізацією технічних засобів негласного отримання інформації: Указ Президента України № 1346/98 від 14.12.1998 р. / Урядовий кур'єр. – № 1. – 1999. – 5 січня.

257 Положення про технічний захист інформації в Україні: Затверджене Указом Президента України № 1229/99 від 27.09.1999 р. / Офіційний вісник України. – 1999. – № 39.

258 Про деякі питання захисту інформації, охорона якої забезпечується державою: Постанова Кабінету Міністрів України № 281 від 13.03.2002 р. / Офіційний вісник України. – 2002. – № 11.

259 Про першочергові організаційні заходи щодо створення Центру та підрозділів технічного захисту інформації в системі МВС України. / Наказ МВС України № 314 від 16.05.1995 р.

260 Про організацію та виконання робіт з технічного захисту інформації з обмеженим доступом у системі МВС України / Наказ МВС України № 059 від 14.07.1998 р.

261 Про затвердження Концепції розвитку системи інформаційного забезпечення органів внутрішніх справ України на 1998-2000 роки та Програми інформатизації органів внутрішніх справ України на 1998-2000 роки / Наказ МВС України № 357 від 14.05.1998 р.

262 Орлов Ю.Ю. застосування оперативної техніки в оперативно-розшуковій діяльності міліції (теоретичні, правові та організаційно-тактичні проблеми) : автореф. дис. ... канд. юрид. наук: 21.07.04 / Ю.Ю.Орлов. – Київ, КНУВС. 2008. – 35 с.

263 Security News: Газета международных новостей по техническим средствам и системам безопасности [Електронний ресурс] Режим доступу // http://www.securityru.com/

264 Хараберюш І.В. Використання оперативно-технічних засобів щодо протидії злочинам у сфері нових інформаційних технологій: автореф. дис. ...канд. юрид. наук: 12.00.09 / І.В. Хараберюш – Львів, ЛДУВС. 2006. – 19 с.

265 Криминалистика: [Учеб. для вузов] / И.Ф. Герасимов, Л.Я. Драпкин, Е.П. Ищенко и др.; [Под ред. И.Ф. Герасимова, Л.Я. Драпкина]. – 2-е изд., перераб. и доп. – М.: Высш. шк., 2000. – 672 с.

266 Криминалистика: [Учебник для вузов] / А.Ф. Волынский, Т.В.

угрупованнями в різних регіонах країни та з її межами; наявність системи проникнення у владні структури та створення механізму лобіювання власних інтересів [41, с. 8-9]. Це не є вичерпним переліком, і нашу думку до специфічних ознак функціонування злочинної діяльності ОЗУ, слід також віднести ознаку використання інформаційних технологій і засобів масової інформації в інтересах ОЗУ.

Поширення інформаційних технологій відкриває шлях для вчинення традиційних злочинів нетрадиційними засобами. Як відзначалося у доповіді генерального секретаря ООН, всесвітній досвід засвідчує, що по мірі розвитку у світі техніки і поява спеціалістів більш високої кваліфікації „..з'являється дедалі більше талановитих людей для створення нових унікальних способів учинення злочинів, особливо в галузі інформаційно-обчислюваних технологій" [42].

Саме неповнота пізнання природи та законів розвитку злочинної діяльності як соціального явища та чинника життєдіяльності злочинності, призвела до поглиблення професіоналізму в злочинності, появи організованої злочинності.

У зв'язку з цим А.В. Дулов слушно зазначає, що не можна пізнати закономірності діяльності з розслідування, не вивчивши той об'єкт, на який вона спрямована, тобто злочинну діяльність [43, 28].

Під злочинною діяльністю слід розуміти систему передбачених кримінальним законом діянь і тісно пов'язаних з ними інших передкримінальних та післякримінальних дій, що психологічно детерміновані загальним мотивом, реалізація якого планується суб'єктом за допомогою постановки і досягнення окремих, проміжних цілей [44, с.96].

Отже, злочинна діяльність охоплює не тільки неодноразове вчинення злочинів, але й учинення одиничного (у тому числі триваючого) злочину, складність підготовки якого передбачає необхідність багатоактної діяльності [45, с.78].

Тому для підвищення ефективності боротьби зі злочинною діяльністю потрібне її вивчення не тільки як соціального феномена, а як одного з різновидів злочинної діяльності, як під час підготовки до злочину, так і в ході його вчинення та приховування, під час якої використовуються інформаційні технології.

На цей час спостерігаються якісні зміни, виявляються нові тенденції розвитку організованої злочинності, які стосуються використання організованими злочинними формуваннями сучасних інформаційних технологій та ЗМІ у протиправній діяльності. Сучасний аналіз діяльності як вітчизняних, так і зарубіжних правоохоронних органів, наукової літератури, а також засобів

масової інформації дає підставу говорити про те, що злочинні формування застосовують інформаційні технології та ЗМІ у своїй протиправній діяльності при наймі як: засіб зв'язку, джерело отримання інформації, спосіб збереження інформації, спосіб передання інформації, знаряддя злочинного посягання, об'єкт злочинного посягання, як засіб впливу на учасників кримінального процесу та протидії правоохоронним органам.

Так В.Ю. Шепітько вказує: "Організована злочинність пристосовується до нових соціально-економічних умов. Злочинці широко використовують різноманітний сучасний радіозв'язок, технічні засоби, новітню вогнепальну зброю. Відсутність чіткої правової регламентації щодо ввезення на територію України та застосування "спеціальних технічних засобів" (підслуховуючих пристроїв, пеленгаторів, радіостанцій) призвело до озброєння ними злочинних формувань. Сучасна організована злочинна діяльність не може обійтись без міцної організаційно-технічної бази, яка робить організовані злочинні угруповання менш вразливими для правоохоронних органів і кримінальних конкурентів, більш мобільними в отриманні необхідної для організованої злочинної діяльності інформації, переміщенні, опорі викриттю" [46, с.42-43].

Як справедливо зазначає М.І. Мельник, організована злочинність за останні роки якісно змінилась, набула рис реальної влади у державі. Цьому сприяє використання організованими злочинними структурами можливостей офіційної влади (через корумповані зв'язки), а також легалізація своєї діяльності через органи державної влади [47, с. 51]. У Постанові Верховної Ради України від 26 грудня 2002 р. № 388-IV відзначено, що організована злочинна діяльність корумповано зрощених із суто кримінальними елементами вищих посадових осіб за останні роки набула рівня реальної загрози конституційним основам державного ладу в Україні, стала негативно впливати на внутрішню і багато в чому також на зовнішню політику держави та її сприйняття у цивілізованому світі. Реалізація злочинних корисливих інтересів певних великих організованих злочинних груп і злочинних організацій, які намагаються контролювати, зокрема, і правоохоронні органи та судову систему, постійно призводить до величезних соціально-економічних втрат, реально гальмує розвиток держави, має вкрай негативні політичні наслідки довготривалої дії [48].

М.П. Яблоков відзначає, що однією із причин тієї ситуації, яка склалась на цей час у сфері боротьби з організованою злочинністю є все ще недостатнє науково-криміналістичне відпрацювання проблем боротьби з цим видом злочинності, відсутність чіткої уяви про стратегію та ідеологію цієї боротьби, а також криміналістичної концепції та відповідних науко-

ванной преступной деятельности /В.В. Трухачев // Юридические записки [Под ред. О.Я. Баева]. – Воронеж, 1999. – Вып. 10. – с. 129-143.

245 Проблеми криміналістичного забезпечення бороть-би з організованою злочинністю: Між-від. наук. зб. / [Проблеми боротьби з корупцією, організованою злочинністю та контрабандою. Президенту України, Верховній Раді України, Уряду України, органам центральної та місцевої виконавчої влади. Аналітичні розробки, пропозиції наукових і практичних працівників], [Під ред. А.І. Комарової, В.В. Медведчука, В.О. Євдокимова, В.Ф. Бойка, О.О. Крикуна]. – К., 1999. – Т. 18. – с. 146-153.

246 Гузь В.І. Організація та тактика діяльності підрозділів внутрішньої безпеки по протидії розвідницьким заходам злочинних формувань: Зб. наук. праць. [Актуальні проблеми сучасної науки в дослідженнях молодих учених] – Х., 1997. – Вип. 3 і 4. – с. 144-148.

247 Сакало В.О. Тактика злочинної діяльності: втореф. дис. … канд. юрид. наук: 12.00.09 / В.О. Сакало. НАВСУ. – К., 2002. – 16 с.

248 Карпов Н.С. Специфічний погляд на проблеми боротьби зі злочинністю / Н.С. Карпов // Вісн. Одес. ін-ту внутр. справ. – 2001. – № 2. – с. 27-32.

249 Федотов М. Экология информации / М. Федотов // Российская юстиция. – 1999. - № 12. – с. 29-30.

250 Криміналістика: [Курс лекцій (ч.1)]. /Бахін В.П., Гора І.В, Цимбал П.В. – Ірпінь: Академія ДПС України, 2002. – 356 с.

251 Загіка Г.В. Деякі питання забезпечення безпеки інформаційної системи в ОВС на транспорті / Г.В. Загіка // Вісн. Одес. ін-ту внутр. справ. – 2000. – № 3. – С. 143-147.

252 Кримінальна тактика протидії правоохоронній системі як складова інфраструктури організованої злочинності: Міжвід. наук. зб. [Проблеми боротьби з корупцією, організованою злочинністю та контрабандою. Президенту України, Верховній Раді України, Уряду України, органам центральної та місцевої виконавчої влади. Аналітичні розробки, пропозиції наукових і практичних працівників]: / [Під ред. А.І. Комарової, В.В. Медведчука, В.О. Євдокимова, В.Ф. Бойка, О.О. Крикуна]. – К., 1999. – Т. 18. – с. 199-202.

253 Брагин О. Еще раз о безопасности /О. Брагин // Служба безопасности. – 1998. – № 6. – С. 8-10.

254 Францович Л. Технології комплексного захисту інформації: [навч. посібник] / Чернівецький національний ун-т ім. Юрія Федьковича / Леонід Францович... Політанський (уклад.). — Чернівці : Рута, 2007. — 140с.

231 О процессуальной безопасности свидетеля и потерпевшего // Сов. юстиция. – 1993. – № 20. – с. 26-27.

232 Майн Х. Средства массовой информации в Федеративной Республике Германии / Х. Майн: [Пер. с нем.: М. Балье, Т. Маневич]. – Б.м.: Коллоквиум, 1996. – 158 с.

233 Бахін В.П. Криміналістика: [Курс лекцій (ч.1)]. / В.П.Бахін, І.В Гора, П.В.Цимбал. – Ірпінь: Академія ДПС України, 2002. – 356 с.

234 Положення про Центр громадських зв'язків МВС, ГУМВС, УМВС, УМВСТ: Наказ МВС України від 31 жовтня 2003 року № 1357. - К.: МВС України, 2003. – 5 с.

235 Про створення Департаменту зв'язків з громадськістю МВС України: Наказ МВС України від 25 березня 2004 р. № 330. – К.: МВС України, 2004. – 1 с.

236 Кузьмичев В.С. Теория и практика следственной деятельности. [Монография]. / В.С. Кузьмичев – К: НТВ "Правник", 1997. – 246 с.

237 Цивільний кодекс України // Голос України. – 2003. - 12 березня.

238 Гудвин против Соединенного Королевства // Российская юстиция. – 1999. - № 7. – С. 56-58.

239 Сучасне Кримінальне законодавство України в порівнянні з Кримінальним кодексом України 1960 р.: / В.Є. Ткаліч, В.М. Пьохов, О.І. Плужнік [Довідник для курсантів, студентів та слухачів ОЮІ НУВС]. - Одеса: Вид-во ОІВС, 2003. - 304с.

240 Правові та криміналістичні проблеми щодо розголошення даних попереднього слідства / Матеріали міжнародної науково-практичної конференції конференції "Проблеми вдосконалення законодавства та практика його застосування з урахуванням прогнозу злочинності", 20-21 травня 1999 р., Луганськ. Вісник Луганського інституту внутрішніх справ МВС України. Спец. випуск. Ч. 3. Луганськ, 1999. – с. 81-84.

241 Бахин В.П., Карпов Н.С. Некоторые аспекты изучения практики борьбы с преступностью (данные исследований за 1980-2002 г.г.). / В.П.Бахин, Н.С.Карпов. – К., 2002. – 458 с.

242 Стулин О.Л. Классификация видов противодействия / О.Л. Стулин // Российский следователь. – 1999. – № 5. – с. 37-41.

243 Идея и перспективы криминалистического преактивизма / Юридическая наука и образование в Республике Беларусь на рубеже XX-XXI веков: Материалы междунар. науч.-практ. Конференции, [Под ред. проф. Г.А. Зорина]. – Гродно: ГрГУ, 1998. – с. 18-28.

244 Трухачев В.В. Криминалистический анализ сокрытия организо-

вих рекомендацій по виявленню, розкриттю, розслідуванню і попередженню організованої злочинної діяльності [49, с. 5].

Використання можливостей інформаційних технологій у протидії організованій злочинності та корупції має бути випереджувальною та адекватною тим технологіям, які використовують ОЗУ та спиратись на обґрунтовані теоретичні засади, нормативно-правові акти, в тому числі й міжнародні, досвід інших країн, а також ці дії повинні розглядатись як складова частина оперативно-розшукової та слідчої діяльності, яка повинна здійснюватись професіоналами належного рівня підготовки.

Більш того, злочинні формування використовують способи прихованого одержання інформації та способи інформаційних впливів безпосередньо проти правоохоронних органів та громадян при вчиненні шахрайських дій. Мають місце використання психотехнік нейролінгвістичного програмування, гіпнозу та інших, які можуть змінювати смаки, формувати нав'язливі потреби, установки, у тому числі страхи, сумніви в колишніх переконаннях, руйнувати й, навпаки, викликати симпатії й антипатії. Схема впливу містить 6 основних механізмів, кожному з яких відповідає психологічний принцип, що лежить в основі людської поведінки: принцип взаємного обміну; зобов'язання й послідовності; соціального доказу; прихильності; авторитету; дефіциту. Постраждалими від цих технологій є тисячі людей, які вкладають свої гроші у „повітря", і не мають правових гарантій захисту своїх прав.

Під час проведення досудового слідства слідчі часто зустрічаються з випадками протидії зі сторони представників організованих злочинних груп, інших осіб, не зацікавлених у позитивних результатах розслідування. Протидія може виражатись в даванні хабара, тиску впливових осіб на слідчого або керівника органу, що проводить розслідування, залякуванні свідків та потерпілих, поміщенні дестабілізуючої інформації у ЗМІ тощо. Саме тиск на слідчого через ЗМІ, на думку М.П. Яблокова, є однією з ознак, за якою можна розпізнати почерк дій організованої групи у кримінальній справі, по якій проводиться розслідування [50, с.49]. Зараз злочинність цілком спроможна організувати цілеспрямовану кампанію в ЗМІ для впливу на прийняття рішень посадовими особами. Є приклади задіяння чотирьох газет, телестудії і депутатського корпусу для розвалу кримінальної справи [51, с.17]. Разом із тим слід відзначити, що до сьогоднішнього часу в криміналістичній науці не достатньо опрацьовані напрямки ефективної взаємодії правоохоронних органів із ЗМІ при розслідуванні злочинів вчинених ОЗУ, які викликали значний суспільний резонанс, а також коли для впливу на процесуальні рішення правоохоронних органів

застосовувалась сила суспільної думки.

Спостерігається підвищена увага кримінального середовища до засобів масової інформації, підсилюється її силовий тиск на журналістів, телерадіокоментаторів, підкуповують не тільки окремих працівників, але й деякі видання, програми, що віддають перевагу тим матеріалам, в яких злочинці мають інтерес.

Як показує досвід правоохоронних органів, у тому числі й міжнародний, в останній час досить часто спостерігається використання злочинцями ЗМІ (Інтернету) для вчинення різного роду злочинів. В.Ю. Шепітько справедливо відмічає, що реалії соціально-економічних перетворень в Україні, формування приватного сектору економіки, зміни в економічних відносинах вплинули на розвиток кримінального бізнесу, виникнення нового типу "інтелектуального" злочинця, нових видів злочинної діяльності і способів її здійснення [52, с. 276]. Цю ж думку підтримують й інші вчені-криміналісти. Так А.Д. Трубачов також відмічає, що в сучасних умовах поряд із традиційними способами посягання на майно також отримало поширення заволодіння грошовими та матеріальними цінностями фізичних та юридичних осіб шляхом шахрайства. У сфері бізнесу виникли нетрадиційні прийоми злочинного втручання в господарську діяльність юридичних осіб різних форм власності, а також заволодіння грошовими коштами окремих громадян. До них можна віднести створення фіктивних підприємств, укладання фіктивних договорів на поставку товарів за рахунок передоплати, використання завідомо неправдивої реклами для залучення клієнтів із наступним привласненням отриманих від них грошей [53, с. 470]. Про зміни способів злочинної діяльності, що включають організацію і проведення організованими злочинними групами шахрайств, поєднаних з використанням активної рекламної кампанії у ЗМІ, пише й І.О. Возгрін [54, с. 789].

Такий стан можна пояснити тим, що сучасні ЗМІ орієнтуються на як найбільшу відкритість та доступність для всіх верств населення. Для вчинення багатьох видів злочинів, пошуку нових потерпілих злочинці поміщають у відповідні ЗМІ повідомлення різного змісту. Така тенденція розвитку злочинності набуває дедалі більших розмірів. Адже зміст та відповідність дійсності таких повідомлень редакціями та установами ЗМІ не перевіряється, вони не несуть відповідальності за оприлюднення такої інформації. В.П. Лавров відмічає використання у злочинних намірах ЗМІ як одну з ознак, якими характеризується організація діяльності злочинних формувань [55, с. 312].

В останні роки активно використовується для вчинення злочинів як

СССР]. Ташк. высш. школа. – Ташкент, 1987. – 166 с.

218 Ратинов А.Р. Судебная психология для следователей: [Учеб. пособие]. /А.Р. Ратинов. – М., 1967. – 290 с.

219 Аленин Ю.П. Процессуальные особенности производства следственных действий. / Ю.П. Аленин. – Кировоград: Центрально-Украинское издательство. – 2002. – 264 с.

220 Далин В.Е. Теоретические и организационные вопросы конспирации данных предварительного следствия / В.Е. Далин. – Волгоград: Организаторская деятельность по повышению качества следственной работы: [Сб. науч. тр.], М-во внутр. дел СССР; Высш. следств. школа., 1984. – С. 92-98.

221 Мепаришвили Г.Д. Охрана тайн личной жизни граждан в советском уголовном процессе: автореф. дисс. … канд. юрид. наук: 12.00.09 / Г.Д. Мепаришвили: АН СССР; Ин-т государства и права. – М., 1987. – 21 с.

222 Петрухин И.Л. Личные тайны (человек и власть). / И.Л.Петрухин. – М.: Ин-т государства и права Рос. Акад. наук, 1998. – 232 с.

223 Устименко Н.В. Таємниці особистого життя людини та їх цивільно-правова охорона: автореф. дис. … канд. юрид. наук: 12.00.03 / Н.В. Устименко.– Х: Нац. юрид. акад. України імені Ярослава Мудрого.., 2001. – 20 с.

224 Про оперативно-розшукову діяльність Закон України // Відомості Верховної Ради України. – 1992. – № 22. – Ст. 303.

225 Конституція України: Прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 р. – К.: Преса України, 1997. – 80 с.

226 Лісогор В.Г. Криміналістичне забезпечення збереження таємниці досудового слідства: автореф. дис. ...канд. юрид. наук: 12.00.09 / В.Г. Лісогор – К., НАВСУ., 2003. – 19 с.

227 Правове регулювання інформаційної діяльності в Україні : станом на 1 січня 2001 р.: [упоряд. С.Е. Демський; відп. ред. С.П. Павлюк.]. – К.: Юрінком Інтер, 2001. – 688 с.

228 Правове регулювання інформаційної діяльності в Україні : станом на 1 січня 2001 р.: [упоряд. С.Е. Демський; відп. ред. С.П. Павлюк.]. – К.: Юрінком Інтер, 2001. – 688 с.

229 Гласность предварительного следствия / Л.Батищева, Е. Конах, А Леви., Г. Пичкалева // Соц. законность. – 1989. – № 1. – с. 60-62..

230 Лісогор В., Москвін Ю. Засоби масової інформації та питання збереження таємниці досудового слідства / В.Лісогор, Ю.Москвін // Наук. вісн. Акад. держ. податк. служби України. – 2000. – № 3. – с. 139-143.

203. Новий тлумачний словник української мови: У 4-х т. - Т. 2. – К.: Аконіт, 1998. - 910 с.

204. Словарь синонимов русского языка [упоряд. Александрова З.Е.], [Под ред. Л.А. Чешко]. – М.: Рус. яз., 1975. – 600 с.

205. Словарь русского языка: В 4-х т. / АН СССР; Ин-т рус. яз. – М.: Рус. яз., 1981. – Т. 2. – 736 с.

206. Киевские ведомости. – 2000. – 23 мая.

207. Киевские ведомости. – 2000. – 1 июня.

208. Человек и закон. – 2000. – № 1 (2).

209. Факты. – 2000. – 7 октября.

210. Быховский И.Е. Процессуальные и тактические вопросы системы следственных действий: автореф. дисс. доктора юрид. наук / И.Е. Быховский: Всесоюз. ин-т по изучению причин и разработке мер предупреждения преступности прокуратуры Союза ССР. – М., 1976. - 32 с.

211. Далин В.Е. К вопросу о психологическом воздействии в правоприменительной деятельности следователя / В.Е. Далин – Волгоград: Проблемы применения правовых норм на предварительном следствии: [Сб. науч. тр. М-во внутр. дел СССР, Высш. следств. шк.], ВСШ, 1982. – с. 97-104.

212 Лукьянчиков Е.Д., Кузьмичев В.С. Тактические основы расследования преступлений: [учеб. пособие]. / Е.Д.Лукьянчиков, В.С. Кузьмичев – К.: КВШ МВД СССР, 1989. – 48 с.

213 Бахин В.П. Тактика использования внезапности в раскрытии преступлений органами внутренних дел: [Учеб. пособие]. / В.П. Бахин., В.С. Кузьмичев, Е.Д. Лукьянчиков - К., 1990. – 56 с.

214 Криминалистическое обеспечение деятельности криминальной милиции органов предварительного расследования: [Учебник], [Под ред. Т.В. Аверьяновой и Р.С. Белкина]. – М.: Новый юристъ, 1997. – 400 с.

215 Уголовно-процессуальный кодекс Украинской ССР: [Науч. - практ. коммент.] / В.Г. Белоусенко, Ю.М. Грошевой, А.Я. Дубинский и др.; [Отв. ред. П.Г. Цупренко]. – К.: Политиздат Украины, 1984. – 595 с.

216 Павлов Н.Е. Общие условия предварительного расследования: (Сравнительное исследование): [Учеб. пособие] / Н.Е. Павлов – М.: Акад. МВД СССР. НИ и РИО, 1982. – 64 с.

217 Арипов Т.А. Сущность и виды противодействия установлению истины в стадии предварительного следствия / Т.А. Арипов // Пути совершенствования деятельности следственных аппаратов органов внутренних дел: [Сб. науч. тр.], [ред. кол.: Г.А. Абдумаджидов (отв. ред.) и др.; МВД

окремими злочинцями, так і організованими групами, Інтернет. Так досить поширеним є вчинення шахрайства під виглядом гри “Піраміда”, створення он-лайн-магазину, проведення інтернет-аукціонів тощо. Проведене Агентством цінних паперів дослідження показало, що чітко визначених кордонів між надійною та ненадійною інформацією в Інтернеті не існує. Так кількість користувачів мережі Інтернет, потерпілих від віртуального шахрайства в 2000 р., згідно з дослідженням, проведеним компанією e-Market, становила 34% [56]. Відомі випадки, коли злочинними угрупованнями наймалися хакери, яким надавалися окремі приміщення, що охоронялися та були обладнані найсучаснішими технологіями для того, щоб здійснювати викрадення грошей шляхом незаконного проникнення у комп’ютерні мережі великих комерційних банків [57].

Можемо лише констатувати безліч випадків використання злочинцями рекламних оголошень у ЗМІ для вчинення шахрайств стосовно великої кількості людей, які повірили цій рекламі, і неефективність традиційних форм діяльності правоохоронних органів протидіяти та попереджати такі випадки.

Вищевикладене потребує нового підходу до розробки тактики виявлення правоохоронними органами ознак злочинів та осіб, що їх вчинили. Тому, пояснюючи причини слабкої результативності боротьби з організованою злочинністю, керівники поліцейських служб указують на неефективність “традиційних криміналістичних методів” [58, с. 295].

Тому для слідчого важливим є володіння методами та прийомами злочинної діяльності. В.П. Бахін, В.С. Кузьмічов, О.О. Садченко зазначають: “Щоб слідчий міг протистояти прийомам і засобам, які використовують злочинці, він повинен їх знати і враховувати” [59, с. 214].

Всебічне пізнання сутності та властивостей злочинної діяльності не можливе, на наш погляд, без аналізу протилежного їй виду людської практики, а саме діяльності із розслідування злочинів. Цілком вірно з цього приводу зауважує В.П. Бахін, що “вся людська діяльність дає можливість пізнавати та перетворювати оточуючий світ, визначати конкретні цілі і діяти відповідно до них” [60, с. 7]. Так ще на етапі становлення криміналістики Г.Ю. Манс, І.М. Якимов, С.О. Голунський, Г.К. Рогінський та інші вчені вказували на два полюси в об’єкті вивчення криміналістики – злочинну діяльність та діяльність із розслідування злочинів [61; 62; 63].

Одним зі специфічних видів соціальної діяльності є боротьба зі злочинністю, зокрема, такий її різновид, як слідча діяльність.

У монографії В.С. Кузьмічова досить повно розглянуті питання, що стосуються природи та сутності слідчої діяльності. Автор зазначає, що в криміналістичній літературі розглядаються різні аспекти слідчої діяльнос-

ті. Серед них: логічний, інформаційний, психологічний, комунікативний, організаційний тощо [64, с.17–18].

Критерій істини, що дозволяє визначити правомірність використання певних засобів розслідування полягає в сутності слідчої діяльності, у факторах, які зумовили її характер. Один з них – у тому, що таємному способу злочинної діяльності та способам протидії їх вияву повинні бути протиставлені відповідні засоби та прийоми слідчої діяльності, які мають примусовий і, в деяких випадках, прихований характер. В.П. Бахін і С.М. Зав'ялов зазначають, що "в даний час, у зв'язку з якісною зміною злочинності та умов, у яких здійснюється і розвивається злочинна діяльність, значення, місце та роль способу вчинення злочинів потребують нового осмислення…" [65, с. 178–182].

Найбільшу загрозу збереженню доказів становить не об'єктивний плин часу, а свідома протидія осіб, зацікавлених у перекручуванні результатів розслідування. Цим розслідування злочинів найбільше відрізняється від усіх інших видів пізнавальної діяльності. Наведене зумовлює необхідність використання таких засобів і методів збирання інформації, які компенсували б або нейтралізували негативні умови та труднощі пізнання. Це забезпечується максимальним використанням науково-технічних досягнень для розширення кола джерел інформації; пошуком засобів виявлення слідів значної давності; акцентуванням уваги на слідах, які залишились поза контролем злочинця (мікрослiди); розробкою методик відновлення умисно пошкоджених джерел інформації (поновлення номерів на металі); застосуванням прийомів поновлення забутого, викриття неправдивих показань тощо [66; 67, с. 105-110; 68]. Г.А. Зорін зазначає, що "одна з найголовніших причин інтенсивного розвитку та зростання злочинності полягає у тому, що розслідування слідує за злочином як у часі, так і за місцем дії. Воно діалектично запізнюється, викликаючи закономірну неготовність в організаційному, методичному, технічному й інформаційному відношенні" [69, с.136]. А це у свою чергу потребує постійного оновлення методик відповідно до виникнення нових технологій вчинення злочинів і зокрема інформаційного характеру.

На часі необхідне вивчення всіх аспектів виникнення та функціонування злочинної діяльності як самостійного явища в цілому, так і на рівні здійснення конкретної злочинної діяльності. В.В. Тіщенко зазначає, що "проблема злочинної діяльності, вивчення її характеру, форм і видів, ознак, структури, а також особливостей розслідування заслуговує подальшого розроблення в криміналістичній науці з метою підвищення ефективності методів, прийомів і засобів розкриття та запобігання злочинам"

тельности. / Н.П. Яблоков – М.: Юристъ, 2002. – 172 с.

191. Восстановительное правосудие: идеи и перспективы для России / Л. Карнозова, Р. Максудов., М. Флямер / Российская юстиция. Юрид. лит., 2000. - № 11. – С. 42-44.

192. Политический режим и преступность: [Под ред. В.Н. Бурлакова, Ю.Н. Волкова, В.Н. Сальникова]. – СПб.: Юридический центр Пресс, 2001. – 365 с.

193. Ільченко Н. М. Механізми реалізації державної політики у сфері засобів масової інформації (регіональний рівень): автореф. дис... канд. наук з держ. управління: 25.00.02 / Академія муніципального управління. / Ільченко Наталія Михайлівна — К., 2008. — 20с.

194. Лашкіна М. Г.. Концептуальні засади взаємодії органів державної влади та засобів масової інформації в умовах демократизації державного управління в Україні: автореф. дис... канд. наук з держ. упр.: 25.00.01 / Національна академія держ. управління при Президентові України. / Лашкіна Марія Григорівна. — К., 2008. — 20с.

195 Квашис В. Преступность и правосудие: ответы на вызовы XXI века / В. Квашис // Российская юстиция. - М.: Юрид. лит., 2000. - № 9. – с. 34-37..

196 Павлов Н.Е. Средства массовой информации в обнаружении и раскрытии взяточничества / Н.Е. Павлов // Коррупция в России: состояние и проблемы. - М., 1996. - Вып. 1. - с. 142-149.

197 Сіренко В. Час захищати правосуддя від сваволі суддів і влади / В.Сіренко // Голос України. – 2003. - 4 лютого.

198. Дрешпак В. М. Практика взаємодії органів державного управління та місцевого самоврядування із засобами масової інформації: [практикум] / Дрешпак В. М. // Національна академія держ. управління при Президентові України. Дніпропетровський регіональний ін-т держ. управління. — Д. : ДРІДУ НАДУ, 2007. — 80с.

199 Про державну таємницю Закон України // Відомості Верховної Ради України. – 1994. – № 16. – Ст. 93.

200 Про внесення змін до Закону України про державну таємницю // Відомості Верховної Ради України. – 1999. – № 49. – Ст. 428.

201 Правовые вопросы защиты информации / С.Борисов, С.Диев, С.Кравченко, Ф.Фатыхов // Бизнес и банки. – 1995. – № 45. – с. 8.

202. Смолькова И.В. Проблемы охраняемой законом тайны в уголовном процессе: дисс… д-ра юрид. наук: 12.00.09 / И.В. Смолькова. - Иркут. гос. экон. акад. – Иркутск, 1998. – 404 с.

їв, 1998. - Вип. 3. - 45 с.

175. Кобець В.В. Деякі напрямки оперативного супроводження судового розслідування злочинів / В.В. Кобець // Вісник Одеського інституту внутрішніх справ. – 1999. – № 2. – с. 88–91.

176. Преступность и статистика / Специальный выпуск по материалам зарубежной печати. – 1976. – № 7.

177. Томин В.Т. Использование средств массовой информации в борьбе с преступностью. [Учебное пособие]. / В.Т.Томин. - Горький, Горьковская высшая школа МВД СССР, 1976. – 96 с.

178. Ткаліч В.Є. Попередження злочинів – пріоритетний напрямок діяльності ОВС / В.Є. Ткаліч //Вісник Одеського інституту внутрішніх справ. - 2000. - №4. - с. 78-80.

179. Взаимодействие милиции и населения: к итогам харьковского эксперимента. – Х.: Нац. ун-т внутр дел, 2003. – 288 с.

180. "Гаряча лінія" завдасть жару харківським злочинцям // День. – 2002. - 23 січня.

181. Карпов Н.С. Злочинна діяльність: [Монографія]. / Н.С. Карпов. – К.: вид-во Семенко Сергія. 2004. – 310 с.

182. Криминалистика: [Учебник] [под ред. И.Ф. Крылова, А.И. Бастрыкина]. – М.: Дело, 2001. – 800 с.

183. Криминалистика: [Учеб. для вузов]: 2-е изд., перераб. и доп / И.Ф. Герасимов, Л.Я. Драпкин, Е.П. Ищенко и др.; [Под ред. И.Ф. Герасимова, Л.Я. Драпкина]. – М.: Высш. шк., 2000. – 672 с.

184. Криминалистика: [Учебник для вузов] / А.Ф. Волынский, Т.В. Аверьянова, И.Л. Александрова и др.; [Под ред. проф. А.Ф. Волынского]. – М.: Закон и право, ЮНИТИ-ДАНА, 1999. – 615 с.

185. Строков І.В. Правові та моральні засади застосування криміналістичних засобів. [Монографія] / Строков І.В. – К.: Редак.-видавн. центр НАВСУ, 2003. – 325 с.

186. Яблоков Н.П. Расследование организованной преступной деятельности. / Н.П. Яблоков – М.: Юристъ, 2002. – 172 с.

187. Нечистая сила – третья // Робітнича газета. – 2002. - 5 лютого.

188. Политический режим и преступность: [Под ред. В.Н. Бурлакова, Ю.Н. Волкова, В.Н. Сальникова]. – СПб.: Изд-во "Юридический центр Пресс", 2001. – 365 с.

189. Яблоков Н.П. Расследование организованной преступной деятельности. / Н.П. Яблоков – М.: Юристъ, 2002. – 172 с.

190. Яблоков Н.П. Расследование организованной преступной дея-

[70, с. 109]. Успіх розслідування залежить не тільки від професійної майстерності слідчого, а й "від глибини його знань, що характеризують передумови, природу, структуру та сутність організованої злочинності. У зв'язку з цим викликає безсумнівний інтерес поглиблений, комплексний розгляд усіх питань з метою удосконалення тактики та методики запобігання, розкриття та розслідування посягань з боку організованих злочинних формувань" [71, с. 5; 72, с. 138–139; 73].

На зорі формування поглядів про організовану злочинність досить прогресивним було введення міркувань про наявність «кримінального середовища» і про необхідність превентивних розвідувальних заходів у цьому середовищі. Багато ознак організованої злочинності базуються на специфічних правилах злочинного середовища і відносинах, що культивуються в ній [74]. Характерною рисою простору злочинності є його експансія в навколишній простір. Процес експансії - поширення своїх кордонів - відбувається саме в "межовій смузі". Для розробки соціальних технологій, спрямованих на запобігання цьому процесу, необхідно ретельне вивчення механізмів і особливостей його здійснення [75, с.117-118]. Поділяючи погляди Т.Е. Караєва, який цілком правильно уточнює, що злочинну діяльність складають також дії незлочинного характеру [76, с. 11–13].

У зв'язку з цим О.Ф. Долженков ставить питання про інфраструктуру злочинності, до змісту якої він відносить елементи, "не маючи прямого злочинного характеру, обслуговують інтереси функціонування злочинності як системи" (підготовка кадрів, злочинна субкультура, "общак" тощо), і зазначає, що небезпека недооцінки значення інфраструктури злочинності полягає у тому, що правоохоронні органи досить чітко бачать свого основного супротивника та мають певний досвід боротьби з ним, а елементи інфраструктури залишаються ніби за кадром, будучи основним живильним середовищем відтворення основних суспільно небезпечних явищ [77, с. 48–49]. Як юридичне поняття «інфраструктура злочинності» складається, на думку деяких авторів, з ряду елементів, що суттєво відрізняється своїм змістом від причин, умов, факторів (обставин), що сприяють злочинів [78, с.39] Елементи інфраструктури злочинності відіграють іншу роль у механізмі злочинної діяльності. Вони не мають прямого криміногенного характеру, а обслуговують інтереси функціонування злочинності як системи, «полегшують» її кримінальний вплив на стан оперативно-тактичної обстановки як у цілому, так і окремих її складових частин.

Необхідно визначити, що злочинність як явище та її інфраструктура перебувають у постійному взаємозв'язку і взаємодії. З посиленням криміногенних процесів у суспільстві розвивається й інфраструктура злочинно-

сті, а розвиток інфраструктури, у свою чергу, забезпечує й полегшує досягнення цілей злочинних угруповань. Злочинність і інфраструктура - динамічна і взаємодоповнююча єдність [79, с. 108-109].

Як свідчать сучасні наукові дослідження протидія злочинності є однією з найскладніших та найактуальніших проблем для усіх країн світу [80, с. 3, 81]. В юридичній літературі протидія злочинності не достаньо науково досліджена [82, с. 21-22]. В етимологічному розумінні термін "протидія" означає дію, яка спрямована проти іншої дії, перешкоджає їй [83, с. 992]. Тобто існує певний зв'язок між дією і протидією.

Шинальський О. І. [84, с. 98] під протидією злочинності розуміє цілеспрямовану діяльність, що проводиться державою та суспільством на основі наукового розуміння злочинності та причин, що її породжують. Протидія злочинності включає всі засоби і методи впливу на злочинність, до яких належать:

— загальнодержавні засоби економічного, політичного і виховного порядку, які безпосередньо не спрямовані на протидію злочинності, але справляють на неї суттєвий вплив;

— засоби законодавчого, правового порядку, що визначають основні напрями, які поєднують переконання і примус у протидії злочинності;

— діяльність державних органів, громадських організацій, правоохоронних органів та інших по виявленню причин та умов скоєння конкретних злочинів та вжиття засобів щодо їх усунення;

— безпосередня, постійна і послідовна робота правоохоронних органів по розкриттю, розслідуванню злочинів, виправленню осіб, що скоїли злочини, нагляд за особами, звільненими з місць позбавлення волі;

— проведення розшукових і оперативно-розшукових заходів, зумовлених ситуацією, що склалася.

Соціальний контроль у суспільстві має здійснюватися на такому рівні, який би забезпечував не тільки ефективність у протидії злочинності, а й обхоплював інші правопорушення або інші соціальні відхилення, які можуть у майбутньому призвести до вчинення тих чи інших видів злочинів. Проблема соціального контролю для українського суспільства у процесі розбудови суверенної, демократичної, соціально-правової держави є вельми актуальною. Оскільки це знаходить свій прояв у тому, що соціальний контроль однаковою мірою стосується як антисуспільної або протиправної поведінки, так і звичайного життя громадян та державних установ.

Соціальний контроль у цілому має слугувати дотриманню соціальних норм, включаючи норми права і кримінально-правові заборони [85, с.39]. Тому соціальний контроль, як і протидія злочинності, визнаються соціальною політикою у цілому, а не тільки каральною політикою як її складовою. Більше того, ці положення відбивають основний методологічний

”Рефл – бук”.: “Ваклер” – 2000. – 576 с.

160. Оперативно-тактичні операції: [Монографія]. / О.Ф.Долженков, В.П. Євтушок, В.Л.Ортинський, М.Б.Саакян. - Львів, Львівський юридичний інститут МВС України, 2004. – 188 с.

161. Журавльов А.В. Інтернет-спільноти у новій хвилі інформаційних війн. [Електронний ресурс] Режим доступу // http://www.specworld.com.ua/2009/03/blog-post_7856.html

162. Цюрюпа А. Ксенофобия как проявление инстинкта этнической изоляции / А. Цюрюпа [Психология национальной нетерпимости: Хрестоматия], [сост. Ю. В. Чернявская]. – Минск: Харвест, 1998. – 200 с.

163. Шерозия А. Психика, сознательное, бессознательное. / А. Шерозия. – Тбилиси: Университет, 1979. – 180 с.

164. Ядов В. А. Социальная идентичность личности. / В. А. Ядов. – М.: Прогресс, 1994. – с. 240 с.

165. Цюрюпа А. Ксенофобия как проявление инстинкта этнической изоляции / А. Цюрюпа [Психология национальной нетерпимости: Хрестоматия], [сост. Ю. В. Чернявская]. – Минск: Харвест, 1998. – 200 с.

166. Шерозия А. Психика, сознательное, бессознательное. /Шерозия А. – Тбилиси: Университет, 1979. – 180 с.

167. Ядов В. А. Социальная идентичность личности. / В. А. Ядов. – М.: Прогресс, 1994. – 240 с.

168. Почепцов Г.Г. Информационные войны. / Г.Г. Почепцов. – М.: ”Рефл – бук”.: “Ваклер” – 2000. – 576 с.

169. Політологія посткомунізму: Політичний аналіз посткомуністичних суспільств / [кер. авт. кол. В.Полохало]. К.: Політична думка, 1995. - 368 с.

170. Потятиник Б., Лозинський М. Патогенний текст. / Б.Потятиник, М. Лозинський. – Львів: Вид-во Львівського університету, 1996. – 160 с.

171. Скуленко М. І. Убеждающее воздействие публицистики./ М. І. Скуленко – К.: Вища школа, 1986. – 180 с.

172. Почепцов Г.Г. Информационные войны. / Г.Г. Почепцов. – М.: ”Рефл – бук”.: “Ваклер” – 2000. – 576 с.

173. Почепцов Г.Г. Информационные войны. / Г.Г. Почепцов. – М.: ”Рефл – бук”.: “Ваклер” – 2000. – 576 с.

174. Стратегія і тактика боротьби з організованою злочинністю та корупцією / Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при Координаційному комітеті по боротьбі з корупцією і організованою злочинністю при Президентові України. - Ки-

144 Преса у політичній системі суспільства. – К.: Либідь, 1992. – 120 с.

145 Слісаренко І. Ю. Аналіз та прогноз у висвітленні міжнародної тематики українськими засобами масової інформації. / І. Ю. Слісаренко. – К.: ПВЦ Київський університет, 1996. – 160 с.

146. Психологія: [Підручник] – 2-ге вид., стереотип. / Ю. Л.Трофімов, В. В.Рибалка, П. А. Гончарук та ін. – К / [За ред. Ю. Л. Трофімова.]: Либідь, 2000. – 576 с.

147 Тихомиров О. К. Понятие «цель» и «целеобразование» в психологии: Психологические механизмы целеобразования. /О. К. Тихомиров. - М.: Политиздат, 1977. – 160 с.

148 Философские проблемы массовых информационных процессов. – М.: Прогресс, 1990. – 180 с.

149 Психологія: [Підручник] – 2-ге вид., стереотип. / Ю. Л.Трофімов, В. В. Рибалка, П. А. Гончарук та ін. – К / [За ред. Ю. Л. Трофімова.]: Либідь, 2000. – 576 с.

150. Тихомиров О. К. Понятие «цель» и «целеобразование» в психологии: Психологические механизмы целеобразования./ О. К. Тихомиров. – М.: Политиздат, 1977. – 160 с.

151. Скуленко М. І. Убеждающее воздействие публицистики./ М. І. Скуленко – К.: Вища школа, 1986. – 180 с.

152. Скуленко М. І. Убеждающее воздействие публицистики./ М. І. Скуленко – К.: Вища школа, 1986. – 180 с.

153 Соппиков А. П. Проблема измерения конформных реакций в малых группах: Автореф. дис. канд. филос. наук. – Л., 1969. ИНИОН CD ROM серия «гуманитарные науки», записи: 1991 – 1995 гг.

154 Теория средств массовой информации и пропаганды как научная дисциплина. – М.: МГУ, 1986. – 200 с.

155 Скуленко М. І. Убеждающее воздействие публицистики. – К.: Вища школа, 1986. – 180 с.

156 Соппиков А. П. Проблема измерения конформных реакций в малых группах: Автореф. дис. канд. филос. наук. – Л., 1969. ИНИОН CD ROM серия «гуманитарные науки», записи: 1991 – 1995 гг.

157 Теория средств массовой информации и пропаганды как научная дисциплина. – М.: МГУ, 1986. – 200 с.

158. Германов В. Г.. Вплив засобів масової інформації на підсвідомість: Дис. ...канд. філологіч. наук: 10.01.08 / Германов Володимир Григорович. – Київ - КНУ ім.. Т. Шевченка. 2003. – 174 с.

159. Почепцов Г.Г. Информационные войны. / Г.Г. Почепцов. – М.:

підхід у процесі розробки та прийняття важливих державних рішень у протидії сучасній злочинності і особливо організованій.

Для ефективної протидії злочинності необхідне використання передового досвіду ОВС із розкриття та розслідування злочинів, до речі Н.С. Карпов у своєму дослідженні докладно розглянув: поняття, сутність та критерії передового досвіду, джерела інформації, форми та методи вивчення, використання його для вдосконалення розкриття та розслідування злочинів [86].

Разом із тим, аналіз досвіду злочинної діяльності, у тому числі і досвіду використання сучасних інформаційних технологій у криміналістиці, належить до маловивченої проблеми. Одна з причин цього полягає у недостатній увазі вчених до категорії досвіду та схильності до ототожнювання його з практикою або діяльністю.

З цього випливає, що вивчати, узагальнювати потрібно будь-який злочинний досвід, але особливо глибоко та всебічно необхідно аналізувати сучасні способи використання новітніх досягнень науки при вчиненні злочинів (зокрема у паливно-енергетичному комплексі, у фінансово-кредитній і банківській сферах, з використанням сучасних інформаційних технологій, у незаконному обігу наркотичних засобів, торгівлі людьми, тероризмі, вбивствах на замовлення).

Об’єктом оцінки виступає злочинний досвід індивіда, групи, організації, співтовариства, як національний, так і міжнародний та транснаціональний [87; с. 137].

Оцінюючим суб’єктом можуть бути різні організації, наукові інститути, окремі громадяни, правоохоронні структури, які відповідно до своїх функцій або наукових інтересів займаються вивченням злочинного досвіду.

Поділяючи думку А.В. Іщенка про необхідність постійного та систематичного вивчення й узагальнення і матеріалів призупинених кримінальних справ, повернених на додаткове розслідування, результати ОРД та результати оперативно-розшукових заходів, ми цілком згоді, що безпосереднє вивчення співробітником наукового чи криміналістичного підрозділу специфіки злочинної діяльності в межах дії ст. 8 Закону „Про оперативно-розшукову діяльність” навряд чи можливе й доцільне. Це повинен здійснювати фахівець оперативно-розшукової кваліфікації. Але узагальнення отриманих таким шляхом матеріалів, вважаємо, повинно здійснюватися при безпосередній участі криміналістів, що дозволить озброїти не тільки оперативно-розшукові підрозділи, а й слідчих, відповідними знаннями про способи скоєння злочинів у цих специфічних галузях.

Слід констатувати, що тенденції використання ОЗУ інформаційних технологій переростає, особливо у сфері економіки, в обов’язків атрибут, в закономірне явище. Динаміка використання ОЗУ сучасних інформаційних технологій та ЗМІ як для вчинення злочинів, так і для протидії розслідуванню викликає закономірну неготовність оперативно-розшукових та слі-

дчих підрозділів в організаційному, методичному, технічному і інформаційному відношенні адекватно вести боротьбу зі злочинністю, єдиним шляхом, який може дозволити скоротити відставання у цьому напрямку являється інтенсифікація використання інформаційних технологій при розкритті та розслідуванні злочинів, учинених ОЗУ.

1.2. Правові основи забезпечення прав людини при використанні інформаційних технологій в діяльності з розкриття та розслідування злочинів

Останнім часом Україна поступово здійснює перехід до інформатизації суспільства, який характеризується зростанням ролі інформації у соціальних процесах, швидкості її обробки, у проникненні електронно-обчислювальної техніки та заснованих на ній сучасних інформаційних технологій у всі сфери суспільного життя.

Втілення у життя умов комплексного вирішення проблем державної політики у сфері суспільних інформаційних відносин здійснюється нашою державою відповідно з Програмою інтеграції України до Європейського Союзу (розділ 13 “Інформаційне суспільство”) [88, 89].

Із часу проголошення незалежності України вже створено значний масив законодавчих та підзаконних нормативних актів, які є базою нормативно-правового регулювання суспільних інформаційних відносин. Сукупність юридичних норм в цій сфері вже досягла критичної маси, що дозволяє на науковому рівні умовно виділити їх в автономну галузь законодавства (інформаційне законодавство) та юридичну наукову інституцію (інформаційне право).

Сьогодні в Україні щодо шляхів правового регулювання інформаційних відносин формуються два напрямки: перший – базується на доктрині англо-американської системи права (фрагментарне вирішення на законодавчому рівні в окремих законах проблем правового регулювання інформаційних відносин); другий – на доктрині європейської (континентальної) системи права (легальне визначення галузей законодавства та їх систематизація на рівні кодифікації).

В останній час теорія та практика правотворення в нашій країні схиляється до другого підходу, більш традиційного для України - юридичної доктрини легальної систематизації законодавства на рівні кодифікації.

В Україні створено наукові засади щодо систематизації інформаційного законодавства на рівні Кодексу про інформацію, що є новацією в теорії права як в нашій країні, так і за кордоном. Реалізація ідеї кодифікації ін-

127 Москаленко А. З. Теорія журналістики. / А. З. Москаленко – К.: ПВЦ Київський університет, 1998. – 280 с.

128 Зимбардо Ф., Ляйппе М. Социальное влияние / Ф.Зимбардо, М.Ляйппе – СПб: Изд-во Питер, 2000. – 300 с.

129 Ионин Л. Культурный шок: конфликт этнических стереотипов / Л. Ионин [Психология национальной нетерпимости: Хрестоматия], [Сост. Ю. В. Чернявская]. – Минск: Харвест. - 1998. – 560 с.

130 Кон И. Психология предрассудка. О социально-психологических корнях этнических предубеждений / И. Кон [Психология национальной нетерпимости: Хрестоматия], [Сост. Ю. В. Чернявская]. – Минск: Харвест. - 1998. – 560 с.

131 Москаленко А.З., Губерський Л.В., Іванов В.Ф., Вергун В.А. Масова комунікація: [Підручник]. / А.З.Москаленко, Л.В.Губерський, В.Ф.Іванов, В.А.Вергун – К.: ПВЦ Київський університет, 1997. – 240 с.

132 Москаленко А. З. Комунікативна політологія: Нові тенденції розвитку мас-медіа. / А. З. Москаленко – К.: ПВЦ Київський університет, 1997. – 180 с.

133 Москаленко А. З. Теорія журналістики. / А. З. Москаленко – К.: ПВЦ Київський університет, 1998. – 280 с.

134 Політологія посткомунізму. – К.: Наукова думка, 1995. – 140 с.

135 Різун В. Літературне редагування: [Підручник] ./ В.Різун – К.: Либідь, 1996. – 240 с.

136 Буржуазная философия XX века [Под ред. Л. Н. Митрохина, Т. И. Ойзерман, Л. Н. Шершенко]. – М.: Политиздат, 1974. – 260 с.

137 Выготский Л. С. История развития высших психических функций. Т. 3. / Л. С. Выготский – М.: Педагогика, 1983. – 120 с.

138 Выготский Л. С. Собрание сочинений: В 6 томах. – Т. 2. /Выготский Л. С. – М.: Педагогика, 1984.– 160 с.

139 . Ананьин С. А. Интерес по учению современной психологии и педагогики. / С. А. Ананьин. – К.: Молодь, 1955. – 160 с.

140 Андреева Г. М. Актуальные проблемы социальной психологии. / Г. М. Андреева – М.: Изд-во Московского государственного университета, 1988. – 240 с.

141 Андреева Г. М. Социальная психология. Изд. 3-е. / Г. М. Андреева – М.: Наука, 1994. – 180 с.

142 Трофімов Ю. Л., Рибалка В. В., Гончарук П. А. та ін. Психологія: [Підручник] - 2-ге вид., стереотип. / Ю. Л. Трофімов, В. В. Рибалка, П. А. Гончарук та ін. [За ред. Ю. Л. Трофімова]. - К.: Либідь, 2000. – 576 с.

143 Скуленко М. І. Убеждающее воздействие публицистики. / М. І. Скуленко – К.: Вища школа, 1986. – 180 с.

В.С. Кузьмічов – К.: НАВСУ – НВТ “Правник”, 2000. – 450 с.

112 Хайдуков Н.П. Тактическо-психологические основы воздействия следователя на участвующих в деле лиц. / Н.П.Хайдуков. – Саратов: Изд-во Саратовского ун-та, 1984. – 124 с.

113 Словарь русского языка [упоряд. С.И.Ожегов]. – М.: Русский язык, 1984. – 797с.

114 Филосовский словарь: 4-е изд. [под ред. И.Т. Фролова].– М.: Политиздат, 1981. – 445с.

115 Психология. Словарь [под ред. П.А. Рудика]. – М.: Физкультура и спорт, 1974. – 512 с.

116 Коновалова В.Е. Организационные и психологические основы деятельности следователя. /В.Е.Коновалова – Киев: РИО МВД УССР, 1973. - 122 с.

117 Томин В.Т. Использование средств массовой информации в борьбе с преступностью. [Учебное пособие]. / В.Т. Томин. - Горький, Горьковская высшая школа МВД СССР, 1976. – 96 с.

118 Наумкин Ю.В. Взаимодействие правоохранительных органов и учреждений массовой информации в обеспечении социалистического правопорядка / автореферат дис. на соиск. уч. степени докт. юр. наук. / Ю.В.Наумкин. - М.: Академия МВД СССР, 1988. – 30 с.

119 Удовиченко В.А. Использование средств массовой информации в деятельности городских, районных органов внутренних дел. [Учебное пособие] / В.А.Удовиченко. – М., 1983. – 71 с.

120 Грошевой Ю.М. Общественное мнение и решение суда. [Конспект лекции]. /Ю.М. Грошевой – Харьков: Харьковский юрид. инст., 1972. – 40 с.

121 Український радянський енциклопедичний словник: У 3-х т. Т. 1. [Відп. ред. А.В. Кудрицький].– К.: Голов. ред. УРЕ, - 1986. – 752 с.

122 Ноэль-Норман Э. Общественное мнение. Открытие спирали молчания. /Ноэль-Норман Э. – М., 1996. – 214 с.

123 Почепцов Г.Г. Информационные войны. / Г.Г. Почепцов. – М.: ”Рефл – бук”.: “Ваклер” – 2000. – 576 с.

124 Богомолова Н. Н. Социальная психология печати, радио и телевидения. / Н. Н. Богомолова. – М.: Изд-во Московского государственного университета, 1991. – 180 с.

125 Дюркгайм Е. Самогубство: Соціол. досл. / Е. Дюркгайм [Пер. з фр. Л. Кононович]. – К.: Основи, 1998. – 420 с.

126 Ильин Е. П. Мотивация и мотивы. /Ильин Е. П.– СПб.: Питер, 2000. – 340 с.

формаційного законодавства дозволить уникнути суспільної невизначеності та багатозначності щодо змісту і сутності правового регулювання в умовах входження України в інформаційне суспільство.

Питання правового регулювання діяльності органів досудового слідства у сфері інформаційних технологій та ЗМІ під час розкриття та розслідування злочинів знайшли своє втілення в Конституції України, Кримінально-процесуальному, Кримінальному, Цивільному кодексах, Законах України “Про міліцію”, “Про прокуратуру”, “Про Службу безпеки України”, “Про основи національної безпеки України”, “Про організаційно-правові основи боротьби з організованою злочинністю”, “Про оперативно-розшукову діяльність”, “Про інформацію”, “Про друковані засоби масової інформації (пресу) в Україні”, “Про телебачення і радіомовлення”, “Про інформаційні агентства”, “Про телекомунікації”, “Про державну таємницю”, “Про державну підтримку засобів масової інформації та соціальний захист журналістів”, “Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації”, “Про демократичний цивільний контроль над Воєнною організацією і правоохоронними органами держави”, „Про визначення можливості застосування радіоелектронних засобів на території України”, Указ Президента України від 07.11.2005 N 1556 «Про додержання прав людини під час проведення оперативно-технічних заходів», Постанова КМУ України від 26 вересня 2007 р. № 1169 „Про затвердження Порядку отримання дозволу суду на здійснення заходів, які тимчасово обмежують права людини, та використання добутої інформації”, Постанова Пленуму Верховного суду від 28.03.2008 № 2 „Про деякі питання застосування судами України законодавства при дачі дозволів на тимчасове обмеження окремих конституційних прав і свобод людини і громадянина під час здійснення оперативно-розшукової діяльності, дізнання і досудового слідства” та ін.

Також було внесено на розгляд проекти нормативно-правових актів: проект Закону про внесення змін до Закону України "Про телекомунікації" (щодо безоплатного отримання рахунків за надані телекомунікаційні послуги) від 06.10.2005 (№8255), Про перехоплення телекомунікацій від 07.09.2005 (№4042-1), Про перехоплення телекомунікацій від 21.03.2005 (№4042-2), проект Закону про внесення змін та доповнень до деяких законодавчих актів України (щодо відповідальності за використання телекомунікаційної мережі для масової розсилки рекламних повідомлень) від 06.09.2004 (№6107), Про інформаційну безпеку України від 01.07.2004 (№5732), Проект Закону про внесення змін та доповнень до Закону України "Про телекомунікації" (щодо вживання мов у сфері телекомунікацій)

від 01.06.2004 (№5583), проект Закону про внесення змін та доповнень до Закону України "Про телекомунікації" від 11.05.2004 (№5491), Про моніторинг телекомунікацій від 07.08.2003 (№4042), Про внесення змін до Закону України "Про організаційно-правові основи боротьби з організованою злочинністю " від 03.06.2003 (№3577), "Про захист прав користувачів телекомунікацій" від 31.03.2003 (№3299), Про електронну торгівлю від 17.02.2003 (№3114), Про захист персональних даних від 10.01.2003 (№2618), Про інформаційну відкритість органів державної влади та вищих посадових осіб України від 20.08.2002 (№2082), Про Інформацію персонального характеру від 22.07.2002 (№2016), Про внесення змін до Закону України "Про інформацію" від 17.05.2002 (№1022) та ін.

Аналіз зазначених нормативно-правових актів констатує, що безпосередньо Конституція України не містить положень, що регулюють відносини правоохоронних органів щодо використання інформаційних технологій у сфері кримінального судочинства. Розгляд цих питань перекладається на інші закони України. Однак ряд конституційних положень гарантує право на свободу думки і слова, вільне вираження своїх поглядів і переконань (ст. 34), право на повагу особистої гідності (ст. 28), захист особистого й сімейного життя (ст. 32), презумпцію невинуватості (ст. 62).

Конституційною основою права на свободу думки і слова, на вільне вираження своїх поглядів і переконань є ст. 34 Основного Закону України. Вона гарантує право вільно збирати, зберігати, використовувати й поширювати інформацію усно, письмово або в інший спосіб – на свій вибір.

Разом із тим, право на свободу думки і слова може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя. У цих положеннях Конституції України відобразились норми міжнародних правових актів, таких як Конвенція про захист прав і основних свобод людини 1950 р., яка ратифікована Законом України від 17 липня 1997 р. (№ 475/97-ВР), Міжнародний пакт про громадянські і політичні права, який прийнято Генеральною Асамблеєю ООН 16 грудня 1966 р. й ратифіковано Указом Президії Верховної Ради Української РСР від 19 жовтня 1973 р. (№ 2148-VIII) та інші [90; 91, с. 44-45].

Інтерес людини відчувати свою автономію в суспільстві, яка захищається правом на приватність (недоторканність приватного життя), перебуває у діалектичному протиріччі з певними інтересами інших осіб і суспільства, зокрема у забезпеченні безпеки і добробуту, захисті прав і свобод

99 Стеценко Ю.В. Науково-методичні засади використання засобів масової інформації при розслідуванні злочинів: дис... канд. Юрид. наук: 12.00.09 / Стеценко Юрій Володимирович. — К., 2006. — 238 с.

100 Федотов М.А. Право массовой информации в Российской Федерации. – М.: Междунар. отношения, 2002. – 624 с.

101 Гудвин против Соединенного Королевства // Российская юстиция. – 1999. - № 7. – С. 56-58.

102 Єрмаков П.А. Використання оперативно-технічних заходів у боротьбі зі злочинністю: автореф. дис. ...канд. юрид. наук: 21.07.04 / П.А. Єрмаков. – Київ, НАВСУ 2002. – 16 с.

103 Хараберюш І.В. Використання оперативно-технічних засобів щодо протидії злочинам у сфері нових інформаційних технологій: автореф. дис. ...канд. юрид. наук:12.00.09 / І.В. Хараберюш. – Львів, ЛДУВС. 2006. – 19 с.

104 Хараберюш І. Ф. Використання оперативно-технічних засобів у протидії злочинам, що вчиняються у сфері нових інформаційних технологій: монографія / Донецький юридичний ін-т Луганського держ. ун-ту внутрішніх справ; Національний ун-т держ. податкової служби України. / Хараберюш І. Ф., Мацюк В. Я., Некрасов В. А., Хараберюш О. І. — К. : КНТ, 2007. — 195с.

105 Защита прав граждан при внедрении системы оперативно-розыскных мероприятий в сетях связи. – СПб.: Информационно-издательское агенство "ЛИК", 2000. – 352 с. Режим доступу: http://www.hro.org/editions/lic/

106 Sharon LaFraniere. Russian Spies, They've Got Mail Regulations Allow Security Services to Tap Into Systems of Internet Providers // Washington Post Foreign Service, Thursday, March 7, 2002; Page A14 Режим доступу: http://www.washingtonpost.com/wp-dyn/articles/A51550-2002Mar6.html

107 Froomkin Michael, The Death of Privacy? // 52 Stanford Law Review 1461 (May 2000)

108 Loick Coriou. 11 September 2001 - 11 September 2002. The Internet on Probation. - Reporters Without Borders / Internet Desk. - France, 2002.

109 Сумин С.А. Вопросы внедрения телекоммуникационных технологий в уголовное судопроизводство России: Воронежские криминалистические чтения: сб. науч. трудов. – Вып. 9 / С.А.Сумин, А.С.Фомина – Воронеж [под ред. О.Я. Баева].: Изд-во Воронеж гос. ун-та, 2008. - 336 с.

110 Сумин С.А. Фиксация и защита доказательственной информации на предварительном и судебном следствии: Воронежские криминалистические чтения: сб. науч. трудов. – Вып. 7 / С.А. Сумин, А.С. Фомина – Воронеж [под ред. О.Я. Баева].: Изд-во Воронеж. гос. ун-та, 2006. - 252 с.

111 Кузьмічов В.С. Криміналістичний аналіз розслідування злочинів. /

ті: Дис. канд. юрид. наук: 12.00.08. / Шинальський Олександр Іванович – К., 2003. – 195 с.

85 Карпец И.И. Проблема преступности. / Карпец И.И. – М.: Юрид. лит., 1969. – 167 с.

86 Карпов Н.С. Использование передового опыта органов внутренних дел по раскрытию и расследованию преступлений в целях совершенствования криминалистической тактики и методики: автореф. дис. канд. юрид. наук: 12.00.09. / Н.С. Карпов – К., 1989. – 24 с

87 Биленчук П.Д. Транснациональная преступность: состояние и трансформация: [Учебное пособие] / П.Д.Биленчук, С.Е. Еркенов, А.В.Кафанов [под ред. акад. П.Д. Биленчука]. – К.: Атика, 1999. – 272 с.

88 Про Програму інтеграції України до Європейського Союзу [Указ Президента України] від 14 вересня 2000 р. № 1072/2000 Режим доступу: http://portal.rada.gov.a

89 Брижко В. М.. Методологічні та правові засади упорядкування інформаційних відносин: монографія / Науково-дослідний центр правової інформатики Академії правових наук України. / Брижко В. М.. — К. : ПанТот, 2009. — 415с.

90 Конопельський В.Я. Збірник міжнародних нормативно-правових актів щодо захисту прав і свобод громадян в сфері правосуддя. / В.Я.Конопельський, В.Є. Ткаліч - Одеса: Вид-во ОІВС, 2003.- 256 с.

91 Правове регулювання інформаційної діяльності в Україні : станом на 1 січня 2001 р.: [упоряд. С.Е. Демський; відп. ред. С.П. Павлюк.]. – К.: Юрінком Інтер, 2001. – 688 с.

92 Иванский В.П. Теоретические проблемы правовой защиты частной жизни в связи с использованием информационных технологий: Дис. канд. юрид. наук: 12.00.01. - М., 1998. - 273 с.

93 Єськов С.В. Процесуальні аспекти використання в кримінальному судочинстві відомостей, отриманих під час зняття інформації з каналів зв'язку в оперативно-розшуковій діяльності: автореф. дис. канд. юрид. наук: 12.00.09 / С.В. Єськов КНУВС. – К., 2007. – 16 с.

94 Ткаліч В.Є. Тактичні засади використання інформаційних технологій в слідчій діяльності / Південноукраїнський правничий часопис. / В.Є. Ткаліч – 2008, - №3. – с.154-160

95 Темник В. Президентские наместники сводят счеты с неугодными / В.Темник. - Вечерние Вести. – 2002. - 19 сентября.

96 Іжик П. Рахунок і міра // День. – 2002. - 30 жовтня.

97 В Виннице появился двойник... "Фактов" // Аргументы и факты. – 2003. – 20 августа.

98 Панченко О. Амбіції за державний кошт // Робітнича газета. – 2003. – 26 вересня.

інших осіб. Заради цих інтересів здійснюється боротьба із злочинністю під час якої не рідко відбувається втручання у приватне життя. Однак це діалектичне протиріччя не може бути вирішено відкиданням одних інтересів на користь іншим. Стаття 32 Конституції України вказує на інтереси національної безпеки, економічного добробуту та прав людини як можливу підставу для обмеження права на приватність інформації персонального характеру, що є цілком виправданим, оскільки право на повагу до приватного життя як ширше за правовим змістом може зазнавати більших обмежень, ніж право на приватність інформації персонального характеру, яке є його складовою частиною. Отже, правове регулювання питань обробки персональних даних в діяльності правоохоронних органів покликано визначити рамки реалізації права на приватність з урахуванням інтересів суспільства у приборканні злочинності. Для його розв'язання вимагається оцінка задіяних інтересів і їх узгодження.

Питання захисту прав людини під час обробки персональних даних у сучасній правовій доктрині європейських країн охоплюються концепцією права на приватність (right to privacy – англ.). Це фундаментальне право, гарантоване серед інших міжнародних документів у галузі прав людини Європейською Конвенцією про захист прав людини і основних свобод 1950 р., ст. 8 якої проголошує:

1. Кожна людина має право на повагу до її особистого і сімейного життя, житла і таємниці кореспонденції.

2. Держава не може втручатися у здійснення цього права інакше ніж згідно із законом та у випадках, необхідних у демократичному суспільстві в інтересах національної та громадської безпеки або економічного добробуту країни, з метою запобігання заворушенням і злочинам, для захисту здоров'я або моралі чи з метою захисту прав і свобод інших людей.

У текстах спеціальних міжнародно-правових актів у галузі захисту прав людини стосовно обробки інформації персонального характеру для позначення фундаментального права людини на контроль за поводженням з персональними даними також використовується термін "приватність". Основними орієнтирам для вдосконалення законодавства України з питань захисту персональних даних та його наближення до відповідного законодавства ЄС є Конвенція Ради Європи «Про захист прав людини і основоположних свобод» від 4 листопада 1950 року, Конвенція Ради Європи від 28 січня 181 року № 108 «Про захист (прав) фізичних осіб у зв'язку із автоматизованою обробкою персональних даних» та Директива 95/46/ЄС Європейського парламенту та Ради ЄС від 24 жовтня 1995 року «Про захист фізичних осіб при обробці персональних даних і про вільне

переміщення таких даних». Про поширення концепції права на приватність на відносини з обробки персональних даних зазначається у частині третій преамбули Конвенції Ради Європи № 108 “Про захист осіб стосовно автоматизованої обробки персональних даних” (м. Страсбург, 28 січня 1981 р.), а також у пункті десятому преамбули до Директиви № 95/46 СЕ Європейського Парламенту і Ради “Про захист фізичних осіб стосовно автоматизованої обробки персональних даних та безперешкодного руху цих даних” (м. Люксембург, 24 жовтня 1995 р.). У текстах міжнародних документів, а також національних законодавчих актів країн Європейського Союзу для позначення правового механізму захисту прав осіб щодо обробки персональних даних часто використовується більш лаконічний термін “data protection”, який буквально перекладається як “захист даних” (англ.). Хоча під цим розуміється саме захист прав громадян у зв’язку з обробкою персональних даних. Тобто йдеться насправді про захист інформаційних прав і свобод, а не про захист інформації.

Сама концепція інформаційної приватності також зазнає вплив інформаційних технологій. Російським вченим В.П. Іванским відповідно до періодизації фаз розвитку інформаційного суспільства запропоновані так звані “еволюційні форми” інформаційної приватності, серед яких “масмедійна”, “комп’ютерна” і “мережева” [92, с.12]. Перелічені форми відповідають домінуючим у визначений час засобам збору і обробки інформації про людину (“основні носії інформації”). У якості таких основних носіїв інформації поступово виступають засоби масової інформації, комп’ютерні бази даних і телекомунікаційні мережі.

З появою перших комп’ютерів і автоматизованої обробки персональних даних постало питання регулювання правил поводження з даними. Перші законодавчі акти були прийнятті деякими Європейськими країнами на початку 80-х років XX ст. Серед перших національних актів про захист даних: Закон Землі Гессе ФРН (1970), Шведський Закон (1973), Закон Землі Райнланд-Фальц ФРН (1974), Федеральний Акт ФРН (1977) та ін. Разом із тим обрані цими державами підходи багато у чому не збігалися. До того ж виникла проблема обміну даними з країнами, що на той час не мали відповідного регулювання з цього питання.

Стаття 5 Конвенції Ради Європи “Про захист осіб стосовно автоматизованої обробки персональних даних” 1981 року № 108 вказує на такі принципи правомірності обробки, “якості” персональних даних з точки зору законності:

- отримуються та обробляються правомірно та законно;
- зберігаються для визначених і законних цілей та не використову-

Дону. - 1999, - 704 с.

72 Воронин Ю.А. Теория классифицирования: надежды и действительность. /Ю.А. Воронин – Новосибирск, 1981. – с.138-139

73 Комплексний підхід к вивченню системи системного впливу на організовану злочинність // Криминогенная ситуация на юге Украины: особенности и проблемы сдерживания: Сб. науч. статей: [Под ред. М.Ф. Орзиха, В.Н. Дремина]. Библиотека журнала «Юридический весник».- Одесса: Феникс, 2003. - с. 196-206.

74 Долженков О.Ф. Генезис соціальних інститутів "злодіїв у законі", "кримінальних авторитетів" в інфраструктурі злочинності / О.Ф. Долженков // Вісник Луганськ. ін-ту внутр. справ. - 2000. - № 2. - с. 178-185.

75 Саппа М.М. Простір злочинності: межові колізії / М.М. Саппа // Вісник НУВС. - 2002. - Спецвип. - с. 117-118.

76 Караев Т.Э. Повторность преступлений. /Караев Т.Э. – М.: Юрид. лит., 1983. – 102 с.

77 Долженков О.Ф. До питання про інфраструктуру злочинності / О.Ф. Долженков // Вісн. Одес. ін-ту внутр. справ. – 1998. – № 1. - с. 48–49

78 Долженков О.Ф. Основи розвідки в середовищі та інфраструктурі злочинності. [Монографія] / О.Ф.Долженков, В.А. Некрасов, Ю.Е.Черкасов. - Одеса: ОЮІ НУВС, 2003. – 726 с.

79 Іщенко А.В. Проблеми криміналістики в сучаних умовах (теоретико прикладний аспект). [Монографія] /Іщенко А.В., Павлов С.В. – Запоріжжя: КП „Видавничо поліграфічний комплекс „Запоріжжя”, 2004.- 191с.

80 Лунеев В.В. Преступность XX века: [Мировые регион. рос. тенденции: Мировой криминолог. анализ.] / Лунеев В.В. – М.: Норма, 1997. – 525 с.

81 Нікітін Ю. В. Протидія злочинності в системі забезпечення внутрішньої безпеки українського суспільства: [монографія]. / Нікітін Ю. В. — К. : ВНЗ "Національна академія управління", 2009. — 373с.; Литвинов О. М.. Соціально-правовий механізм протидії злочинності в Україні: [монографія] / Харківський національний ун-т внутрішніх справ. / Литвинов О. М — Х., 2008. — 446с.

82 Анашкин Г.З. Актуальные проблемы уголовного права : [Сб. науч. ст. / Ин-т управления, бизнеса и права; Отв. ред. А.А. Витвицкий.] / Анашкин Г.З. – Ростов на Дону, 2001. – 194 с.

83 Великий тлумачний словник сучасної української мови: [Укл. і голов. ред. В. Т. Бусел.] – К.; Ірпінь: ВТФ "Перун", 2001. – С. 992.

84 Шинальський О. І. Покарання в системі засобів протидії злочиннос-

2000. – 367 с.

59 Бахін В.П.. Вивчення злочинної діяльності з метою удосконалення криміналістичних прийомів і засобів / В.П. Бахін, В.С. Кузьмічов, О.О. Садченко – К.: Актуальні питання розслідування злочинів у сучасних умовах: тактика, методика, інформаційне забезпечення: Збірник наукових праць. УАВС, 1996. – с. 206-214.

60 Бахин В.П. Следственная практика: проблемы изучения и совершенствования. /В.П. Бахин. – К.: Лыбидь, 1991. – 142 с.

61 Манс Г.Ю. Криминалистика как прикладная дисциплина и предмет преподавания / Манс Г.Ю. – Иркутск, Труды профессоров и преподавателей Иркутского гос. ун-та. Отдел 1. - 1921.- 212 с.

62 Якимов И.Н. Практическое руководство к расследованию преступлений. / И.Н. Якимов - М., 1924 - 209 с.

63 Голунский С. А.. Техника и методика расследования преступлений вып. I. / С. А Голунский., Г. К. Рогинский. - М. [под редакцией М. С. Строговича]. - 1934. - с. 41.

64 Кузьмічов В.С. Криміналістичний аналіз розслідування злочинів. / Кузьмічов В.С. – К.: НАВСУ – НВТ "Правник", 2000. – 450 с.

65 Бахін В.П. Актуальні проблеми способу вчинення злочинів за умов істотної зміни характеру злочинної діяльності / В.П.Бахін, С.М. Зав'ялов – 2000. Науковий вісник НАВСУ.– № 2. – с. 178–182.

66 Лазеры в криминалистике и судебных экспертизах. – Киев: Вища школа, 1986. – 231 с.

67 Золотарь А.В. Возможности применения фотоакустической спектроскопии в экспертизах вещественных доказательств: Вып. 27. / Золотарь А.В. – К.: Криминалистика и судебная экспертиза., 1983. – с. 105–110.

68 Громовенко Л.И. Криминалистическое исследование средств и материалов магнитной звукозаписи: [Учеб.-практ. Пособие] / Л.И Громовенко. – Киев: КВШ МВД СССР, 1981. – 94 с.

69 Проблемы международного законодательства в уголовном судопроизводстве / Юридическая наука и образование в Республике Беларусь на рубеже XX–XXI веков., Гродно. - 1998. – с. 133–136.

70 Криминалистические аспекты изучения преступной деятельности: Проблемы государства и права Украины: Тематический сборник научных трудов. – Киев, 1992.- с. 48–49.

71 Воронцов С.А. Правоохранительные органы и спецслужбы Российской Федерации. История и современность. / Воронцов С.А.– Ростов на

ються у спосіб несумісний з цими цілями;

- мають бути адекватними, відповідними не надмірними з точки зору цілей, заради яких вони зберігаються;
- мають бути точними та у разі необхідності мають поновлюватися;
- зберігаються у формі, що дозволяє ідентифікувати суб'єктів даних не довше, ніж це необхідно для цілі, заради якої такі дані зберігаються.

Правова конкуренція задіяних інтересів, особи - у захисті приватності інформації персонального характеру, з однієї сторони, і суспільства – у здійсненні обробки персональних даних (у тому числі в цілях боротьби із злочинністю), з другої сторони, покладає на державу зобов'язання щодо визначення, встановлення і підтримання балансу цих інтересів.

Обмеження права може перетворитися на його порушення, якщо законодавством детально не регламентуються умови і порядок застосування таких обмежень, не передбачаються механізм контролю і гарантії відновлення обмежених прав. Саме такі недоліки властиві чинному законодавству України у галузі регулювання обробки персональних даних правоохоронними органами.

Частина 3 ст. 32 Конституції України надає громадянам право на доступ до відомостей, що стосуються їх особисто, які не є державною або іншою захищеною законом таємницею. Цим фактично визнається, що інформація персонального характеру може бути віднесена до державної або іншої захищеної законом таємниці, що позбавляє громадян права на доступ до неї.

Заплутаність в питанні визначення режиму інформації персонального характеру за чинним законодавством України, віднесення її чи до відкритої, чи до конфіденційної або таємної, стала однією з причин розгляду Конституційним Судом України справи щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України "Про інформацію" та статті 12 Закону України "Про прокуратуру" (справа К.Г. Устименка).

Конституційний Суд України дав офіційне тлумачення лише частинам четвертій і п'ятій статті 23 та статті 48 Закону України "Про інформацію", не знайшовши невизначеності в статтях 3, 31 , 47, як і в частині першій, другій, третій і шостій статті 23 Закону України "Про інформацію", які вимагали б офіційного тлумачення у контексті справи заявника.

На нашу думку, ч. 3 ст. 32 Конституції України слід розуміти у такому значенні, що право на ознайомлення з відомостями про себе може обмежуватися лише тоді, якщо це необхідно в інтересах національної безпеки, економічного добробуту та прав людини. Саме в цих рамках слід тлумачити вислів, "які не є державною або іншою захищеною законом таємницею".

Крім того, навіть застосовуючі обмеження права на приватність персональних даних в інтересах національної безпеки, економічного добробуту та прав людини слід виходити з принципу пропорційності. Тобто застосуванню обмежень у кожному конкретному випадку повинна передувати оцінка задіяних інтересів, наслідків дій правоохоронних органів, які обмежують права громадян тощо. Таку функцію повинен виконувати незалежний контрольний орган, насамперед, суд. Для цього законодавство повинно детально визначити порядок і підстави застосування обмежень, умови, межі, строки та інші суттєві ознаки цих обмежень.

Згідно з Постановою Пленуму Верховного суду від 28.03.2008 № 2 „Про деякі питання застосування судами України законодавства при дачі дозволів на тимчасове обмеження окремих конституційних прав і свобод людини і громадянина під час здійснення оперативно-розшукової діяльності, дізнання і досудового слідства" зазначається, що відповідно до ст. 64 Конституції України конституційні права і свободи людини і громадянина не можуть бути обмежені, крім випадків, передбачених Конституцією України.

Як зазначає Єськов С.В. обмеження прав громадян на таємницю телекомунікацій може відбуватися в таких сферах: у сфері кримінального судочинства; у розвідувальній і контррозвідувальній сферах при забезпеченні державної безпеки; в умовах надзвичайного стану [93, с.7]. Конституцією і законами України передбачається можливість тимчасового обмеження конституційних прав і свобод людини і громадянина, передбачених статтями 30, 31, 32 Конституції України, під час проведення ОРД, дізнання та досудового слідства. Підстави і порядок здійснення заходів, пов'язаних із тимчасовим обмеженням цих конституційних прав і свобод людини і громадянина, визначені Кримінально-процесуальним кодексом України, законами України від 18 лютого 1992 р. "Про оперативно-розшукову діяльність", від 20 грудня 1990 р. "Про міліцію", від 26 грудня 2002 р. "Про контррозвідувальну діяльність", від 30 червня 1993 р. "Про організаційно-правові основи боротьби з організованою злочинністю". Відповідно до пунктів 7, 9 ч. 1, ч. 2 ст. 8 Закону України "Про оперативно-розшукову діяльність", п.6 ч.2 ст.7 Закону України "Про контррозвідувальну діяльність", ст. 15 Закону України "Про організаційно-правові основи боротьби з організованою злочинністю" за вмотивованим рішенням суду можуть бути застосовані такі обмеження конституційних прав і свобод людини і громадянина, передбачених статтями 30, 31, 32 Конституції України : негласне проникнення до житла чи до іншого володіння особи; зняття інформації з каналів зв'язку; контроль за листуванням, телефонними розмовами, телеграфною та іншою кореспонденцією; застосування інших технічних засобів одержання інформа-

организованными группами и преступными организациями. /В.Ю Шепитько. – Х., 2000. – 88 с.

47 Мельник М.І. Корупція: сутність, поняття, заходи протидії: [Монографія]. /М.І. Мельник – К.: Атіка, 2001. – 304 с.

48 Про підсумки розгляду звіту Голови Комітету Верховної Ради України з питань боротьби з організованою злочинністю і корупцією, доповідей Голови Координаційного комітету по боротьбі з організованою злочинністю, Голови Служби безпеки України, Міністра внутрішніх справ України про стан боротьби з організованою злочинністю, а також доповіді Генерального прокурора України про стан прокурорського нагляду у сфері боротьби з організованою злочинністю: Постанова Верховної Ради України від 26 грудня 2002 р. / Голос України. – 2003. - 21 січня.

49 Яблоков Н.П. Расследование организованной преступной деятельности. / Н.П. Яблоков – М.: Юристъ, 2002. – 172 с.

50 Яблоков Н.П. Расследование организованной преступной деятельности. / Н.П. Яблоков - М.: Юристъ, 2002. - 172 с.

51 Федотов М.А. Право массовой информации в Российской Федерации. / М.А. Федотов - М.: Междунар. отношения, 2002. - 624 с.

52 Шепитько В.Ю. Теория криминалистической тактики: [Монография]. /В.Ю.Шепитько – Харьков: "Гриф", 2002. – 349 с.

53 Криминалистика: [учеб. для вузов] 2-е изд., перераб. и доп./ И.Ф. Герасимов, Л.Я. Драпкин, Е.П. Ищенко и др.; [Под ред. И.Ф. Герасимова, Л.Я. Драпкина.] – М.: Высш. шк., 2000. – 672 с.

54 Криминалистика: [Учебник]: [под ред. И.Ф. Крылова, А.И. Бастрыкина]. – М.: Дело, 2001. – 800 с.

55 Криминалистика: [Учебник для вузов] / А.Ф. Волынский, Т.В. Аверьянова, И.Л. Александрова и др.; [Под ред. проф. А.Ф. Волынского]. – М.: Закон и право, ЮНИТИ - ДАНА, 1999. – 615 с.

56 Кримінал у потаємних кутках мережі // Міліція України. – 2001. - № 8. Фашизм – психологічна проблема? // Дзеркало тижня. – 2002. - 23 березня.

57 Поливанюк В. Д.. Особливості розслідування злочинів, вчинених у банківській системі України з використанням сучасних інформаційних технологій: дис... канд. юрид. наук: 12.00.09 / Запорізький юридичний ін-т Дніпропетровського держ. ун-ту внутрішніх справ. / Поливанюк Василь Дмитрович — Запоріжжя, 2007. — 215 с.

58 Овчинский С.С. Оперативно-розыскная информация / Овчинский С.С. – М. [Под ред. Овчинского А.С. и Овчинского В.С.]: ИНФРА – М.,

33 Зелинский А.Ф. Криминология. Курс лекций. /Зелинский А.Ф. - Х.: Прапор, 1996. - 260 с.

34 Словарь русского языка: В 4-х т.: 2-е изд., испр. и доп. / АН СССР, Ин-т рус. яз. [под ред. А. П. Евгеньевой].– М.: Русский язык, 1981–1984.

35 Про організаційно-правові основи боротьби з організованою злочинністю: Закон України від 30 червня 1993 року №3341-XII: [Збірник нормативних актів України з питань правопорядку]. – К.: Штаб МВС України., 1993. - 507 с.

36 Толковый словарь живого великорусского языка. В 4 т. [упоряд. В.И.Даль] - М.: Гос. издательство иностранных и национальных словарей, 1956.

37 Корж В.П. Криміналістична характеристика організованих злочинних утворень у сфері економіки / В.П. Корж – К.: Вісник Верховного Суду України.: Видавничий Дім "Ін Юре", 2002. – №4(32). – с. 45.

38 Науково-практичний коментар до Кримінального кодексу України: У двох частинах. Особлива частина. [Під заг. Ред. М.О.Потебенька, В.Г.Гончаренка]. – К.: Форум, 2001 р. – 942 с.

39 Гуров А.И. Профессиональная преступность. Прошлое и современность. /А.И. Гуров – М.: Юридическая литература, 1990. – 304 с.

40 Криміналізація участі в організованій злочинній діяльності // Проблеми боротьби з організованою злочинністю в регіоні (на матеріалах Харківської та Полтавської областей): [Зб. матеріалів міжнар. наук.-практ. Конф]. – Х.: Право, 2000. – с. 78.

41 Потайчук І.В. Організація та тактика виявлення організованих злочинних груп загально кримінальної спрямованності: автореф. дис. ...канд. юрид. наук: 21.07.04 / Потайчук І.В. - ОДУВС. – Одеса, 2008. – 20 с.

42 Доклад генерального секретаря Организации Обьединенных Наций “Воздействие организованной преступной деятельности на общество в целом»// Комиссия ООН по предупреждению преступности уголовному правосудию. Вена, 13-23 апр., E/CN/ 15/1993/3.

43 Дулов А.В. Основы расследования преступлений, совершенных должностными лицами. /Дулов А.В. – Минск: Изд-во “Университетское”, 1985. – 168 с.

44 Зелинский А.Ф. Криминальная психология. / А.Ф. Зелинский - К.: Юринком Интер, 1999. - 240 с.

45 Гуторова Н.А. Соучастие в преступлении по уголовному праву Украины: [Учеб.пособие] / Н.А. Гуторова - Х.,1997. - 102 с.

46 Шепитько В.Ю Тактика расследования преступлений, совершаемых

ції. КПК передбачено можливість застосування таких обмежень зазначених конституційних прав і свобод людини і громадянина: огляд та обшук житла чи іншого володіння особи (ст. 14-1, ч. 5 ст. 177; ч. 4 ст. 190 КПК); примусова виїмка із житла чи іншого володіння особи (ст. 14-1, ч. 4 ст. 178 КПК); арешт на кореспонденцію і зняття інформації з каналів зв’язку (ст. 14-1, ч. 4 ст. 187 КПК); огляд і виїмка кореспонденції та дослідження інформації, знятої з каналів зв’язку (ст. 187-1 КПК).

Обмеження вказаних конституційних прав і свобод людини і громадянина під час проведення ОРД, дізнання та досудового слідства допускається лише за вмотивованим рішенням суду (крім випадку, передбаченого ч. 3 ст. 30 Конституції України) і носять винятковий та тимчасовий характер. До порушення кримінальної справи вони застосовуються з метою запобігання тяжкого чи особливо тяжкого злочину, якщо іншим способом одержати інформацію неможливо. Надання дозволу на проведення оперативно-розшукових заходів після порушення кримінальної справи не залежить від тяжкості злочину. У випадках, передбачених п. 4 ч. 1 ст. 8 Закону України "Про оперативно-розшукову діяльність", п. 5 ч. 2 ст. 7 Закону України "Про контррозвідувальну діяльність", за рішенням суду можуть бути витребувані документи та дані, що характеризують діяльність підприємств, установ, організацій, а також спосіб життя окремих осіб, підозрюваних у підготовці або вчиненні злочину, джерело та розміри їх доходів.

Більшість питань обробки персональних даних у діяльності правоохоронних органів України регулюються відомчими нормативними актами з грифом „таємно”. В той же час, стаття 32 Конституції України встановлює, що випадки застосування обмежень права на приватність персональних даних повинні визначатися законом. Це означає, що підзаконні нормативні акти, а тим більше відомчі “для службового користування” не можуть встановлювати будь-яких обмежень прав і свобод людини. Таким чином вважаємо за потрібне врахувати це при розробці Кримінально-процесуального кодексу і пропонуємо перебачити розділ „Порядок тимчасового обмеження окремих конституційних прав і свобод людини і громадянина під час здійснення оперативно-розшукової діяльності, дізнання і досудового слідства”.

Також для ліквідації існуючих недоліків і прогалин у законодавстві, що регулює обробку персональних даних в діяльності правоохоронних органів, вимагається прийняття як базового закону, що захищатиме право громадян на приватність персональних даних, так і спеціальних законів з обробки персональних даних у діяльності правоохоронних органів України. Але прийняття Закону України «Про захист персональних даних» від

10.01.2003 (№2618), в такій редакції, яка знаходиться на розгляді комітету ВР України може тільки додати трудностей для функціонування автоматизованих систем в правоохоронних органах, також, слід зазначити, що в Законах України «Про міліцію» та «Про оперативно-розшукову діяльність» є посилання на введення в системі МВС України та суб'єктів оперативно-розшукової діяльності обліків (п.п.4, 13 ст.11 Закону України «Про міліцію») та застосовування автоматизованих інформаційних систем (п.17 ст.8 Закону України «Про оперативно-розшукову діяльність»). Це обумовлює потребу сьогодення законодавчого врегулювання питань застосування обмежень права на приватність персональних даних. У цьому може бути корисним досвід європейських країн [94].

Також слід зазначити, неналежний рівень правового забезпечення, а також різне розуміння науковців стосовно проведення ОРД і порушення кримінальних справ за повідомленнями ЗМІ.

Повідомлення ЗМІ, із яких правоохоронні органи мають можливість отримувати інформацію про підготовку або вчинення злочинів, можуть бути різного роду – матеріали про результати журналістських розслідувань злочинних діянь, які не відомі правоохоронним органам, наприклад, корупційних діянь з указуванням винних осіб або без нього [95]. Також це можуть бути аналітичні матеріали [96], інтерв'ю [97], репортажі [98] тощо.

Поділяючи думку Ю.В.Стеценка, якщо матеріали ЗМІ про підготовку чи вчинення злочину можливо перевірити шляхом відібрання пояснень від указаних у повідомленні громадян або в разі сприяння працівниками ЗМІ розкриттю та розслідуванню злочинів наданням документів, іншої інформації, яка може стати доказами, викриттям джерел інформації та іншим чином або коли таке повідомлення містить інформацію про події та факти кримінального характеру, перевірка яких не потребує проведення оперативно-розшукових заходів, то тоді кримінальна справа порушується за п. 4 ст. 94 КПК України – "повідомлення, опубліковані в пресі" [99, с.48]

Слід також відмітити, про невідповідність деяких положень чинного занодавства, які обмежують свободу діяльності засобів масової інформації, пов'язану зі встановленням та розслідуванням журналістами причин та умов певних подій, фактів пов'язаних із скоєнням злочинів. Адже ст. 32 не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом і лише в інтересах національної безпеки, економічного добробуту та прав людини. Слід врахувати, що ст. 26 Закону України "Про друковані засоби масової інформації (пресу) в Україні" дозволяє журналісту збереження таємниці авторства та джерел інформації, за винятком

проблемы./ Р.С.Белкин, А.И.Винберг. - М.: Юрид. лит., 1969. – 216 с.

23 Салтевский М.В. Собирание криминалистической информации научно-техническими средствами на предварительном следствии: [Учебное пособие]. / М.В.Салтевский – К.: НИиРИО КВШ МВД СССР, 1980. – 111 с.

24 Денісова О. О. Інформаційні системи і технології в юридичній діяльності: [Навч. посібник.] / О. О. Денісова - К.: КНЕУ, 2003. - 315 с.

25 Ромашко С. Інформаційні технології в державному управлінні: [навч. посіб.] / Ромашко С. Новосад В., Козій Б.. // Львівський регіональний ін-т держ. управління Національної академії держ. управління при Президентові України. — Л. : ЛРІДУ НАДУ, 2007. — 264с.

26 Вехов В.Б.. Расследование компьютерных преступлений в странах СНГ: Монография / В.Б. Вехов, В.А. Голубев.- Волгоград [под. ред. заслуженного деятеля науки Российской Федерации, д-ра юрид. наук, проф. Б.П. Смагоринского]: ВА МВД России, 2004. - 304с.

27 Проблемы выявления, фиксации и изъятия следов преступлений, совершенных с применением компьютерных технологий: збірник наукових праць Харківського Центру по вивченню організованої злочинності спільно з Американським Університетом у Вашингтоні. Вип.9.- Харків: Східно-регіональний центр гуманітарно-освітніх ініціатив, 2004. – с.278-309.

28 Пономарев Д. А. Информационные технологии как криминогенный фактор организованной преступности в условиях глобализации. [Електронний ресурс] / Пономарев Д. А. - Режим доступу до журн.: - http://www.ifap.ru/pi/06/r16.htm

29 Бірюков Г. М. Злочинні технології ухилення від сплати податків: [навч. посібник для студ. вищ. навч. закладів] / Бірюков Г. М. // Національний ун-т держ. податкової служби України. — Ірпінь : Національний ун-т ДПС України, 2008. — 146с.

30 Карпець О. Фашизм – психологічна проблема? / О. Карпець, 2002: Дзеркало тижня. –- 23 березня.

31 О внесении дополнений и изменений в закон об уголовной ответственности за государственные преступления и в основы уголовного законодательства [Указ Президиума Верховного Совета СССР] от 18 мая 1961 г. // Ведомости Верховного Совета СССР. - 1961. - №21. - ст. 222.

32 Про внесення змін і доповнень до Кримінального та Кримінально-процесуального кодексу Української РСР [Указ Президії Верховної Ради УРСР] від 27 червня 1961 р. // Відомості Верховної Ради УРСР. - 1961. - №28. - с. 342.

14 Федорович В.Ю. Организационные и научно-технические основы использования автоматизированных дактилоскопических систем в раскрытии и расследовании преступлений: дис... канд. юрид. наук /В.Ю.Федорович. - М., 2000. - 209 с.

15 Словарь психолога-практика. / [авт.- уклад. Головин С.Ю. - Мн.: Харвест АСТ, 2001. - 976 с.

16 Бірюков В.В. Використання комп'ютерних технологій для фіксації криміналістично значимої інформації у процесі розслідування: дис… канд. юрид. наук: 12.00.09. / В.В. Бірюков - Луганськ, 2000. – 206 с.

17 Криминалистика: [Учебник для вузов: 2-е изд. перераб. и доп.] / Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. [Под ред. заслуженного деятеля науки РФ, проф. Р.С. Белкина]. - М.: Изд-во НОРМА, 2003. – 992 с.

18 Сегай М.Я. Научно-технический прогресс и методологические проблемы судебной экспертизы материальных следов преступления: Вып. 10 / М.Я.Сегай – К. Криминалистика и судебная экспертиза. Республиканский междуведомственный сборник научных и научно-методических работ: Вища шк., 1973. - 416 с.

19 Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия / / В.Б.Вехов - М. [Под ред. акад. Б.П. Смагоринского]: Право и Закон, 1996. – 182 с.; Специализированное программное обеспечение при расследовании компьютерных преступлений: Криминалистическая экспертиза: исследование документов. Межвузовский сборник научных статей / [Науч. ред.: Морозов Б.Н.] - Саратов: Изд-во Сарат. юрид. ин-та МВД РФ, 1999. - 72 с.

20 Проблемы противодействия преступности в информационно-психологической сфере: Сборник тезисов докладов VI Международной конференции «Информатизация правоохранительных систем». - М., 1997. - с. 11; Современные информационные технологии в деятельности следователя: Международная научная конференция «Информатизация правоохранительных систем». - М., 1999. - с. 66-68.

21 Проблемы использования специальных познаний при раскрытии и расследовании преступлений в сфере компьютерной информации: Международная научная конференция «Информатизация правоохранительных систем». - М., 2000. - с. 429. Правовое регулирование отношений в информационной сфере: X Международная научная конференция «Информатизация правоохранительных систем». - М., 2001. - с. 66-72.

22 Белкин Р.С. Криминалистика и доказывание: методологические

випадків, коли ці таємниці обнародуються на вимогу суду. Тобто журналіст не зобов'язаний давати свідчення правоохоронним органам щодо встановленого ним факту скоєння злочину, його свідків, що містяться в підготовленому ним повідомленні ЗМІ. Право журналіста на відмову від дачі показань як свідка або викриття джерел інформації закріплено у ряді міжнародно-правових документів (напр., у Резолюції Європейського парламенту про конфіденційність журналістських джерел від 18 січня 1994 р., Софійській декларації ЮНЕСКО 1997 р., Резолюції про права та свободи журналістів, прийнятій на 4-й Європейській конференції міністрів по політиці у сфері ЗМІ (Прага, 1994 р.) [100, с. 333-334] та інші), а також у нормах кримінально-процесуального законодавства багатьох країн світу. Захист джерел інформації отримав закріплення у міжнародних актах про свободи журналістів (наприклад, Резолюція про свободи журналістів і права людини, прийнята на четвертій конференції міністрів європейських країн у Празі 7-8 грудня 1994 р., Резолюція Європейського парламенту про конфіденційність журналістських джерел від 18 січня 1994 р.) [101, с. 58].

У порівняні з уже звичайними засобами передачі інформації, такими як телебачення чи радіомовлення, Інтернет є новим видом медіуму з унікальними характеристиками. Унікальність цієї мережі полягає у тому, що вона функціонує не тільки як звичайний транслятор, тобто поширювач інформації, але до того ж є комунікаційним засобом для спілкування між людьми.

Як будь-яку іншу технологію для передачі інформації, Інтернет можна використовувати з метою порушення прав окремих індивідів, поширюючи образливу чи протизаконну інформацію або ж порушуючи таємницю листування в Інтернет, збираючи інформацію персонального характеру про користувачів без їх згоди тощо. Однак ці проблеми слід вирішувати у спосіб, який не буде перекреслювати позитивний потенціал Інтернет як інструменту демократизації суспільств і захисту прав і свобод людини незалежно від кордонів.

Так технології блокування, фільтрування чи маркування можуть перешкодити індивідам користуватись Інтернет для обміну повідомленнями за тематиками, що можуть бути неоднозначними чи непопулярними. Це надаватиме можливість розвитку шаблонів на рівні держав і сприятиме створенню глобальної/універсальної рейтингової системи бажаної деякими урядами, тим самим блокуючи доступ до змісту в цілих доменах, блокуючи доступ до змісту Інтернет доступному у будь-якому домені чи сторінці, які містять специфічні ключові слова чи ланцюжки символів в адресі. Це може бути поширено набагато далі за початкові рейтингові категорії запроваджені самостійно творцями змісту і провайдерами.

З огляду на постійні посягання на свободу слова в Інтернет, правозахисники пропонують визнати на міжнародному рівні і просувати два важливі принципи свободи вираження поглядів, які мають безпосереднє значення для Інтернет:

Перший з них, це однозначна заборона попередньої цензури, тобто, вимоги офіційного погодження комунікацій перед тим, як зробити їх публічно доступними. Така практика використовувалась репресивними урядами проти преси і може бути застосована проти електронних комунікацій. Другий - це однозначна заборона обмеження свободи вираження поглядів непрямими методами, такими як зловживання контролем над обладнанням чи частотами поширення інформації; чи будь-якими іншими засобами спрямованими на перешкоджання комунікаціям і циркуляції ідей і поглядів.

Здійснення оперативно-розшукових заходів із застосуванням електронних комунікацій в глобальній мережі підлягає щонайменше такому ж самому контролю і законодавчому обмеженню, як прослуховування телефонних розмов.

Оперативно-технічні заходи супроводжуються з суттєвим обмеженням прав, свобод і законних інтересів людини, передбачених Конституцією України [102, с.6]. Приведення використання оперативно-технічних засобів у відповідність до світових стандартів та враховуючи вимоги Указу президента України від 7 листопада 2005 року №1556/2005 «Про додержання прав людини під час проведення оперативно-технічних заходів», потребує розробки базовий закон з цього приводу, і як зазначав Хараберюш І.Ф. єдина міжгалузева інструкція щодо взаємодії усіх суб'єктів відносин у сфері моніторингу телекомунікаційний та під час проведення відповідних оперативно-технічних заходів у телекомунікаційних мережах [103, с.14, 104]. Перехоплення персональних комунікацій в Інтернет дозволяє не тільки дізнатися про зміст он-лайнового спілкування підозрюваних осіб, а надає набагато більше інформації про особу, яка в більшій частині не стосується безпосередньо мети перехоплення, але є надзвичайно вразливою як для об'єкта стеження, так і його респондентів. Серед такої вразливої інформації може бути інформація про стан здоров'я, фінансові дані, відомості про сексуальне життя та багато іншого, що може бути використано без згоди і не в інтересах користувачів Інтернет. Стеження в Інтернет фактично поєднує усі можливі традиційні засоби негласного збирання різнопланової інформації про людину, але у набагато вразливіший спосіб. Це вимагає запровадження чітких і детальних правил для здійснення оперативно-розшукових заходів в комп'ютерних мережах і лише у виняткових випадках, за умови ефективного контролю за діяльністю спецслужб.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Лайон Д. Інформаційне суспільство: проблеми та ілюзії / Д. Лайон. - К.: Сучасна зарубіжна соціальна філософія, 1996. - с.362-380.

2 Денісова О. О. Інформаційні системи і технології в юридичній діяльності [Навч. посібник]. / О. О.Денісова. - К.: - КНЕУ, 2003. - 315 с.

3 Советский энциклопедический словарь. - М.: [Советская энциклопедия]. - 1979. – 1599 с.

4 Словарь русского языка [авт.-уклад. Ожегов С. И.]. - 21-е изд., перераб. и доп.: Рус. яз. - М.: [под. ред Н.Ю.Шведовой]. 70000 слов., 1989. - 924 с.

5 Новий тлумачний словник української мови. [авт.-уклад. проф. В.В. Яременко, к.філол.н. О.М. Сліпушко.].: 3-й том – К.: Вид-во "Аконіт". 2001.- 863 с.

6 Дяблова Ю.Л. О гносеологической сущности информационных технологий / Ю.Л. Дяблова // Воронежские криминалистические чтения: сб. науч. трудов. – Вып. 9 / [под ред. О.Я. Баева]. – Воронеж: Изд-во Воронеж. гос. ун-та, 2008. - 336 с.

7 Возможности применения информационно-интеллектуальных систем для решения задач в судебном почерковедении: Сб. науч. статей / Актуальн. вопр. угол. судопроизв. и криминалист. – М.: Акад. Упр. МВД России, 2007. – с. 191-194

8 Дяблова Ю.Л. О гносеологической сущности информационных технологий/ Ю.Л. Дяблова // Воронежские криминалистические чтения: сб. науч. трудов. – Вып. 9 / [под ред. О.Я. Баева]. – Воронеж: Изд-во Воронеж. гос. ун-та, 2008. - 336 с.

9 Об информации, информационных технологиях и о защите информации / Федеральный закон от 27 июля 2006 г. №149-ФЗ / Рос. газета. - 2006. - №165

10 Про Національну програму інформатизації / Закон України від 4 лютого 1998 р. №74/98-ВР // Юрид. Вісн. України.- 1998. - №18.

11 Криминалистика: [Учебник для вузов: 2-е изд. перераб. и доп.] / Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. [Под ред. заслуженного деятеля науки РФ, проф. Р.С. Белкина]. – М.: Издательство НОРМА, 2003. – 992 с.

12 Оперативно-розыскная деятельность: Учебник. / [Под ред. К.К. Горяинова]. – М.: ИНФРА , 2002. – 794 с.

13 Денісова О. О. Інформаційні системи і технології в юридичній діяльності [навч. посібник] / О. О.Денісова - К.:. КНЕУ, 2003. — 315 с.

	Створення злочинної організації	7	9	28.6	9	13	44.4	8	12	50.0		
	Сприяння учасникам злочин організацій та укриття їх злочин. діяльності											
	Бандитизм	17	27	58.8	27	20	-25.9	14	12	-14.3		
	Умисне вбивство (та замах)	34	40	17.6	40	45	12.5	33	14	-57.6		
	у т.ч. вчинене на замовлення	2	2		2	9	4,5 р	6	1	-83.3		
	Розбій	232	185	-20.3	185	129	-30.3	93	73	-21.5		
	Вимагання	13	44	3.4 р	44	29	-34.1	13	7	-46.2		
	Захоплення заручників	2	1	-50.0	1				1			
	Торгівля людьми або ін. незак. угода щодо передачі людини	101	91	-9.9	91	90	-1.1	40	50	25.0		
	Незаконний обіг зброї (ст. ст. 262, 263 КК)	37	36	-2.7	36	22	-38.9	19	15	-21.1		
	Злочини у сфері обігу нарк. засобів, психотр. речов., їх аналог. або прекур.	789	957	21.3	957	770	-19.5	516	682	32.2		
	Крадіжка	653	660	1.1	660	528	-20.0	394	353	-10.4		
	Привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем	166	180	8.4	180	181	0.6	103	216	109.7		
	у т.ч. в особливо великих розмірах	129	119	-7.8	119	103	-13.4	73	100	37.0		
	Злочини у сфері службової діяльності	208	271	30.3	271	206	-24.0	184	148	-19.6		
	зловживання владою або службовим становищем	65	72	10.8	72	37	-48.6	52	48	-7.7		
	у т.ч. перевищення влади або службових повноважень	7	7		7	1	-85.7					
	хабарництво	27	43	59.3	43	31	-27.9	14	31	121.4		
	Легалізація (відмивання) доходів,одержаних злочинним шляхом	44	110	2.5 р	110	57	-48.2	44	48	9.1		
	Шахрайство з фінансовими ресурсами	57	43	-24.6	43	13	-69.8	1		-100.0		
	У членів ОГ і ЗО вилучено вогнепальної зброї (одиниць)	60	53	-11.7	53	30	-43.4	21	17	-19.0		
	наркотичних засобів (г)	472490	232023	-50.9	232023	558678	2,4 р	133421	191252	43.3		
	автомобілів (шт.)	38	27	-28.9	27	39	44.4	22	33	50.0		

Правоохоронні органи в деяких країнах намагаються нав'язати телекомунікаційним компаніям співробітництво, за умовами якого на останніх покладають зобов'язання надавати їх службовцям фізичний доступ до комунікаційного обладнання, а також здійснювати інсталяцію обладнання для автоматичного перехоплення повідомлень за рахунок операторів. Такі переговори часто відбуваються без ознайомлення громадськості, а самі умови співробітництва засекречуються.

В Росії Федеральна служба безпеки з 1995 р. пропонувала провайдерам впровадження системи оперативно-розшукових заходів в мережі (СОРМ). Ці пропозиції зустріли протести лише лічених провайдерів, які ризикуючи втратою ліцензії відстоювали не тільки свої майнові інтереси, але й права і свободи громадян. Запропонований службовими документами ФСБ Росії порядок доступу до телекомунікаційного обладнання для зняття інформації не передбачав пред'явлення провайдерам документів, які санкціонували б такі оперативні заходи, виключає їх участь в процесі доступу до обладнання, а також покладає на них зобов'язання за власний рахунок придбати і встановити обладнання для стеження [105].

У країнах, де існує монополія чи суттєвий вплив держави на телекомунікаційний ринок через ліцензування діяльності на ньому, відсутня координованість дій учасників цього ринку, - порушення конституційних прав громадян не зустрічає протестів з боку операторів, яким спецслужби нав'язують співробітництво для суцільного стеження за користувачами Інтернет [106].

Нові технології значно спрощують суцільне стеження за людиною, тобто негласне збирання інформації персонального характеру не тільки з боку спецслужб, але й приватних компаній. Як із занепокоєнням зазначає американський професор права М. Фрумкін, "якщо існуючі тенденції залишаться незмінними, колись, не так далеко у майбутньому, на землі не буде місця, де звичайна людина буде мати можливість уникнути стеження" [107].

Наприклад, в США, усього через два дні після атак, 13 вересня 2001 року, приймається Акт про приборкання тероризму (Combating Terrorism Act), який дозволяє спецслужбам використовувати систему запису й зберігання даних щодо користування Інтернет (traffic data), без попереднього одержання судового ордера.

24 жовтня 2001 року Палата Представників США ухвалює антитерористичний закон за назвою "Патріотичний закон США" (USA Patriot Act), яким підтверджуються раніше надані повноваження ФБР щодо інсталяції програмного забезпечення Carnivore ("Хижак за комахами"), для суцільного пере-

хоплення електронних комунікацій осіб, які мають закордонні контакти.

Криптографічне програмне забезпечення також підпало під атаку ФБР за допомогою програми Magic Lantern ("Магічний Ліхтарик"), яка розсилає електронною поштою вірус, призначений для секретного запису вчинених натискань на клавіатуру користувачами Інтернет. Це надає ФБР можливість дізнатися про використовувані криптографічні коди для розшифрування повідомлень, що надсилаються з комп'ютерів.

Одним з значних документів цього періоду є лист Президента США Джорджа Буша до Європейського Союзу датований 16 жовтня 2001 року, яким пропонується низка вимог щодо співробітництва між США і ЄС проти тероризму. Це включає обмін телекомунікаційними даними, прямий обмін інформації з Європолом, запровадження спільного поліцейського контролю на кордонах, включаючи обмін даними про осіб, що шукають притулку, і нову категорію "небажаних" осіб, яким відмовлятиметься у в'їзді.

У Доповіді «Інтернет - на випробуванні», підготовленій правозахисною організацією «Репортери без кордонів», відслідковуються зміни, яких зазнала політика щодо перехоплення електронних комунікацій як європейських, так й інших країн:

Німеччина - ліквідація відмінностей між повноваженнями поліції і служб безпеки щодо зняття інформації з каналів зв'язку, надання останній необмеженого доступу до поліцейської бази даних;

Канада - стеження за активністю в Інтернет і перехоплення електронних повідомлень - в основі канадського антитерористичного закону С-36;

Данія - запроваджене зберігання даних про користування телекомунікаціями на строк до одного року, антитерористичне законодавство дозволило поліції ознайомлюватися з зібраними відомостями без попереднього судового дозволу і вмонтовувати системи стеження за електронним листуванням в обладнання провайдерів;

Іспанія - прийнятий у липні 2002 року закон зобов'язує зберігати відомості про користування Інтернет щонайменше впродовж річного строку, однак поліції заборонено мати до них доступ без судового ордера;

Франція - змінами у законодавстві збільшено строк зберігання записів про користування послугами і електронне листування до одного року, надано повноваження для судів використовувати секретні засоби для декодування і вимагати від компаній надання кодів від їх програмних засобів для шифрування;

Велика Британія - закон прийнятий у грудні 2001 року збільшив до од-

Організована злочинність		2006	2007	Динаміка, %	2007	2008	Динаміка, %	Торік	Поточний рік	Динаміка, %
Виявлено організованих груп і злочинних організацій		466	420	-9.9	420	378	-10.0	244	246	0.8
З них	загальнокримінальної спрямованості	305	268	-12.1	268	237	-11.6	154	155	0.6
	економічної спрямованості	161	152	-5.6	152	141	-7.2	90	91	1.1
	з корумпованими зв'язками	26	13	-50.0	13	15	15.4	8	17	112.5
	з міжнародними зв'язками	28	29	3.6	29	18	-37.9	10	8	-20.0
	у сфері зовнішньоекономічної діяльності	7	7		7	5	-28.6	5	2	-60.0
	у фінансово-кредитній системі	50	61	22.0	61	70	14.8	41	36	-12.2
	у сфері приватизації	7	6	-14.3	6	2	-66.7	1		-100.0
	у паливно-енергетичному комплексі	14	13	-7.1	13	7	-46.2	5	7	40.0
	в системі АПК	17	11	-35.3	11	11		7	5	-28.6
	в металургійній промисловості	4	3	-25.0	3	3		2	4	100.0
	сформовані на етнічній основі	6	12	2.0 р	12	4	-66.7	2	5	150.0
Тривалість дії ОГ і ЗО	до одного року	356	307	-13.8	307	282	-8.1	186	178	-4.3
	до двох років	75	70	-6.7	70	59	-15.7	37	50	35.1
	від 3-х до 6-ти років	32	41	28.1	41	35	-14.6	19	16	-15.8
	більше 6-ти років	3	2	-33.3	2	2		2	2	
Виявлено осіб, вчинивших злочини у складі ОГ і ЗО		1754	1628	-7.2	1628	1457	-10.5	934	976	4.5
Учинено злочинів організованими групами і злочинними організаціями		3977	4682	17.7	4682	3670	-21.6	2493	2395	-3.9
З них	загальнокримінальної спрямованості	2774	3104	11.9	3104	2476	-20.2	1575	1624	3.1
	економічної спрямованості	1203	1578	31.2	1578	1194	-24.3	918	771	-16.0
	тяжких та особливо тяжких	3037	3649	20.2	3649	2928	-19.8	2058	1983	-3.6

ДОДАТКИ

Додаток А

Статистичні дані МВС України

Динаміка та структура загальнокримінальної злочинності

Характеристика злочинів загальнокримінальної спрямованості, скоєних групою осіб

2005	**2006**	**Динаміка, %**
44606	30133	-32.4
14.7	11.3	питома вага, %
2006	**2007**	**Динаміка, %**
30133	27922	-7.3
11.3	10.3	питома вага, %
2007	**2008**	**Динаміка, %**
27922	24390	-12.6
10.3	9.2	питома вага, %
Торік	**Поточн. рік**	**Динаміка, %**
14234	13143	-7.7
10.3	9.7	питома вага, %

Злочинність у сфері високих інформаційних технологій

2005	**2006**	**Динаміка, %**
615	583	-5.2
2006	**2007**	**Динаміка, %**
583	656	12.5
2007	**2008**	**Динаміка, %**
656	691	5.3
Торік	**Пот. рік**	**Динаміка, %**
503	574	14.1

ного року строк зберігання відомостей про активність в Інтернет, звільнив поліцію від обов'язків одержувати попередній дозвіл на оперативні заходи у багатьох випадках щодо доступу до приватних комунікацій; безуспішно намагались внести зміни до законодавства, що дозволять місцевим представницьким і виконавчим органам мати доступ до відомостей про користування телекомунікаціями;

Індія - антитерористичне законодавство дозволяє державним органам здійснювати моніторинг усіх видів комунікацій, у тому числі електронних, без попередньої згоди чи офіційного дозволу, інформація знята з каналів зв'язку може використовуватися як доказ у суді проти осіб;

Італія - прийняте законодавство спростило порядок ініціювання стеження за підозрюваними особами, збільшило коло правоохоронних органів уповноважених здійснювати перехоплення комунікацій, у тому числі без попереднього судового дозволу [108].

Заходи, до яких удаються країни зі сталими демократичними традиціями, стимулюють репресивний режим у країнах, які вважаються традиційними ворогами свободи в Інтернет.

Так, наприклад, у Китаї влада зобов'язала провайдерів послуг Інтернет і веб-портали підписати угоду про само-цензуру. Аналогічні приклади можна навести щодо В'єтнаму, Саудівської Аравії, Тунісу...

Для уникнення несанкціонованого розголошення персональних даних осіб, при зміні його зовнішності й місця проживання, а також з метою зменшення ризику при застосуванні інших мір безпеки необхідно виключити сам факт присутності таких осіб у будинках і приміщеннях правоохоронних й судових органах [109, с.291]. Фізична відсутність осіб, що захищаються, не виключить можливості проведення з ними процесуальних дій без яких-небудь обмежень за умови розробки «організаційного, тактичного й технічного забезпечення незалежного й дистанційного (віддаленого) спілкування будь-якого учасника кримінального судочинства один з одним [110 , с.252]. У цьому випадку акцентуємо увагу на проблемних ситуаціях, пов'язаних з ефективним забезпеченням безпеки й взаємодії територіально розрізнених учасників кримінального судочинства, можна уникнути, запропонувавши використання в кримінально-процесуальній діяльності сучасних засобів телекомунікацій. З урахуванням сучасного рівня розвитку інформаційно-телекомунікаційних технологій і їхнім постійним удосконалюванням пропонується здійснювати процес відеоконференренцзв'язку не тільки в традиційному розумінні «телемостів», а з використанням цифрової платформи мережі Інтернет.

Ще одне питання, яке стосується захисту прав користувачів електро-

нних комунікацій, не можливо обійти стороною, оскільки це має безпосереднє відношення до захисту прав і свобод українських користувачів Інтернет. Громадськими організаціями усього світу критично була сприйнята й Європейська Конвенція про кіберзлочинність (ETS no. 185), яку було відкрито для підписання 8 листопада 2001 р. Конвенція була підписана у Будапешті 30 країнами, серед яких США, Канада, Японія, Південно-Африканська Республіка, а також 26 із 43 держав-членів Ради Європи, у тому числі Україна

Поспішність, з якою готували текст і підписували зазначену Конвенцію під впливом трагедії 11 вересня, негативно вплинула на якість кінцевої версії документа. Статті 16-21 Конвенції, в яких визначаються процедурні питання здійснення оперативних заходів щодо телекомунікацій, потребують суттєвого доопрацювання.

Положення зазначених статей ставлять під загрозу права і свободи користувачів електронних комунікацій, оскільки надають майже необмежені повноваження правоохоронним органам щодо збирання й використання персоніфікованої інформації, а гарантій додержання законності й відновлення обмежених чи порушених прав не містять. Принципи гарантування законності і захисту права на приватність, мають бути втілені у реальні норми, якими регламентуються повноваження правоохоронних органів і процедури щодо зняття інформації з каналів зв'язку і комп'ютерних систем, а не проголошуватись в окремій статті, як це зроблено у ст. 15 Конвенції Ради Європи про кіберзлочинність.

Дискусійними залишаються питання використання впливу, який може бути за формою зовнішнього вираження фізичним і психічним. Правомірність фізичного впливу, спрямованого на об'єкти неживої природи, визначити порівняно нескладно. Слідчий вправі впливати на ці об'єкти в межах і випадках, зумовлених необхідністю, що виникла в справі й приписаннями закону. Тому примус внутрішньо властивий слідчій діяльності, відображає її характер і проявляється у процесуальних і тактичних заходах щодо подолання протидії [111, с. 32–33].

Особисті й майнові права й інтереси громадян можуть бути обмежені при цьому в строгій відповідності із установленнями закону, заподіювана майнова шкода повністю обґрунтована. Настільки ж зрозумілим є питання про фізичний примус, який у процесі судочинства є припустимим лише при прямому приписанні закону й стосуються лише примусових заходів: затримання, взяття під варту, приводу, примусового огляду й одержання зразків для порівняльного дослідження.

З урахуванням принципової можливості та необхідності примусового

час судового розгляду.

Тенденції динамічного розвитку інформаційних технологій зумовлюють впроваджувати в практику діяльності ОВС сучасні здобутки науки і техніки, лише завдяки цьому можливий ефективний попереджувальний вплив на всі криміногенні фактори, що детермінують злочинність. Протидія злочинності з використанням сучасних інформаційних технологій, засобів масової інформації і масової комунікації, спроможна підняти на якісно новий рівень систему правосуддя взагалі.

яльності організованих злочинних угруповань необхідно передбачати заходи щодо ведення інформаційної боротьби з ними. Рекомендується використання інформаційних технологій, пов'язаних з методами правомірного психологічного впливу на підозрюваного, обвинуваченого та інших осіб, основною метою яких є вплив на слідчу ситуацію в цілому або на її компоненти.

Автор враховуючи міжнародний досвід протидії злочинності пропонує проведення тактичних операцій з використанням Інтернет-пасток при проведенні тактичних операцій по виявленню та затриманню осіб, які підозрюються у вчиненні злочинів, які вчиняються ОЗУ.

Зміст й перспективи розвитку застосування інформаційних технологій і комп'ютерної техніки доцільно розглядати як один з істотних напрямків методології розділу криміналістики - криміналістичної техніки.

З метою виявлення потрібної інформації шляхом моніторингу повідомлень ЗМІ наголошується на необхідності створення загальнодержавних спеціальних інформаційно-аналітичних підрозділів.

Наголошується на доцільності легалізації матеріалів оперативно-розшукової діяльності за допомогою засобів масової інформації, для чого залучати журналістів до співпраці з оперативними підрозділами.

Пропонується прийняття як базового закону «Про захист персональних даних», що захищатиме право громадян на приватність персональних даних, так і спеціальних законів з обробки персональних даних у діяльності правоохоронних органів України. Крім цього автор дійшов висновку, що є нагальна необхідність при розробці КПК України перебачити розділ „Порядок тимчасового обмеження окремих конституційних прав і свобод людини і громадянина під час здійснення оперативно-розшукової діяльності, дізнання і досудового слідства".

Пропонується внести зміни до Закону України "Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації", і закріпити обов'язок журналістів погоджувати зі слідчим текст майбутньої публікації в ЗМІ, що ґрунтується на матеріалах кримінальної справи, й отримання від нього письмового дозволу на висвітлення певної інформації по обставинам розслідування злочину.

З метою гарантування безпеки осіб, які на конфіденційній основі надавали допомогу оперативно-розшуковим органам, в КПК України передбачити проведення слідчих дій з використанням дистанційного спілкування за допомогою телекомунікаційних технологій без присутності таких осіб на місці проведення зазначеної дії, як у ході досудового слідства, так і під

характеру заходів розслідування, у випадках вчинення протидії не може бути однозначного рішення чи заборони без конкретизації засобів, методів, прийомів та умов їх застосування. З метою вирішення цих проблемних питань, наполягаємо на необхідності проведення комплексного аналізу фахівцями з різних галузей знань, тобто психології, психіатрії та інших, положень по визначенню критеріїв допустимості фізичного, психічного та психологічного впливу.

За сучасних умов більш складно й неоднозначно вирішується питання про психічний вплив.

Розрізняють два види психічного впливу: неправомірний й правомірний. Неправомірний психічний (як і фізичний) вплив - насильство над особистістю - прямо заборонено законом у всіх формах. Припустиме тільки правомірний психічний вплив, але від того, що розуміти під таким впливом, залежить і визначення засобів впливу, визнання законними і припустимими або, навпаки, незаконними і аморальними тих або інших прийомів і засобів впливу. Загальне визначення впливу на людину сформулював Н.П. Хайдуков: "Вплив на людину є процес передачі інформації від суб'єкта впливу за допомогою різних методів і засобів, відображення цієї інформації в психіці даної особи, здатної викликати відповідну реакцію, що проявляється в його поведінці, діяльності, відносинах і станах, стаючи доступною для сприйняття особою, що впливає за допомогою "зворотного зв'язку" [112]. Основною ознакою правомірного психічного впливу вважається збереження у особи, що піддалася впливу волі вибору позиції. До цього додають і наявність умов для викладу своєї позиції, для її вибору і несуперечність законності й моральних принципів суспільства.

До цього можна додати, що психічний вплив здійснюється слідчим на всьому протязі провадження в справі, тому що всяке спілкування є вплив, а не тільки при допиті. Психологічний вплив є результатом застосування тактичного прийому, а не тактичним прийомом. Той самий прийом, та сама слідча дія в різних ситуаціях і до різних осіб можуть справляти вплив, а можуть залишитися до нього байдужими і не виявляти будь-якої відповідної реакції.

В етимологічному плані вплив може бути визначений як «дія, спрямована на кого-, що-небудь із метою добитися чогось, навіяти щось» [113, с. 79]. З позиції філософії вплив (взаємодія) – це найбільш універсальна форма зміни (перетворення) навколишньої дійсності, вид діяльності [114, с. 50, 51]. Більш чітко формулюється поняття впливу в психологічній літературі, що характеризується як цілеспрямоване перенесення руху й інформації одного учасника взаємодії до іншого [115, с. 58].

У криміналістичній літературі також початі спроби по визначенню поняття психологічного впливу і його ролі в судово-слідчій діяльності. Зокрема, В. Е. Коновалова вказує, що сутність психологічного впливу визначається «комплексом прийомів, спрямованих на діагностику психічного стану особистості свідка, обвинуваченого, підозрюваного й вибором найбільш ефективних прийомів виконання слідчої дії» [116, с. 102]. У криміналістиці й судовій психології питання про правомірність засобів впливу досліджено досить докладно, сформульовано ті умови (критерії) допустимості прийому, засоби впливу, які є необхідними для визнання його правомірним.

Відповідно до ст. 22 КПК України „Забороняється домагатись показань обвинуваченого та інших осіб, які беруть участь у справі, шляхом насильства, погроз та інших незаконних заходів".

Неоднозначність тлумачення положень ст. 22 КПК України породжує проблемні питання щодо практики її застосування, тому ми вважаємо за потрібне в контексті нашого дослідження змінити редакцію цієї статті: „Забороняється домагатись показань обвинуваченого та інших осіб, які беруть участь у справі, шляхом протиправних і недопустимих методів та інформаційних технологій, які можуть спричини шкоду життю, здоров'ю, майну, честі, гідності і ділової репутації, або позбавляють умов свободи вибору позиції чи лінії поведінки особи, а також дій пов'язаних з розголошенням інформації персонального характеру без згоди обвинуваченого і інших заходів, що порушують права і свободи громадян, які гарантовані чинними Законами України".

Висновки до розділу 1

Динаміка активного використання ОЗУ сучасних інформаційних технологій та ЗМІ як для вчинення злочинів, так і для протидії розслідуванню свідчить про недостатню готовність оперативно-розшукових та слідчих підрозділів в технічному і інформаційному відношенні адекватно вести боротьбу з цим видом злочинів. У зв'язку з цим практика розкриття і розслідування злочинів вчинених ОЗУ потребує інтенсифікації використання новітніх інформаційних технологій, програмно-технічних засобів, комунікаційних засобів прийому-передачі інформації, створення єдиної загальнодержавної інформаційно-обчислювальної мережі й інтегрованих банків даних на основі типізації й уніфікації при розкритті та розслідуванні злочинів, учинених ОЗУ.

Аналіз питань правового регулювання захисту прав людини під час

ВИСНОВКИ

Динаміка активного використання організованими злочинними угрупованнями сучасних інформаційних технологій та ЗМІ як для здійснення злочинів, так і для протидії розслідуванню свідчить про недостатню готовність оперативно-розшукових та слідчих підрозділів в технічному і інформаційному відношенні адекватно вести боротьбу з цим видом злочинів. У зв'язку з цим практика розкриття і розслідування злочинів, учинених ОЗУ потребує інтенсифікації використання новітніх інформаційних технологій, програмно-технічних засобів, комунікаційних засобів прийому-передачі інформації, створення єдиної загальнодержавної інформаційно-обчислювальної мережі й інтегрованих банків даних на основі типізації й уніфікації при розкритті та розслідуванні злочинів вчинених ОЗУ.

Оптимізація вдосконалення інформаційного забезпечення діяльності оперативних уповноважених, слідчих та слідчо-оперативних груп повинно вирішуватися за допомогою створення мобільних автоматизованих робочих місць. Останні містять у собі портативну ЕОМ із необхідним програмним забезпеченням і периферійним устаткуванням, а також засобу зв'язку й передачі даних.

Дієвими заходами розкриття та розслідування злочинів, учинених ОЗУ є типові тактичні операції з використанням ЗМІ під умовною назвою «свідок», «підозрюваний». На матеріалах публікацій ЗМІ, вивчання досвіду протидії організованій злочинності пропонується тактика проведення різновидів тактичних операцій: «полювання за жертвою», «імітація», «міраж», «витік інформації», «протидія».

Аналізуючи дискусійні питання щодо понять тактична комбінація та операція, автор вважає, що вони є самостійними категоріями криміналістики і пропонує авторське бачення цих понять: тактична комбінація - це визнана обставинами справи ефективна сукупність тактичних прийомів або слідчих дій, яка проводиться з метою зміни слідчої ситуації, поведінки чи позиції підозрюваних, обвинувачених та інших осіб і створюють сприятливі умови для вирішення конкретного завдання розслідування; тактична операція – це система процесуальних і непроцесуальних дій і заходів (слідчих і оперативно-розшукових, організаційних), тактичних комбінацій з використанням інформаційних технологій, яка зумовлена ситуаційною необхідністю взаємодії посадових осіб різних служб правоохоронних органів і спрямована на вирішення проміжного завдання розслідування.

При плануванні заходів щодо виявлення та розкриття протиправної ді-

вання поліграфа при опитуванні громадян».

3) Доповнити КПК України ст.. 85^3 «Застосування спеціального психофізіологічного обстеження з використанням поліграфа при провадженні досудового слідства», зміст, якої викласти в наступній редакції «Психофізіологічне обстеження з використанням поліграфа може використовуватись при проведенні обшуку, відтворення обстановки та обставин події, допиту та при проведенні інших слідчих дій. Особа, відносно, якої проводиться психофізіологічне обстеження з використанням поліграфа, повинна до початку цієї дії бути проінформована о сутності цього дослідження, і дати письмову згоду. Після цього таке тестування здійснюється поліграфологом (спеціалістом), а розшифрована ним поліграма повинна приєднуватися додатком до протоколу слідчої дії, який підписується всіма учасниками слідчої дії.»

4) Доповнити ст. 128^1 КПК України правом застосування спеціалістом (поліграфологом) спеціального психофізіологічного обстеження з використанням поліграфа.

Через появу нових технологій і тих, які ще будуть з'являтися, можуть бути вилучені докази, які представлені у вигляді сигналів в аналоговій цифровій формі або іншій формі, що не може бути представлена в доступному для сприйняття виді через відсутність спеціального програмного забезпечення, пропонується у КПК України закріпити положення про процедурою зберігання таких доказів і передбачити, що носії даних прилучаються до справи, які отримані із застосуванням інформаційних технологій, що містять інформацію, яку можна аутентифікувати або ідентифікувати.

обробки персональних даних в діяльності правоохоронних органів України виявив протиріччя, недоліки і прогалини у законодавстві. Для ліквідації існуючих недоліків і прогалин у законодавстві, пропонується прийняття як базового закону «Про захист персональних даних», що захищатиме право громадян на приватність персональних даних, так і спеціальних законів з обробки персональних даних у діяльності правоохоронних органів України. Крім цього автор дійшов висновку, що є нагальна необхідність при розробленні КПК України перебачити розділ „Порядок тимчасового обмеження окремих конституційних прав і свобод людини і громадянина під час здійснення оперативно-розшукової діяльності, дізнання і досудового слідства".

Принципи гарантування законності і захисту права на приватність, мають бути втілені у реальні норми, якими регламентуються повноваження правоохоронних органів і процедури щодо зняття інформації з каналів зв'язку і комп'ютерних систем, а не проголошуватись в окремій статті, як це зроблено у ст. 15 Конвенції Ради Європи про кіберзлочинність.

Характерними ознаками сучасних ОЗУ є: використання ними новітніх інформаційних технологій, а також ЗМІ, як для підготовки та здійснення злочинів, так і для протидії розслідуванню.

Впровадження систем моніторингу та перехоплення оперативними підрозділами персональних комунікацій в Інтернеті вимагає запровадження чітких і детальних правил здійснення оперативно-розшукових заходів в комп'ютерних мережах і підлягає такому ж самому контролю і законодавчому обмеженню, як і прослуховування телефонних розмов.

Неоднозначність тлумачення положень ст. 22 КПК України статті породжує проблемні питання щодо практики її застосування, тому ми вважаємо за потрібне змінити редакцію цієї статті: „Забороняється домагатись показань обвинуваченого та інших осіб, які беруть участь у справі, шляхом протиправних і недопустимих методів інформаційних технологій, які можуть спричини шкоду життю, здоров'ю, майну, честі, гідності і ділової репутації, або позбавляють умов свободи вибору позиції чи лінії поведінки особи, а також дій пов'язаних з розголошенням інформації персонального характеру без згоди обвинуваченого і інших заходів, що порушують права і свободи громадян, які гарантовані чинними Законами України".

РОЗДІЛ 2
ТЕХНОЛОГІЇ ТА НАПРЯМКИ ВИКОРИСТАННЯ ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ ПРИ РОЗКРИТТІ І РОЗСЛІДУВАННІ ЗЛОЧИНІВ, УЧИНЕНИХ ОРГАНІЗОВАНИМИ ЗЛОЧИННИМИ УГРУПОВАННЯМИ

2.1. Можливості використання засобів масової інформації при формуванні суспільної думки під час досудового слідства

Одним із важливих напрямків підвищення якості роботи правоохоронних органів країн ЄС розглядається орієнтація їх на суспільну думку. А враховуючи прагнення України бути членом ЄС, то й відповідно належні вимоги висуваються до діяльності правоохоронних органів нашої держави. Вирішення ними завдань зміцнення правопорядку та боротьби зі злочинністю повинно бути тісно пов'язане з формуванням належної суспільної думки в нашому суспільстві, що вимагає збільшення обсягу та інтенсивності їх взаємодії із різними соціальними групами та верствами населення, соціальними інститутами, серед яких важливе місце займають ЗМІ.

На думку багатьох відомих учених-юристів (В.Т. Томіна [117], Ю.В. Наумкіна [118], В.А. Удовиченка [119], Ю.М. Грошевого [120] та ін.), значна роль у забезпеченні відповідного рівня правопорядку належить силі суспільної думки, вона є одним із чинників, що в значній мірі впливає на діяльність правоохоронних органів, покликаних протидіяти злочинності, здійснювати як профілактику, так і розкриття та розслідування злочинів. Суспільна думка за своєю сутністю представляє собою "спосіб вияву суспільної свідомості; сукупність суджень та оцінок різних соціальних груп і верств населення з питань суспільного й державного життя. Формується в процесі спілкування людей як стихійно, так і під впливом політичних партій, громадських організацій, засобів масової інформації" [121]. Багато провідних учених переконані, що серед різних факторів, які впливають на формування суспільної думки, найбільша роль належить ЗМІ. Так відомий соціолог Е. Ноель-Нойман із ФРН, яка свого часу очолювала Всесвітню асоціацію по вивченню суспільної думки, відзначає, що в суспільстві існує два основних джерела, які породжують суспільну думку. Перший – це безпосереднє спостереження людьми за ситуацією, відчуття, чи схвалюються оточуючими ті чи інші дії, явища, заяви тощо. Другий – це ЗМІ і так званий "дух часу", який вони породжують [122, с. 222]. А Г.Г. Почепцов вважає, що на сьогодні ЗМІ стали найоптимальні-

родуються на вимогу суду

В умовах постійного зростання криміналістичних дактиломасивів їх обробка не гальмувалася через ручний метод перевірок, ефективним шляхом вирішення цієї проблеми є автоматизація нагромадження дактилоскопічної інформації та процес перевірок з використанням ЕОМ, на основі єдиної програми.

Пропонуються шляхи впровадження автоматизації обліку об'єктів, отриманих за допомогою сучасних методів голографії, що дозволить фіксувати об'ємне зображення об'єктів та їх відображень для покращення можливостей експертних досліджень.

На практиці при передачі «орієнтувань» в інші ОВС є загальний недолік - неповнота й недосконалість наявних у них відомостей, використання ж комп'ютерів, повне й грамотне кодування наявних даних дозволяють зафіксувати значно більшу кількість ознак і тим самим підвищити їх криміналістичну значимість.

Завдання вдосконалювання інформаційного забезпечення слідчо-оперативних груп при проведенні слідчих дій повинно вирішуватись за допомогою створення мобільного АРМ. Останнє необхідно обладнати портативною ЕОМ із відповідним програмним забезпеченням і периферійним устаткуванням, а також засобу зв'язку й передачі даних.

Своєрідність тактики й технічних засобів, застосовуваних для виявлення й вилучення інформації, що зберігається в оперативній пам'яті комп'ютера або на фізичних носіях, дозволяє виділити новий вид обшуку - обшук засобів комп'ютерної техніки.

Перспективним є використання безконтактного поліграфу для діагностики фізіологічного стану особи при проведенні слідчих дій.

Пропонується внесення наступних змін до чинного законодавства України стосовно нормативного закріплення проведення спеціального психофізіологічного обстеження з використанням поліграфа при провадженні досудового слідства, а також участі спеціаліста-поліграфолога у слідчих діях:

1) Доповнити статтю 8, що називається "Права підрозділів, які здійснюють оперативно-розшукову діяльність" Закону України "Про оперативно-розшукову діяльність", нормою, яка б конкретно регулювала застосування технічних засобів взагалі і поліграфу –зокрема, при проведенні опитування громадян.

2) Видати наказ МВС України «Про забезпечення впровадження поліграфа в діяльність органів внутрішніх справ» та спільну інструкція МВС, СБУ та Генеральної прокуратури України «Про порядок застосу-

льності організованих злочинних угруповань необхідно передбачати заходи щодо ведення інформаційної боротьби з ними. Рекомендується використання інформаційних технологій, пов'язаних з методами правомірного психологічного впливу на підозрюваного або обвинуваченого, основною метою яких є вплив на слідчу ситуацію в цілому або на її компоненти.

Новітні технічні засоби, які використовують злочинці, повинні братися на озброєння правоохоронними органами, тобто необхідно прагнути до досягнення адекватної протидії в процесі розкриття й розслідування злочинів

Зміст і перспективи розвитку застосування інформаційних технологій і комп'ютерної техніки доцільно розглядати як один з істотних напрямків методології розділу криміналістики - криміналістичної техніки.

Із метою виявлення потрібної інформації шляхом моніторингу повідомлень ЗМІ наголошується на необхідності створення спеціальних інформаційно-аналітичних підрозділів, які б передавали її відповідним підрозділам для перевірки та реагування.

Питання про розкриття особистості негласного співробітника може бути поставлено з його згоди по тяжких злочинах і в тому випадку, коли мова йде про відомості, здатні вплинути на долю справи. Рішення його залежить від того, наскільки істотною є інформація негласного співробітника й чи є в справі прямі докази винності підсудного. Ці питання відповідно до Програми вдосконалення агентурно-оперативної роботи ОВС України на 2007-2010 роки, потребують вирішення.

Із метою гарантування безпеки осіб, які на конфіденційній основі надавали допомогу оперативно-розшуковим органам, передбачити за їх згодою проведення слідчих дій, але з використанням дистанційного спілкування за допомогою телекомунікаційних технологій без присутності таких осіб на місці проведення зазначеної дії, як у ході досудового слідства, так і під час судового розгляду.

Наголошується на доцільності залучати журналістів до співпраці з оперативними підрозділами і використовувати їх публікації для легалізації матеріалів оперативно-розшукової діяльності. Поширення інформації в засобах масової інформації здебільшого є надійним і ефективним способом легалізації результатів проведення оперативно-розшукових заходів, за легендою, наприклад журналістського розслідування. Причому ініціатор подібних інформаційних заходів, виражених у проведенні відповідної тактичної комбінації залишає первинне джерело інформації в безпеці. Відповідно до ст. 26 Закону України "Про друковані засоби масової інформації (пресу) в Україні" дозволяє журналісту збереження таємниці авторства та джерел інформації, за винятком випадків, коли ці таємниці обна-

шим способом впливу на суспільну думку, це технологічно найбільш вигідний спосіб [123, с. 415].

Якщо говорити про формування суспільної думки, то не можна оминути таке важливе поняття, як зміна суспільної думки [124; 125; 126; 127]. Деякі вітчизняні та іноземні вчені вважають це поняття чи не найважливішим у сучасній системі діяльності ЗМІ [128; 129, с.20-45; 130 с. 45-63; 131; 132; 133]. Адже, на думку вчених, ступінь зміни основних соціальних орієнтирів, установок та асоціацій у певному часовому еквіваленті характеризується ступенем ефективної діяльності ЗМІ.

Негаразди соціального життя, невідповідність задекларованого владою життя реаліям, свобода поглядів стали причиною того, що суспільна думка швидко змінюється. Переважна більшість науковців поняття формування (або зміну) суспільної думки пов'язує саме з поняттям ефективності засобів масової інформації. Принаймні визначається такий взаємозв'язок: ЗМІ, які впливають на суспільну думку, є більш ефективними, ніж ті, які такого впливу не мають [134, с. 69]. Причому відзначається, що зміни в суспільній думці є більш важливими, аніж ситуативні емоції аудиторії з приводу певних журналістських матеріалів [135]. Отже, відповідно до визначень вчених, ефективні ЗМІ – це ті ЗМІ, які у своєму впливі орієнтовані на формування, зміну, трансформацію суспільної думки.

Вчені наводять кілька систем впливу ЗМІ на формування суспільної думки, де кінцевим підсумком ефективної діяльності ЗМІ стає, наприклад, зміна владного режиму або політичного устрою [136; 137; 138]. Ці системи за визначенням збігаються з психологічними схемами, які пояснюють сутність зміни соціальних установок, коли кінцевою метою таких змін є перехід установки в поведінку . Відповідно теми нашого дослідження аналіз літератури та практики розкриття та розслідування злочинів свідчить про не використанні потенційні можливості ЗМІ у формуванні думки не тільки громадськості, а і суб'єктів кримінального процесу, направленої на встановлення істини по кримінальних справах.

Механізмами формування (зміни) суспільної думки, є використання навіювання, стереотипу, іміджу, повторів (аби уникнути критичного сприйняття аудиторією пропонованої ЗМІ інформації) і формування потрібного ставлення аудиторії до тієї чи іншої події, явища.

Ці механізми, за визначеннями науковців, спрямовані на свідомість індивіда, адже суспільна думка є продуктом свідомості. Психологи дають таке визначення свідомості [139; 140; 141]: свідомість – це відображення у психіці людини ідеальних образів дійсності, своєї діяльності, самої себе. Свідомість – це особливе утворення, яке сформувалося в ході суспільно-

історичного розвитку на основі праці як специфічного виду людської діяльності, специфічна форма цілеспрямованого психічного відображення [142, с. 97].

Визначення свідомості у контексті впливу ЗМІ має такий вигляд: свідомість аудиторії – це сукупність етнічних, соціальних, громадсько-політичних сталих, які сформувалися або актуалізувалися за допомогою цілеспрямованого впливу ЗМІ, орієнтованого на зміни, трансформацію суспільної думки. Якщо ж всі вищесказані поняття поставити в один ряд, то виходить приблизно така закономірність: вплив ЗМІ орієнтований на суспільну думку, яка є продуктом свідомості, з метою її закріплення, зміни, трансформації. Таким чином, основною метою впливу ЗМІ є вплив на свідомість аудиторії.

Деякі вчені механізми формування суспільної думки схильні називати маніпуляційними прийомами ЗМІ, маніпуляційними технологіями.

Маніпулювання в ЗМІ сьогодні є досить актуальним, адже зараз триває “доба інформаційних воєн”, які можна виграти за допомогою більш вдалої інформаційної кампанії, яка, використовуючи маніпуляційні прийоми, здатна ефективніше вплинути на свідомість аудиторії.

Стає очевидним, що ЗМІ впливають на свідомість за допомогою маніпуляційних прийомів, які впливають на підсвідомість. Інакше кажучи, виявляється, що ефективний вплив ЗМІ неможливий без застосування механізмів впливу на підсвідомість.

На жаль, ні вітчизняні, ні іноземні вчені майже не говорять про те, що маніпуляція в ЗМІ розрахована, по суті, на те, щоб впливати на підсвідомість аудиторії з метою переносу і закріплення нових підсвідомих утворень (асоціацій, стереотипів, установок) у свідомості, де і відбувається зміна суспільної думки [143]. Українські вчені, зокрема, констатують наявність такого впливу, однак без достатнього обґрунтування [144; 145].

У дослідженнях по психології вчені схиляються до того, що “підсвідомість” – це сукупність психічних процесів, операцій і станів, які безпосередньо впливають на формування свідомості [146; 147; 148]. Однак психологи виокремлюють не лише свідомість і підсвідомість. Виділяють ще й таке поняття, як “позасвідоме” (або “несвідоме”) [149; 150].

Як вже зазначалося, діяльність засобів масової інформації спрямована на те, щоб впливати на свідомість (формувати суспільну думку). Але впливати на свідомість можна трьома шляхами: або безпосередньо, прямо звертаючись до неї, або йдучи обхідним шляхом – через підсвідомість і, врешті, впливати на свідомість, коли у самого індивіда виникає така потреба (свідомо очікувана інформація).

конфліктність - властивість, що випливає з особливостей характеру [456].

Основна причина конфліктних ситуацій, що виникають у злочинній групі, - корисні мотиви. "Уже в самій діяльності злочинної групи закладений предмет злочинного зіткнення. Тому що одночасне задоволення своєкорисливих особистісних інтересів і потреб проблематично" [457].

Інформаційна й аналітична робота в даних злочинних групах дозволяє встановити "слабкі ланки" конфліктних ситуацій, що є одним з найбільш важливих умов боротьби з організованою злочинністю.

З метою виявлення каналів інформації, визначення механізму її руху при психологічному аналізі злочинної групи дуже важливо усвідомити спосіб передачі інформації між її членами [458].

Виявлення способів, каналів руху інформації в злочинному співтоваристві забезпечує успіх в оперативно-розшукових заходах, гарантує необхідний рівень перетворення інформації на докази [459, с. 59].

Крім того, можливо активний інформаційно-психологічний вплив на злочинне співтовариство, наприклад шляхом поширення компрометуючих матеріалів через ЗМІ, у комп’ютерних комунікаціях, тобто створення "тривожної ситуації" у розроблюваних злочинних структурах, що дозволяє фіксувати активність шляхом зняття інформації з різних каналів [460].

Ефективність слідчої діяльності безпосередньо пов’язане з метою теоретичного осмислення сутності й значення психологічного забезпечення процесу збору, оцінки й використання доказів, з метою встановлення істини при розкритті й розслідуванні злочинів.

Вищевикладене дозволяє констатувати, що зв’язки і відносини, які виникають в організованих злочинних групах, механізм руху інформації - основа психологічної характеристики об’єднань злочинців, знання яких дозволяє одержати оперативно-розшукову інформацію й більш ефективно вести боротьбу зі злочинністю.

Висновки до розділу 3

Однією з умов підвищення ефективності розкриття й розслідування злочинів є впровадження в практику діяльності правоохоронних органів сучасних інформаційних технологій, програмно-технічних засобів, комунікаційних засобів прийому - передачі інформації, створення загальнодержавної єдиної інформаційно-обчислювальної мережі й інтегрованих банків даних на основі типізації й уніфікації.

При плануванні заходів щодо виявлення та розкриття протиправної дія-

прямих доказів, розкриття особистості такого свідка припустимо в інтересах правосуддя й тільки з його згоди. При цьому необхідно вжити додаткових заходів по забезпеченню безпеки цієї особи. Ці питання відповідно до Програми вдосконалення агентурно-оперативної роботи ОВС України на 2007-2010 роки, потребують вирішення.

З метою гарантування безпеки осіб [455], які на конфіденційній основі надавали допомогу оперативно-розшуковим органам передбачити за їх згодою проведення слідчих дій, але на наш погляд тільки з використанням дистанційного спілкування за допомогою телекомунікаційних технологій, тобто без присутності таких осіб на місці проведення зазначеної дії, як у ході досудового слідства, так і під час судового розгляду.

Потенційні можливості криються й у психологічних аспектах виявлення інформації про організовані злочинні групи оперативно-розшуковими методами.

Кожна злочинна група, з погляду психології, поєднує людей прагненням до досягнення злочинної мети. Для слідчого важливим є знання того, що дозволяє розкрити суб'єктивні механізми, що складаються в рамках організованих злочинних формувань, що зумовлюють як групову, так і індивідуальну поведінку злочинців. Необхідний пошук і знання найбільш уразливих елементів і зв'язків структур організованих злочинних формувань, що дає можливість здійснення правоохоронними органами дійсно ефективної боротьби з ними.

Закономірністю формування й функціонування злочинної групи є постійна дія в ній двох протиборчих цінностей: одна з них спрямована на подальшу інтеграцію й зімкнення членів злочинної групи, а інша - на їх роз'єднання. Об'єктивно супутня стратегія поведінки членів організованої злочинної групи породжує різні відносини, у тому числі й конфліктні.

Конфлікти можна розділити на: внутріособистісні; міжособистісні; міжгрупові.

Найчастіше вони виникають між організатором і всією групою; організатором і опозицією (опозиціонером); старими й новими членами злочинної групи; членами, що вирішили припинити злочинну діяльність, і всією групою; членами злочинної групи, що виконують різні функціональні ролі при скоєні злочинів; членами групи, що прагнуть зайняти більш високе ієрархічне положення в структурі групи; групою в цілому й одним з її членів, що скомпрометували себе; окремими членами групи на ґрунті особистих неприязних взаємин; окремими членами на ґрунті недотримання деякими з них норм поведінки й правил, встановлених у групі; групою в цілому й однієї або декількома конфліктними особистостями, для яких

Перший шлях впливу на свідомість ефективний тоді, коли застосовується технологія повторів. Через застосування надмірних повторів одна й та ж інформація поступово перестає усвідомлюватися і починає впливати на підсвідомість. Це сприяє тому, аби відбулося асоціативне закріплення певної інформації у потрібному емоційному контексті. Далі таке закріплення починає діяти у зворотному напрямку, тобто знову на свідомість. Схема такого впливу має такий вигляд: інформація – свідомість – підсвідомість – свідомість.

Другий шлях впливу особливо ефективний тоді, коли треба подолати опір свідомості, яка може не сприймати певну інформацію. У такому випадку певне знання відкладається в підсвідомості і при потребі «висвічується» свідомістю, перетворюючись на усвідомлені судження, оцінки тощо. Схема впливу набуває такого вигляду: інформація – підсвідомість – свідомість.

І, нарешті, третій шлях, коли існує свідома потреба індивіда в певній інформації (наприклад, для підозрюваного такою інформацією можуть стати відомості про результати розслідування). Таке поняття, як свідомо очікувана інформація, на нашу думку, є відображенням свідомого прагнення людини до отримання певної інформації, яка є життєво необхідною для неї. За допомогою засобів маніпуляції можна майже з будь-якої інформації зробити свідомо очікувану. Але види маніпуляції спрямовані на те, щоб "приспати" критичне сприйняття індивідом непотрібної йому інформації. Зацікавлення – це вже похідна від певного впливу ЗМІ на підсвідомість аудиторії. Тобто у цьому випадку свідомість і підсвідомість виступають одним цілим: сформований у підсвідомості потяг стає усвідомленим і життєво необхідним. Схема такого впливу: інформація – свідомість і підсвідомість.

Таким чином, весь загал інформаційних повідомлень (включаючи рекламу), які передаються каналами ЗМК, за впливом на свідомість можна поділити на такі види: свідомо очікувана інформація (або життєво необхідна інформація), пряма інформація (за допомогою повторів може закріпитися у підсвідомості), а також підсвідома інформація (яка впливає на підсвідомість з метою змін у свідомості).

Загальними засадами впливу ЗМІ на підсвідомість є використання в журналістських творах стереотипів, іміджу, а також повторів [151, с. 131 – 148]. А інформацію, яка переходить із підсвідомої у свідому, можна поділити на такі види: сенсаційна інформація; свідомо очікувана інформація; інформація-аналогія; інформація-застереження; інформація-протиставлення.

Стереотип – це стандартизовані, спрощені інформативні поняття з емо-

ційною оцінкою (позитивною чи негативною) будь-якого явища оточуючої дійсності, які сприймаються індивідом на рівні підсвідомості поза процесом їх усвідомлення [152, с. 136]. Стереотипи – це реальний продукт людської психіки. Без них масове спілкування та взаєморозуміння неможливі. Саме ставлення надає стереотипу риси емоційної образності, яка відіграє чим не найголовнішу роль у сприйнятті індивідом інформації та виробленні до неї певних оціночних суджень. Апелюючи, перш за все, до емоційно-чуттєвої складової людської психіки, стереотип несе в собі й певне раціональне навантаження. А раціональний зміст стереотипу може бути як істинним, так і хибним. Все залежить від того, наскільки глибоко стереотип відображає реальний взаємозв'язок між явищами, наскільки ілюстровані в стереотипі риси людей та події є типовими. Якщо ці зв'язки та риси несуттєві чи поверхові, то стереотип далекий від життя, він є хибним. Такі стереотипи легше складаються та засвоюються, оскільки "схоплюють" лише найпримітніше – те, що спричиняє зовнішній ефект та сильніше за все "б'є" по емоціях, викликаючи бурхливу реакцію свідомості [153; 154].

І навпаки: якщо зв'язки та риси, відображені у стереотипі, є суттєвими та основними в характеристиці явищ, то такий стереотип є істинним. Такий стереотип складається повільніше і формується за участю апарата логічного мислення [155, с. 138].

Використання хибних стереотипів викликано бажанням більш швидкого і ситуативного закріплення у суб'єкта чи в аудиторії певного ставлення до тієї чи іншої резонансної події, її учасників, з метою упезпечення учасників резонансу від створення істинного стереотипу, який може негативно позначитися на репутації певної особи, або ж, навпаки, - для того, щоб пришвидшити перенесення і закріплення негативних асоціацій на саму подію чи на її учасника. Стереотипом може стати поняття, позбавлене зовнішньої емоційної образності, але яке має в собі певне (позитивне чи негативне) соціальне забарвлення. Такі поняття стають стереотипами лише через їх щоденне вживання.

Імідж – це також образ дійсності, що сприймається, але, на відміну від стереотипу, він відображає її неповторні, одиничні риси. Імідж відрізняється від художнього образу не лише безпосереднім зв'язком із реальністю, з її конкретними проявами, але й відсутністю цілісності, що властива художньому образу.

Імідж на відміну від художнього образу ілюструє не всю сукупність рис, що складають єдину картину. В ньому відображено лише окремі характеристики об'єкта. Більше того, імідж абстрагується від решти, висвітлюючи лише ці аспекти суб'єкта, акцентуючи увагу лише на них.

усіх доступних джерел, зокрема СКБД Oracle, Microsoft Access і SQL Server, текстових файлів;

- Analyst's Workstation – продукт, який інтегрує всі технології від i2 Group, включаючи оброблення даних за допомогою системи візуальних запитів за принципом «намалюй запитання – отримай картинку-відповідь» і засоби інтеграції із зовнішніми додатками, наприклад із ГІС. [454, с.5].

Інформаційно-технічна складова розкриття й розслідування більшості злочинів є на нинішньому етапі, на наш погляд, найбільш пріоритетним й дозволить скоротити часові витрати співробітників оперативних і слідчих підрозділів і строки розслідування кримінальних справ, а також підвищити якість розслідування.

Одним із методів, що мають реальну перспективу бути використаними в процесі доказування, є одержання відомостей від негласних співробітників. У більшості правових держав Заходу допустимість відомостей негласних співробітників як доказ визнаний законом як об'єктивна необхідність. При цьому, однак, необхідне дотримання цілого ряду вимог, що забезпечують як надійність одержуваних від цієї особи відомостей, так і його власної безпеки. Законодавчо закріплено вимогу про те, що така особа для одержання оперативних даних може використовувати тільки законні засоби; особа не звільняється від кримінального переслідування за скоєний їм злочин у ході таємної операції, якщо тільки воно не було викликано гострою потребою або в стані необхідної оборони.

Про гарантії безпеки розглянутої категорії осіб згадується в ст. ст. 8, 12, 13 Закону України "Про оперативно-розшукову діяльність". Найважливіша з них стосується в забезпеченні повної конфіденційності такого співробітництва громадян із правоохоронними органами. Проблема полягає в тому, щоб використовувати ці дані, не розшифровуючи негласний спосіб їх одержання. Відомості про їх особистість є державною таємницею й можуть бути віддані гласності тільки у випадках, спеціально передбачених законом.

На жаль, Закон України "Про оперативно-розшукову діяльність" не містить переліку таких випадків. На наш погляд, питання про розкриття особистості негласного співробітника може бути поставлений у тому випадку, коли мова йде про відомості, здатних вплинути на долю справи і тільки по тяжким злочинам. Рішення його залежить від того, наскільки істотною є інформація негласного співробітника й чи є в справі прямі докази винності підсудного. Якщо ця особа є найважливішим свідком по питанню винності або невинності підсудного і якщо в справі немає інших

Групові СППР (комунікаційні СППР) — це інтерактивні автоматизовані системи, призначені для підтримки розв'язування неструктурованих і напівструктурованих проблем кількома особами, що приймають рішення, що працюють як група. Групові СППР є гібридними системами – вони підтримують електронні, візуальні та звукові комунікації, складання розкладів, спільне використання даних і моделей, колективне генерування альтернатив, консолідацію ідей та інтерпретацію результатів. Крім цього, групові СППР мають можливості, які вже були розглянуті стосовно інших класів СППР.

Нині більшість використовуваних СППР є внутрішньоорганізаційними – їх розроблено для індивідуального або групового використання в межах окремої організації. На відміну від них інтерорганізаційні СППР, що належать до порівняно нової категорії систем, можуть мати серед своїх користувачів і зовнішніх осіб. Створити такі системи вдалося насамперед завдяки розширенню доступу до мережі Інтернет, яка забезпечує комунікаційні зв'язки різних типів, зокрема й необхідні для СППР. На базі Web-технологій створюються та використовуються системи, які дістали назву Web-зорієнтованих.

Очевидно, що в юридичній діяльності доводиться застосовувати численні як загально- так і функціонально зорієнтовані системи. Наприклад, аналітичні продукти англійської компанії i2 Group, що їх сьогодні Інтерпол та Європол прийняли як стандарт, використовують 1300 державних і комерційних організацій у 90 країнах світу. Технології i2 добре зарекомендували себе, коли йдеться про введення оперативно-слідчої інформації, аналіз даних, візуалізацію результатів і планування заходів, спрямованих на боротьбу з організованою злочинністю, незаконним обігом наркотиків та економічними злочинами. Системи забезпечують перевірку висунутих слідчих версій, аналіз результатів слідчих дій, виявлення прихованих зв'язків, формування напрямків дій слідчого, візуалізацію фактів, які свідчать про винність або невинність конкретної особи, контроль за розслідуванням кримінальних справ. Серед продуктів, що їх пропонує компанія, можна назвати такі:

- Analyst's Notebook – програма для відображення взаємозв'язків між особами, подіями, банківськими рахунками, номерами телефонів, автомашин та іншими об'єктами, виявлення динаміки послідовності подій, діаграми дій у кожній події;

- IBase – програмне забезпечення для збирання, структуризації та зберігання даних із різних джерел;

- IBridge – інструментарій для вилучення та об'єднання інформації з

Особливістю іміджу і одночасно однією з його переваг є те, що він може брати участь не лише у навіюванні, але й в усвідомленому впливі. Якщо імідж підкріплено серйозним логічним обґрунтуванням, якщо він спирається на міцний фундамент доказових фактів, то він виконує функцію не стільки навіювання, скільки більш чіткого усвідомлення описаного явища.

Необхідність повторів обумовлена перш за все схильністю людини до навіювання через повтори, масовістю аудиторії, на яку впливає журналістика. Донести до думки читачів, слухачів, глядачів окремий факт, не повторюючи повідомлення, просто неможливо. Як частина роз'яснювальної та обгрунтовуючої інтерпретації повтори характеризуються тенденцією диверсифікації, тобто потягом до різноманітності. Існує два способи диверсифікації повторів: синонімічність та смислова варіативність. Повтори синонімічного виду є викладом одного і того ж факту або судження про нього іншими словами. Даний прийом дає змогу уникнути тавтології і одночасно використовувати всі переконуючі якості повторів: привернення уваги до повідомлюваної думки, полегшення сприйняття та засвоєння знань, закріплення інформації в пам'яті.

Смислова варіативність – це повтори тієї чи іншої тези в різних змістових аспектах, розгляд одного й того ж питання в різних площинах. Журналіст не просто повторює свою думку, – він повертається до неї, аналізуючи її в іншій площині, під іншим кутом зору. Перевага смислових варіантів для роз'яснення і обгрунтовуючої інтерпретації полягає в тому, що в них, як правило, до мінімуму зведено зовнішні ознаки повторів. В аудиторії не виникає психологічного дискомфорту, який зазвичай викликає "розжовування" одного й того ж положення [156; 157].

Одночасно смислові варіанти дають можливість глибше вивчити явище, досліджуючи його окремими частинами, і допомагають аудиторії легше засвоїти інформацію.

Після того як аудиторія отримала необхідні дані, усвідомила і засвоїла їх, свідомість "блокується", відмежовуючись від подальшого сприйняття, вивчення, дослідження даного інтерпретованого знання. Людський розум перемикається на сприйняття іншої інформації. В цьому випадку спрацьовує природний захисний механізм, який убезпечує мозок від надмірного перевантаження. Якщо ж повтори засвоєної інформації продовжуються, то відбувається вплив вже не на свідому, а на підсвідому складову людської психіки, тобто повтори перетворюються в інструмент навіювання.

Якщо для повторів на рівні роз'яснення та обґрунтування властива диверсифікація (синонімічне багатство, смислова варіативність), то для повторів на рівні навіювання властива ідентичність, стереотипність. Збері-

гаючи свою однотипність, повтори здатні впливати на людину поза її свідомістю.

Стереотипні ідентичні повтори як засіб навіювання необхідні у випадку різко негативного, критичного ставлення до повідомлюваної інформації. В таких ситуаціях свідомість відштовхує інформацію, відключаючись від її сприйняття. Малоефективними в цьому випадку стають диверсифіковані повтори із залученням найрізноманітнішої аргументації. І тут на допомогу приходить навіювання зі своїми стереотипними повторами. Поступово, ці повтори будуть проникати у підсвідомість, відкладаючись і закріплюючись там з тим, щоб у майбутньому, за допомогою нового досвіду і знання, перетворитися в переконання. Для переконання на рівні навіювання властива не лише стереотипність, а й максимальна спрощеність. Лаконічні, прості фрази легше засвоюються без зусиль раціонального усвідомлення.

До свідомо очікуваної інформації відносимо інформацію, необхідну для різноманітних життєвих потреб. Це і прогноз погоди, політичні, економічні, спортивні новини тощо. Свідомо очікувана інформація впливає на повсякденне життя, формує настрій, задовольняє запити людей в різних сферах діяльності. Так, наприклад, від прогнозу погоди залежить, що сьогодні одягне людина, а також що вона запланує зробити. Музичні новини формують смаки аудиторії, політичні – громадянську позицію, економічні – господарські заходи. Інформація по кримінальній справі впливає на поведінку суб'єктів, які заінтересовані в результатах розслідування. Тому свідомо очікувана інформація, окрім підсвідомості суб'єкта чи аудиторії, впливає також на свідомість, тобто відбувається швидкий перехід цієї інформації із підсвідомої у свідому, від якої значною мірою залежить поведінка суб'єкта чи групи людей.

Інформація-аналогія також має здатність швидкого переходу із підсвідомої інформації у свідому. Але, на відміну від попереднього виду, така інформація не становить нагальної життєвої необхідності.

Основна мета інформації-аналогії – дати змогу аудиторії провести паралель між журналістськими фактами та реальністю. Темою таких матеріалів може бути життя в інших країнах, опис історичних подій, біографії видатних особистостей, поведінка підозрюваних по аналогічним кримінальним справам тощо. Ці матеріали сприймаються не тільки на підсвідомому рівні, а й свідомо. Інформація-аналогія здатна змусити суб'єкта чи аудиторію осмислено порівняти своє життя з досвідом інших людей.

Загалом такі матеріали збагачують журналістську палітру і активно формують особисту або громадську думку.

До інформації-застереження належать, в основному, матеріали з пи-

складу програмного забезпечення сучасних автоматизованих робочих місць оперативного працівника та (або) слідчого.

Це буде істотним просуванням у реалізації принципу єдиного інформаційного верховенства, яка сформована кожним учасником єдиної системи, інформація акумулюється й обробляється в головному інформаційному центрі на основі єдиних технологічних принципів і підходів, з використанням одного набору програмних і апаратних засобів і поширюється всім зареєстрованим користувачам системи. Створені колись аналогічні системи не передбачали централізованого адміністрування, забезпечуючи лише створення засобів керування між розподіленими сховищами інформації, контроль над якими кожне відомство здійснювало незалежно. Велику категорію становлять системами підтримки прийняття рішень називають інтелектуальні системи, за допомогою яких особи, що приймають рішення (СППР), мають змогу аналізувати ситуації, формулювати задачі, виробляти, контролювати й оцінювати варіанти рішень, які забезпечують досягнення поставленої мети., зорієнтовані на доступ та маніпуляцію моделями – статистичними, фінансовими, оптимізаційними та (або) імітаційними. Приклади таких СППР: засоби аналізу рішень, які допомагають розбити проблему на складові й структурувати її; засоби лінійного програмування – засоби використання відповідних математичних моделей для пошуку оптимального розв'язку задач розподілу ресурсів і т. ін.; мітаційні засоби – засоби проведення певної кількості експериментів для перевірки результатів, що випливають з кількісної моделі системи.

Деякі системи, що дають змогу виконувати складний аналіз даних, можуть бути класифіковані як гібридні СППР, що забезпечують і моделювання, і пошук та підсумковий аналіз даних. Гібридним підходом до СППР вважаються також технології здобування даних (Data Mining). Синонімами терміна «здобування даних» є «виявлення знань у базах даних» та «інтелектуальний аналіз даних». Мета здобування даних полягає у виявленні прихованих правил і закономірностей у наборах даних.

Засоби здобування даних та експертні системи становлять ще одну категорію СППР — рекомендаційні СППР (Suggestion DSS). Експертні системи (ЕС) як системи штучного інтелекту часто розглядають як окремий клас ІС, але останнім часом спостерігається тенденція реалізації їхніх модулів у складі СППР і виконавчих ІС.

СППР, зорієнтовані на документи розробляються для управління неструктурованими документами і Web-сторінками, такі СППР інтегрують різноманітні технології зберігання та оброблення гіпертекстових документів, зображень, звуків, відео тощо.

осіб чути, бачити й спілкуватися один з одним, перебуваючи при цьому на різних континентах.

Це спілкування, що створює ефект присутності в одній аудиторії, супроводжується передачею всілякої текстової й графічної інформації, що може бути моментально оброблена за допомогою комп'ютера й поміщена у відповідну базу даних. Подібні нововведення вже відомі практиці кримінального судочинства при випадках проведення судових засідань без безпосередньої присутності учасників кримінального судочинства, а також для виконання окремих слідчих дій (допит і огляд і ін.).

Говорячи про сучасні інформаційні технології, необхідно докладніше зупинитися на одній із найбільш популярних технологій 90-х рр. XX ст. - мультімедіа. Поки ще немає чіткого формулювання, що розкриває зміст цього поняття. У літературі зустрічаються всілякі визначення, часто суперечливі. На наш погляд, найбільш вдалим визначенням можна вважати наступне: мультімедіа - це діалогове програмне забезпечення, під керуванням якого на екрані комп'ютера досягається взаємодія візуальних і аудіоефектів. Технологія мультімедіа знаходить все більше застосування в моделюванні різних процесів. Комп'ютери, оснащені відповідними програмами, дозволяють відтворити різні ситуації, що виникають у реальному житті. За допомогою ЕОМ можливе проведення окремих епізодів таких слідчих дій, як відтворення обстановки й обставин події злочину й ін. На це лише буде потрібно час і правове закріплення подібних дій. Умовно все різноманіття комп'ютерних програмних комплексів і систем, застосовуваних у правоохоронних органах, можна розділити на шість типів: інформаційно-довідкові системи; автоматизовані робочі місця й системи керування; експертно-консультуючі системи; розрахунково-аналітичні системи; комп'ютерні навчальні системи; комп'ютерні системи обробки зображень.

З погляду ефективного розкриття й розслідування злочинів значно зручніше мати справу з єдиним інформаційним простором, а не з гетерогенними, територіально роз'єднаними СКБД (системами керування базами даних), тому що це дозволяє зібрати всі необхідні для аналізу дані в центральній базі даних, очистити їх від помилок, привести до єдиних форматів і представити в зручному для користувача виді. Немаловажним представляється й зниження вартості пристроїв зберігання інформації. Це дозволило користувачам зберігати первинні дані із трансакційних систем з високим ступенем деталізації й за тривалі інтервали часу. Необхідно оснащувати типовими програмними засобами для створення й ведення баз даних в органах внутрішніх справ, поряд із традиційними, вхідних до

тань правознавства та правоохоронної тематики. Мета цих повідомлень – застерегти аудиторію від можливої небезпеки. Повчальність – одна з основних характеристик матеріалу. Дієвість таких текстів, як і власне сенсаційних, дуже висока, бо аудиторія усвідомлює всі аспекти повідомлень з негативним "навантаженням".

Психологами доведено, що негативна інформація здатна викликати більшу зацікавленість аудиторії, ніж позитивна, і ця особливість "кримінальної" тематики також підвищує її ефективність.

Конкретність висновків – характерна властивість інформації-застереження. У багатьох інших випадках журналістські висновки не дають очікуваного результату, бо аудиторія схильна трактувати їх як нав'язування певної думки. Але в інформації-застереження люди очікують висновків, щоб краще усвідомити зміст матеріалу.

Інформація-протиставлення покликана об'єктивно подавати події, представляючи різні погляди на розсуд особи або аудиторії, які самі мають обрати позицію відповідно до своїх переконань. Інакше кажучи, одна з протилежних позицій відповідає установкам індивіда, і в матеріалах-протиставленнях ця підтримувана позиція або ще більше зміцнюється, або змінюється на користь іншої сторони. Суб'єкт або аудиторія охоче сприймають інформацію-протиставлення, бо журналіст нічого не нав'язує, а лише намагається об'єктивно викласти існуючі розбіжності. Але в такому випадку можливо бажану лінію поведінки розкрити більш привабливо, ненав'язливо її прорекламувати і це дасть можливість навіяти необхідну позицію для вчинків.

Отже, інформація, яка здатна із підсвідомої переходити у свідому, характеризується наявністю потреб аудиторії у такій інформації, усвідомленням її життєвої необхідності. Така інформація відзначається високою ефективністю, оскільки майже у всіх випадках роль журналіста полягає в його основній функції – інформувати суспільство, а не робити замість аудиторії конкретні висновки. Потреба аудиторії усвідомити інформацію, з одного боку, спрощує, а з другого, – ускладнює завдання журналіста [158, с.10 - 45].

Г. Почепцов – відомий дослідник впливу ЗМІ на аудиторію, трактує інформаційну війну як комунікативну технологію за силою впливу на масову свідомість, включаючи підсвідомість з короткочасними та довгостроковими цілями [159, с. 45].

Скидання компрометуючої інформації сьогодні є звичайною справою, в комп'ютерних, телекомунікаційних мережах, радіоефірі, Інтернеті, відбуваються справжні інформаційні війни. „Інформаційна зброя", повною мірою повинна бути використана при виконанні завдань ОРД не тільки

стратегічного характеру (маючи на увазі велику аудиторію ЗМІ), але й тактичного (локального). Тобто це може відбуватися щодо окремих ОЗУ, злочинних організацій, в рамках відповідної справи оперативної розробки. Безумовно організація, проведення, забезпечення „інформаційної акції" потребує здійснення ряду різного роду заходів залучення відповідних сил, їх взаємодії за єдиним задумом та планом, узгодженості за місцем та часом єдиного управління, тобто проведення операції (інформаційно-психологічної) [160, с. 135-136] .

На цей час з'явився новий тип цензури: цензура інформаційного шуму. Сутність такої цензури полягає у реагуванні на небажані інформаційні повідомлення створенням нових, часто штучних інформаційних повідомлень, які мають поховати під собою небажану інформацію. Відслідковувати джерела таких повідомлень, що швидко розповсюджуються через перехресні посилання інформаційних сторінок та агентств дуже важко, а притягнути до відповідальності когось майже неможливо, бо всі посилаються одне на одного. Таким чином створюються величезні, значною мірою неправдиві масиви інформації, які не можуть бути адекватно опрацьовані та сприйняті суспільством. Можемо впевнено казати лише про загальний емоційний фон, який створюється інформаційними хвилями і впливає на настрої суспільства. Такі хвилі інформаційного шуму вже стали звичними для громадян України, які живуть в умовах постійної політичної боротьби, і викликають лише негативну реакцію і небажання людей розбиратися у потоках інформації, що виливають на них ЗМІ та Інтернет. Люди вже давно звикли, що всі засоби масової інформації є насамперед інструментом маніпулювання їхньою думкою, і, згадуючи кому належить той чи інший ресурс, легко здогадуються чого від них хочуть на цей раз. В цих умовах генератор інформаційних хвиль ризикує отримати негативну реакцію цільової аудиторії.

Інформаційна війна між Росією та Грузією виявила нову зброю – Інтернет-спільноти, або соціальні мережі. Інтернет-спільнота – це неформальне відкрите або закрите об'єднання людей за певними інтересами, які спілкуються за допомогою Інтернет. Ці об'єднання, зазвичай, досить динамічні: є постійні учасники, є випадкові та періодичні відвідувачі. Територіально учасники можуть знаходитись у будь якій країні, їх об'єднує лише мова та спільні інтереси. До речі, деякі дослідники питань тероризму бачать у таких об'єднаннях модель динамічних терористичних організацій майбутнього. Одна з характерних рис таких спільнот – свобода, бо їх учасники можуть не знати справжніх імен одне одного, не бачити облич. До того ж учасники таких спільнот – це, як правило, найбільш освічена та соціально активна части-

і комерційних структур свідчить про активні розробки і використання технологій інтелектуального аналізу даних (ТІАД) і геоінформаційних систем (ГІС-технологій). Багато в чому це пов'язано з тим, що на застосуванні вищевказаних технологій обробки даних базуються перспективні концепції керування силами і засобами в складній оперативній обстановці. На основі їх активного використання приймаються складні політичні, економічні й інші рішення. Найбільше поширення в цей час одержали автоматизовані інформаційні системи. Вони не змінюють складу об'єктів оперативно-розшукових і профілактичних обліків і не створюють нових. Інформація в системі концентрується, обробляється, зберігається й видається користувачам відповідно до нормативних актів, що регламентують ведення оперативно-розшукових і профілактичних обліків ОВС.

Сфери застосування таких систем різноманітні. Серед них можна виокремити:

- розслідування фактів шахрайства – оперативне збирання та аналіз інформації з різних джерел (повідомлення, результати розслідування, банківська і фінансова інформація), установлення неявних зв'язків, часовий аналіз, що виявляє нестикування в подіях, виявлення нових слідів у справі і т. ін.;

- розвідувальний аналіз (комп'ютерна розвідка) — знімання інформації з радіоефіру й телефонних ліній, нагромадження даних оперативної роботи (фіксація подій, де з'являються підозрювані, аналіз їхніх зв'язків і т. ін.); аналіз послідовності малозначущих на перший погляд подій (наприклад регулярне перерахування невеликих сум різними особами на один рахунок) з метою виявлення прихованих закономірностей; а також планування цілей розвідки, формування і перевірка робочих гіпотез, організація збирання, тестування та інтерпретації даних із подальшим поданням результатів у вигляді діаграм, схем, таблиць, графіків;

- визначення потенційних об'єктів і суб'єктів кримінальної активності – профілактика злочинів, ідентифікація порушників закону, з'ясування цілей, часу та об'єктів можливого злочину, запобігання масовим злочинам і терористичним актам, прогнозування можливостей і напрямків промислового шпигунства, побудова картини обвинувачення і врахування всіх факторів;

- непроцесуальне використання даних – аналіз публікацій у відкритому друці, формування суспільної думки, підготовка контрактів для комерційних структур і т. ін.

Сполучення телефону й телебачення з можливостями техніки цифрової обробки й передачі інформації дозволило створити новий вид інформаційних послуг - телеконференції. Вони допомагають широкому колу

техніки. Ми також, поділяємо висловлену думку Романенко М.О.[451, с. 147-155] про необхідність введення до змісту криміналістичної техніки судової дигітології.

Роль інформаційних технологій у боротьбі зі злочинністю сама по собі різноманітна. В ОРД вони можуть успішно використовуватися для виявлення, документування, розкриття, попередження злочинів та припинення злочинної діяльності на ранніх стадіях їхньої підготовки й здійснення. Активно використовуватися як докази в кримінальному судочинстві матеріали, що отримані в ході проведення оперативно-технічних заходів, відносно осіб, які вчинили тяжкі та особливо тяжкі злочини.

У кримінальному процесі нові інформаційні технології ефективно можуть застосовуватися для ефективного проведення різних слідчих дій. Застосування названих технологій має значні перспективи також і в правоосвітній, правовиховній діяльності і профілактиці злочинів. Інформатизація у правоохоронних органах України має певну практику та історію [452].

Водночас аналіз теоретичної розробленості проблем протидії злочинності у сфері інформаційних технологій для їх викриття та документування свідчить, що потребують дослідження способи та прийоми отримання інформації при розкритті та розслідуванні злочинів у сфері нових інформаційних технологій.

Це потребує, у свою чергу, формування й розвитку нових напрямків інформаційно-технічного забезпечення оперативно-розшукової й слідчої діяльності. Організація практичної роботи в значній мірі визначатиметься тим, як нові напрямки інформаційно-технічного забезпечення протидії злочинності будуть співвідноситися зі сталими методами й прийомами діяльності органів внутрішніх справ [453, с. 313, 317]. Рішення покладених завдань на сучасному етапі розвитку науково-технічного прогресу неможливо без використання новітніх інформаційних технологій. Тому розроблення та впровадження інтелектуальних систем аналізу і обробки інформації в контррозвідувальну діяльність СБУ та ОВС є актуальними чинниками підвищення ефективності оперативно-службової діяльності.

Питанням інформаційно-аналітичного забезпечення оперативно-службової діяльності правоохоронних органів присвячені праці вітчизняних науковців: Азарова С.С., Вертузаєва М.С., Голубєва В.О., Калюжного Р.А., Костюченка М.І., Цимбалюка В.С., Хахановського В.Г., Хорошка В.О., Швеця М.Я. та багатьох інших. Проте досліджень щодо впровадження інтелектуальних інформаційних систем нового покоління в діяльність правоохоронних органів України – практично відсутні. Аналіз сучасних технологій обробки даних в інтересах державних, правоохоронних

на нації. Отже зазвичай такі спільноти знаходяться у пасивній протидії державі, в різній мірі засуджуючи її більш-менш неоднозначні кроки. Але війна з Грузією при всій своїй неоднозначності викликала майже одностайну підтримку Інтернет-спільнот російськомовного Інтернету. Інформаційна війна, що мала підготувати суспільну думку росіян до вторгнення в Грузію, була виграна РФ, а Інтернет-спільноти з аудиторії та об'єкту війни перетворились на інструмент ведення такої війни. Кожна інформація, правильно введена до цільової спільноти одразу тиражувалася і розповсюджувалася без перевірки. Організовувалися атаки хакерів-патріотів на сайти Грузії, флеш-моби з одночасного розміщення десятками росіян англомовної антигрузинської інформації на сайтах Євросоюзу та Сполучених Штатів. За рахунок перехресних посилань та перепублікацій будь-яка негативна інформація про дії Грузії у вигляді свідчень очевидців миттєво розліталася Інтернетом. Весь Інтернет облітали фотографії грузинського президента, де він перелякано ховається від обстрілу та жує краватку перед камерами. Інформаційна війна була виграна, але як би не державою, а свідомими громадянами, які об'єдналися у Інтернет-спільноти. Такі засоби використовуються і фінансовими колами для завдання шкоди конкурентам . Коли людина начебто випадково отримує інформацію з джерела, яке звикла вважати безпристрасним та вільним від політики та/або економіки, вона сприймає цю інформацію без упередження, яке мало б місце перед офіційними виданнями. Але не всі, хто бере участь у інформаційних війнах є «віртуалами». В цих Інтернет-спільнотах народився новий тип людини, що впливає на громадську думку: громадянин-кореспондент. Це людина, яка має власну думку, хоче і здатна ділитися нею та шукає свого місця в системі формування громадської думки [161].

У період інформаційних війн особливу роль відіграє "дестабілізуюча інформація". Вагомими дестабілізаторами можуть бути повідомлення про "некерованість ситуації" (катастрофи, землетруси, повені тощо). У результаті людина виводиться з раціонального стану і, діючи емоційно, залишається без багатьох соціальних обмежувачів. Своєю панікою вона заражає інших. Типи "панічних повідомлень" включають більш старші ланки мозку, які несуть у собі виключно тваринні реакції на ситуації (втікати, битися тощо) [162; 163; 164]. У таких випадках існує лише несвідоме; варіанти поведінки, які були б різними або ж мали нетваринну природу, залишаються викресленими. Слід також пам'ятати, що агресивність натовпу є природною психологічною реакцією на зняття напруги через наявність недосяжної мети.

На цей час найбільше маніпуляцій свідомістю українців відбувається навколо світової фінансової кризи і всі відчули вплив спекуляцій навколо

фінансової кризи. Криза в банківській сфері України та карколомні віражі валютного ринку спровоковані більше інформаційними впливами ніж реальним станом речей. Різні партії в боротьбі за владу критикують уряд, погрожують акціями протесту, змагаються ефектними антикризовими програмами, уряд списує власні проблеми на світову кризу, банки переглядають кредитні угоди, притримують депозити та спекулюють валютою прикриваючи все це світовою фінансовою кризою. На цей час вже значна кількість людей потрапила у скрутне матеріальне становище через високі кредитні ставки банків, через затримки заробітної платні, примусові неоплачувані відпустки, скорочення і просто через інфляцію. Ці жертви спекуляцій навколо економічної кризи стають благодатним об'єктом інформаційних маніпуляцій і спекуляцій навколо політичної кризи.

Інформаційна війна не лише робить сильнішим акцент на аудиторії, але також спрямована на пошуки точок уразливості підсвідомості [165; 166; 167]. Уразливість створює систему входу, в той час як "резонанс" задає систему руйнування на випадок психологічних операцій.

Виділяють такі інструменти впливу на маси: перенесення любові або ненависті на інший об'єкт; ідентифікація дає змогу зближувати одну людину з іншою; міфологізація як відсилання до існуючих у суспільстві міфологічних уявлень, які сприймаються як даність [168, с. 56].

Слід підкреслити наявність відкритих і закритих переходів між інформаційним полем і полем дії. Відкритий перехід зрозумілий і доступний для свідомості споживача (приклад – дії при вигуках "Пожежа!"), закриті ж переходи незрозумілі. Вони можуть включати імплантовані зв'язки, типу зомбування, не доступні для свідомості. По суті вся система пропаганди спрямована на те, щоб досягти автоматизації зв'язків між деякими концептами.

Когнітивний характер інформаційної війни опирається на введення до інформаційного простору супротивника нових елементів, які в кінцевому результаті повинні призвести до змін у просторі його діяльності [169, с.140; 170; 171]. Можемо уявити собі такі види цих нових елементів (назвемо їх трансформаторами), що трансформують інформаційний простір [172, с. 110]: 1) хибні факти (спеціально вигадані, які покликані впливати на підсвідомість у потрібному напрямі); 2) хибні судження, які роблять акцент на емоційному, а не раціональному осмисленні вже наявного фактажу; 3) звичайні факти, введення яких змінює пріоритетність фактів, вже записаних у підсвідомості на перших місцях; 4) стандартні судження, які дають змогу, спираючись на відомості (хибні чи істинні), дійти потрібних висновків.

Чисто фізичні методи управління інформаційним простором – це варі-

мації (пресу) в Україні" дозволяє журналісту збереження таємниці авторства та джерел інформації, за винятком випадків, коли ці таємниці обнародуються на вимогу суду [448, с. 261]. При залученні журналістів для легалізації матеріалів оперативно-розшукової діяльності, відповідно до наказу МВС України від 4 жовтня 2003 р. № 1155 "Про вдосконалення реагування на повідомлення про злочини, інші правопорушення і події та забезпечення оперативного інформування в органах і підрозділах внутрішніх справ України" зазначено: "Відповідальність за... достовірність, повноту і своєчасність подання інформації до... засобів масової інформації покласти особисто на начальників органів та підрозділів внутрішніх справ або осіб, які їх заміщають".

У співдружності з журналістами і коментаторами можливе також проведення ефективних тактичних ігор із злочинними структурами, особливо при вчиненні ними насильницьких злочинів. Широке коло джерел, із яких журналісти можуть черпати свої відомості, у сукупності з агентурно-розвідувальними можливостями оперативних апаратів дозволили б створити цілісну систему спостереження за поведінкою організованих злочинних структур. У ст. 6 Закону України "Про оперативно-розшукову діяльність" зазначено, що підставою для проведення ОРД можуть бути матеріали ЗМІ, в яких міститься достатня інформація про: 1) злочини, що готуються або вчинені невстановленими особами; 2) осіб, які готують або вчинили злочин; 3) осіб, які переховуються від органів розслідування або ухиляються від відбування кримінального покарання; 4) осіб, які безвісти зникли; 5) розвідувально-підривну діяльність спецслужб іноземних держав, організацій та окремих осіб проти України [449, с. 40].

Більш того з урахуванням технологій правомірного психологічного впливу, можливе формування належної суспільної думки відносно певних подій чи діяльності певних осіб.

Таким чином, законодавство України визначає, що повідомлення ЗМІ можуть бути приводами та підставами, як для проведення ОРД, так і для порушення кримінальної справи. Про проблемні питання правового врегулювання порушення кримінальної справи за повідомленнями, оприлюдненими у ЗМІ правильно відмічає Стеценко Ю.В. [450].

Підвищення ефективності роботи правоохоронних органів по розкриттю й розслідуванню злочинів у сфері високих технологій у цей час неможливо без інтеграції в криміналістику нових інформаційних технологій.

Думаємо, що зміст й перспективи розвитку застосування інформаційних технологій і комп'ютерної техніки доцільно розглядати як один з істотних напрямків методології розділу криміналістики - криміналістичної

Слід звернути увагу, що суттєве підвищення ефективності протидії сучасній злочинності може бути досягнуто шляхом широкого використання можливостей спеціальної техніки і сучасних інформаційних технологій. В ОРД вони можуть успішно використовуватися під час підготовки і проведення тактичних і оперативних комбінації та відповідних інформаційних заходів, що пов'язані з методами правомірного психологічного впливу на осіб, які сприяють встановленню істини у конкретних кримінальних справах. Як свідчать результати анкетування працівників оперативних підрозділів карного розшуку, УБОЗ, УКП, ДСБЕЗ, ефективність застосування оперативної комбінації, за їх оцінкою, визначається як: низька – 12,86 %, середня – 64,26 %, висока - 22,88%.

Основною причиною невисокої ефективності застосування оперативних комбінацій є об'єктивні та суб'єктивні фактори. Серед суб'єктивних чинників працівники оперативних підрозділів виділили такі, як відсутність професійних знань 77,12%, а серед об'єктивних – указали на протидію злочинців – 46,28 % опитаних.

Тактичні комбінації з використанням інформаційних технологій можуть використовуватись слідчим, оперуповноваженим, щодо осіб, що становлять оперативний інтерес, або підозрюються в учиненні злочину; з метою збору інформації про особу та її зв'язки; документування злочинної діяльності; встановлення місця знаходження та затримання осіб; при зверненні до осіб, які скоїли злочин і переховуються від органів дізнання та досудового слідства; з метою активізації вольових якостей правослухняних громадян, які з тих чи інших причин уникають можливості повідомити слідчому відому їм інформацію; з метою формування помилкового уявлення про хід розслідування кримінальної справи або дій слідчого; з метою дискредитації, активізації діяльності, поширення тривожної або цікавої для підозрюваного (учасників організованої групи) інформації; з метою попередження (подолання) можливої протидії розслідуванню злочинів, підвищення авторитету правоохоронних органів, зміцнення законності, віри громадян у справедливість закону тощо.

Доцільно, на наш погляд, залучати журналістів до співпраці з оперативними підрозділами і використовувати їх при легалізації матеріалів ОРД. Поширення інформації в ЗМІ здебільшого є надійним і ефективним способом легалізації результатів проведення оперативно-розшукових заходів, за легендою, наприклад журналістського розслідування. Причому ініціатор подібних інформаційних заходів, виражених в проведенні відповідної тактичної комбінації залишає первинне джерело інформації в безпеці. Відповідно до ст. 26 Закону України "Про друковані засоби масової інфор-

анти руйнування інформаційних систем, заглушення технічних об'єктів і психотропного впливу на людину. У фізичному методі інформаційних технологій йдеться про знищення об'єктів або інші варіанти припинення їх нормального функціонування. Для гуманітарних методів інформаційних технологій характерним є збереження функціонування, але з іншим напрямом. Гуманітарні технології намагаються вивести системи, на які вони впливають, на інший рівень шляхом зміни вхідних сигналів. При цьому характерною для них є мінімізація впливу при максимальній зміні результату [173, с. 123].

У рамках організації діяльності щодо протидії злочинності пропонується вважати доцільними використання зазначених властивостей інформації під час проведення оперативно-розшукових заходів з метою впливу на поведінку і позицію осіб шляхом поширення інформації через канали ЗМІ, при проведенні оперативних комбінацій наприклад, через незалежного журналіста, негласного співробітника або конфідента. Можливості ЗМІ необхідно використовувати і слідчими підрозділами.

Важливим аспектом забезпечення ефективності боротьби зі злочинністю є організація взаємодії оперативно-розшукових та слідчих підрозділів із ЗМІ. З множини напрямів і завдань контактування зі ЗМІ відзначимо такі: привертання уваги громадськості до проблем боротьби зі злочинністю; організація допомоги населення у роботі з розкриття та розслідування злочинів; об'єктивне інформування про діяльність правоохоронних органів і запобігання використанню ЗМІ злочинними угрупованнями; використання ЗМІ для виявлення злочинних елементів і дезінформації злочинців.

Щодо перших трьох напрямів, то варто зауважити, що, по-перше, спілкування зі ЗМІ правоохоронних органів, як й інших державних структур, – це веління часу, перетворень, що відбуваються у суспільстві, по-друге, відсутність інформації з боку правоохоронних органів забезпечує свободу появи власної інформації ЗМІ, що може бути як помилковою або такою, що шкодить справі, так і цілеспрямовано перекрученою. Прикладом першого може бути випадок, коли у зв'язку з відмовою в інформації, журналіст розпочав власний аналіз ситуації по вбивству на замовлення і зазначив: "Оскільки на місці вбивства сліди злочинця не виявлені, тепер важливо швидше знайти автомашину, на якій зник вбивця (якщо він її не знищить), щоб там спробувати виявити сліди, які його викривають". Як бачимо, утворилася свого роду методична рекомендація (нагадування) злочинцям. Для появи цілеспрямовано перекрученої публікації видача інформації представником прес-служби правоохоронних органів не буде перешкодою, однак дозволить аргументовано та принародно викривати в

умисному перекручуванні та робити з цього певні висновки (відстежувати, чиї конкретно інтереси “обслуговує” певний журналіст або видання, привселюдно позбавляти їх акредитації з вказівкою підстав для такого рішення тощо [174, с.8; 175, с. 89].

Четвертий напрям використання ЗМІ пов’язаний з новими підходами до боротьби зі злочинністю. У даний час кілери та замовники вбивства іноді шукають один одного через газетні оголошення, вимагателі та квартирні злодії шукають своїх “клієнтів” на основі аналізу оголошень тощо. Ми згодні з думкою, що правоохоронні органи також мають використовувати систему газетних оголошень:

а) з метою виявлення потенційних замовників злочинів і готових їх виконати шляхом розміщення оголошень-пасток;

б) для видачі дезінформації, реакція на яку злочинців або пов’язаних з ними осіб може відстежуватися оперативними службами [176, 12–13].

Небезпека маніпулювання суспільною думкою під час досудового слідства полягає у можливості впливу на дії та рішення слідчого, прокурора, дізнавача, а також програмування поведінки потерпілого, свідків, інших підозрюваних особами, не зацікавленими в об’єктивному розслідуванні злочину. Про можливість впливу ЗМІ на характер прийняття процесуальних рішень зазначає Ю.М. Грошевий. Так проведені ним дослідження показують, що 35% опитаних працівників прокуратури підтвердили те, що на їх позицію як державного обвинувача впливають оцінки злочину та злочинця, що містились у пресі, на радіо та телебаченні. 20% суддів відповіли, що оцінка ЗМІ вплинула на формування їх внутрішнього переконання. У зв’язку з цим Ю.М. Грошевий відзначає, що вплив суспільної думки через повідомлення ЗМІ на слідчих, прокурорів, суддів є явищем, невід’ємним від кримінального судочинства. А тому їм належить вчитись створювати позитивну суспільну думку, а негативну вміти нейтралізувати. При цьому ЗМІ слід розглядати як спеціально створену систему управління суспільною думкою [177, с. 19]. Чільне місце в системі запобігання злочинам належить ЗМІ, нав’язування всьому населенню цілей матеріального успіху, господарювання при недопустимості або явної нерівної допустимості законних засобів для заволодіння ними – у цьому суть аномії як фактора росту злочинності. Використання раціональної системи планування заходів боротьби із злочинністю, основаної на аналізі місцевих особливостей, дасть можливість правоохоронним органам виключити існуючі недоліки, в тому числі в обміні інформацією та використання методів прогнозування, дозволить уникнути негативних наслідків неузгоджених дій з іншими суб’єктами боротьби із злочинністю. Особливим

докладно описуються тяжкі злочини: убивства з особливою жорстокістю, зґвалтування, розбійні напади, вимагання, катування людей і т.ін. Автори "смакують" способи здійснення злочинів, страждання жертв і як би попутно повідомляють о безпомічних, як правило діях правоохоронних органів. У громадян створюється враження, що подібні злочини є звичайною кримінальною практикою [447].

Підтримка дій терористів у ЗМІ, висловлена навіть у непрямій формі, зміцнює єдність терористичних організацій, зменшує внутрігрупові протиріччя, сприяє виправданню самих нелюдських кроків і провокує інших людей до подібних актів соціальної непокори. ЗМІ можуть впливати на формування мотивів і цілей терористичної діяльності, обмін досвідом терористичних дій, рішучість учинити той чи інший злочин. Відомо, що більшість терористичних актів здійснюються по декількох досить поширених сценаріях, про зміст яких стає відомо тільки зі ЗМІ.

Боротьба з подібними явищами, природно повинна охоплювати «інформаційні сфери», які містять у першу чергу засоби масової інформації, а також засоби телекомунікацій і зв’язку, глобальні комп’ютерні мережі, індустрію найрізноманітніших інформаційних послуг.

У контексті організації боротьби з організованою злочинністю і корупцією в державі напрошується висновок, що при плануванні заходів щодо виявлення та розкриття протиправної діяльності організованих злочинних формувань необхідно передбачати заходи щодо ведення інформаційної боротьби з ними, у тому числі захисту від негативного інформаційного впливу на суспільство: протидії формуванню негативного іміджу працівників правоохоронних органів, паніки у суспільстві, кризи влади тощо. Необхідно, також, ввести до навчальних дисциплін “Інформаційне право” та “Теорія організації інформаційної безпеки”, що запроваджуються до навчальних планів вищих закладів освіти МВС України, тематики стосовно технологій ведення інформаційного захисту: інформаційних відносин працівників правоохоронних органів із мас-медіа, журналістами; контрзаходи інформаційного впливу з боку злочинних угруповань на формування негативного ставлення суспільної думки до правомірної діяльності правоохоронних органів.

Водночас аналіз теоретичної розробленості проблем протидії злочинності у сфері інформаційних технологій, їх викриття та документування свідчить, що потребують дослідження способи та прийоми отримання інформації. Виявленню ознак злочинної діяльності сприятиме ефективне використання можливостей ЗМІ, операторів зв’язку, провайдерів, розвідка відкритих джерел інформації в Інтернет тощо.

нів на спроби доведення таких справ до судового вирішення. При цьому, як свідчить практика боротьби з такими злочинами, вагомість, надійність одержання доказів збільшується в декілька разів під час використання сучасної техніки при виявленні та фіксації інформації про злочин.

Згодні, що за окремим таким епізодом порушувати питання про кримінальну відповідальність неправомірно. Подібне може бути підставою для перевірки даної особи, її взяття на оперативний облік, попередження про неналежну поведінку та проведення профілактичної роботи з нею. Але три-чотири попередження можуть слугувати преюдиційною обставиною, оскільки випадково людина не зможе потрапити у подібні ситуації, тим більше декілька разів. Для впровадження таких заходів потрібні зміни в законодавстві, відповідно до якого наведені вище дії можуть бути і самостійними фактами вчинення злочину і особи мають бути притягнуті до відповідальності, якщо в їх діях міститься склад злочину.

Указане вище стосується й боротьби з корупцією, тому що одне з її основних джерел - закритість, непрозорість процесу прийняття рішень владними структурами. Говорячи про цю інформаційну закритість, у першу чергу варто згадати проблеми з доступом до інформації про рішення, прийнятих державними й муніципальними органами влади й управління, проблеми із прозорістю діяльності комерційних структур і проблеми, що виникають із можливістю публікації в ЗМІ матеріалів по антикорупційній тематиці.

Більш того, актуальність цього напрямку дослідження ґрунтується на тенденціях та напрямах протидії тероризму, головною умовою якого є швидка й бурхлива реакція ЗМІ, з метою впливу на суспільство. Не випадково деякі терористи називають ЗМІ передавальним механізмом ("ретранслятором") між терористами й адресатами терору. Дана проблема в науковому й практичному плані є складовою частиною більш широкої проблеми: механізму відтворення злочинності. Як вказує директор Одеського інформаційно-аналітичного центру з проблем протидії організованої злочинності при ОНЮА Дрьомін В.М., сьогодні ми фактично маємо справу із двома видами злочинності: фактичної, з якої зіштовхуються люди в реальному житті, і інформаційною злочинністю (інформзлочинність), тобто злочинністю, вигляд якої створюється засобами масової інформації. Очевидно, що ці два явища не збігаються ні по обсягу, ні по змісту. Якщо в структурі фактичної злочинності переважають корисливі ненасильницькі злочини, то в інформзлочинності домінують тяжкі насильницькі злочини. Дрьомін В.М, методом контент-аналізу вивчив біля п’ятисот публікацій на правові теми в декількох українських центральних і регіональних газетах і виявив, що приблизно 80% з них присвячені проблемам злочинності, причому в переважній більшості статей

моментом в розробленні та реалізації програм профілактики злочинів є підтримка суспільної думки регіону. Для необхідно за допомогою місцевого ЗМІ вивчати пропозиції громадян із питань безпеки та зміцнення правопорядку та вжиття їх при розробці програмних заходів, особливо на стадії реалізації [178, с. 79-80].

Слід відзначити належні зрушення в діяльності правоохоронних органів України по формуванню позитивної суспільної думки, що відбулись останнім часом. Це, зокрема, показали результати програми “Зупини злочинця” у рамках українсько-британського проекту “Впровадження моделі поліцейської діяльності, заснованої на підтримці громадськості, в Україні”, що діяла з 15 січня 2002 р. до 1 квітня 2003 р. в Харкові [179, с. 54]. Програма була організована Харківським МУ МВС спільно з НУВС України за фінансової підтримки уряду Великобританії. Її суть полягала в роботі анонімної телефонної лінії, по якій будь-яка людина могла подзвонити й повідомити будь-яку інформацію про злочин, який готується, або вже скоєний. При цьому кожному, хто телефонує, гарантується повна анонімність. У разі, якщо надана інформація приводить до арешту злочинця, то особа може отримати грошову винагороду. Для створення позитивного відношення громадськості, програма широко висвітлювалась у ЗМІ [180].

Варто привести результати анкетувань, проведених Н.С. Карповим. Так за необхідність встановлення матеріальної винагороди громадянам за допомогу в розкритті злочину висловились переважна більшість (від 89,2 до 100%) практичних працівників правоохоронних органів (керівники, слідчі, оперуповноважені – всього 2215 осіб). Цю ж ідею підтримали від 85,4 до 91,2% проанкетованих громадян України, Росії, Молдови, Білорусі (всього 5038 осіб) [181, с.210].

Нового значення має набути формування правоохоронними органами України у взаємодії із ЗМІ належної суспільної думки для протидії сучасній організованій злочинності та корупції.

Зазначимо, що головною й закономірною метою будь-якого організованого злочинного співтовариства є отримання незаконних прибутків та надприбутків. У міру вирішення цього завдання, а також організаційного й функціонального укріплення організованого злочинного співтовариства у керівників та інших членів такого угруповання можуть виникати й інші цілі, в тому числі й отримання ними політичної влади [164, с. 55]. Про політизацію організованої злочинної діяльності неодноразово відзначається у роботах таких учених-криміналістів, як І.О. Возгрін [182, с. 781], Л.Я. Драпкін [183, с. 364], В.П. Лавров [184, с. 312], І.В. Строков [185, с. 25], М.П. Яблоков [186, с. 35], та інших.

Наприкінці 90-х років XX ст. в Україні, Росії та деяких інших країнах не поодинокими випадками стали намагання учасників організованих злочинних груп просувати своїх членів до органів державної влади, в тому числі й представницьких. Російський оглядач К. Сорокін відзначає, що у кримінальному світі на сьогодні утворилась досить велика група людей, що нажили значно більше матеріальних засобів, ніж це необхідно для задоволення навіть найвибагливіших особистих потреб. Такі люди відчувають зростаючу потребу легалізувати свій капітал, вкласти його у прибуткову, престижну, а головне, легальну справу. Для цього їм самим необхідно "влаштуватись у систему" – наприклад, створити власний суспільно-політичний рух і з його допомогою увійти до органу законодавчої або виконавчої влади, хоча б для початку на регіональному або місцевому рівнях [187]. Перебування в органах влади дозволяє представникам кримінальних структур крім легалізації капіталу, здобутого злочинним шляхом, також уникнути відповідальності за раніше скоєні злочини, уберегтись від тиску та посягань представників інших ОЗУ, продовжувати захоплення уже державної власності, а також здійснювати заступництво та покривання діяльності членів "своїх" організованих злочинних груп. При цьому слушне зауваження робить Н.Б. Бараєва. Вона вважає, що організовані злочинні групи не зацікавлені в отриманні офіційних владних позицій, їх мета – забезпечити власну діяльність, а не приймати на себе обов'язки по управлінню державою. Для цього вони намагаються підсилити свої позиції шляхом укріплення кадрів держапарату [188, с. 315].

В українських ЗМІ також було ряд повідомлень, згідно з якими до представницьких органів влади проникли представники організованих злочинних груп.

Як ми зазначали, М.П. Яблоков серед характерних рис сучасної організованої злочинності Росії виділяє активне використання у своїх інтересах ЗМІ, аж до організації пропагандистських кампаній, які мають на меті не тільки посилення свого впливу на населення, але й розширення свого фінансового, корупційно-кадрового та силового впливу на легальну та тіньову економічну діяльність [189, с. 20-21]. Політизація організованої злочинної діяльності, як її характерна риса за сучасних умов, обов'язково повинна враховуватись при створені відповідних засобів державного й соціального контролю за активністю організованих злочинних груп, тактичних та організаційних прийомів та методів протидії таким суспільно небезпечним проявам. Без сумніву, слід погодитись з твердженням М.П. Яблокова, який вважає, що серед завдань боротьби з організованою злочинною діяльністю входить не тільки власне розкриття та розслідування вчинених членами таких груп злочинів, але й,

необхідне не тільки збільшення потенціалу науково-технічних засобів і методів виявлення та фіксації доказової інформації, а й удосконалення організаційних аспектів її одержання. Це, зокрема, розширення організаційних можливостей використання реєстраційно-облікових даних, наприклад, загального дактилоскопіювання, створення генного обліку, організації зведеного обліку даних про особу на підставі зосередження зведень з усіх видів обліку, наявних у державі, введення особливих форм контролю за поведінкою та діяльністю особи тощо.

Такі пропозиції неодноразово висловлювалися і раніше [444, с. 50; 445]. Винятково важливим для підвищення ефективності боротьби з організованою злочинністю та корупцією є визначення поняття "провокація" та можливостей використання даного засобу у запобіганні та розкритті злочинів, про що йдеться у Програмі "Стратегія і тактика боротьби з організованою злочинністю і корупцією". Необхідно "дати чітке визначення у законодавчому порядку поняття провокації з тим, щоб оперативні комбінації спецпідрозділів при затриманні злочинців з речовими доказами або для одержання доказів їхньої вини у процесі оперативно-розшукової діяльності не були протиправними" [446, с. 32]. Деякі судді підтверджували це своїми вироками про провокаційний характер дій при підготовці та проведенні операцій по затриманню на "гарячому" хабарника на підставі заяви особи, у якої вимагався хабар. Можливість провокації при цьому є і було чимало прикладів, коли таким шляхом усували слідчих. Тому мають бути чітко визначені умови, за яких ця операція може розглядатися правомірною та навпаки – не бути припустимою (наприклад відсутність контролю за обставинами передачі предмета хабара). Є країни, де на рівні державних органів або адміністрацій фірм провадиться "перевірка стійкості на одержання презенту". І там це кваліфікується як засіб очищення державного апарату від несумлінних працівників, а не як шлях притягнення таких до кримінальної відповідальності.

З урахуванням цього було б доцільно передбачити можливість проведення подібних перевірок щодо осіб, на яких надходить інформація про вимагання хабарів або вчинення інших протиправних дій (виявлення зброї, наркотиків, сутенерство тощо). Результатом таких перевірок могло б бути офіційне державне попередження про "неналежну поведінку", що при повторності ситуації могло розглядатися як підстава для вжиття адміністративних заходів і прийняття судового рішення про заборону займатися певною діяльністю, займати визначені посади. Це, зрозуміло, не викорінило подібні соціальні явища, але дозволило б, по-перше, скоротити масовість явищ, подібних хабарництву, по-друге, зменшити витрати правоохоронних орга-

дають можливість реалізувати принципово нові технологічні системи таємного добування інформації.

Розв'язання проблеми нейтралізації протидії ОЗУ органами внутрішніх справ через ЗМІ практичні працівники вбачають у співпраці з журналістами усіх видань і коментаторами програм. Не володіючи журналістською майстерністю, буває досить важко, а часом і неможливо спростувати упереджену необ'єктивну інформацію про дії правоохоронних органів, розповсюджувану ЗМІ. Подана у формі викладу фактів із різким безкомпромісним коментарем є потужним засобом впливу на суспільну думку. Для її спростування потрібний професійний коментар, щоб у кожному прокоментованому факті чітко проглядалася психологічна оболонка, яка містить оцінки, що без відповідних навичок у публіцистиці підготувати дуже складно. У співпраці із журналістами та коментаторами можливе проведення ефективних тактичних ігор із злочинними структурами, особливо при вчиненні насильницьких злочинів. Навмисно поширена у ЗМІ інформація з використанням неправдивої версії здатна відвернути увагу злочинців від здійснюваних оперативно-розшукових заходів, спрямованих на ретельне розкриття злочину. Широке коло джерел, з яких журналісти можуть черпати свої відомості, у сукупності з агентурно-розвідувальними можливостями оперативних апаратів створює цілісну систему спостереження за поведінкою у злочинному середовищі [438, с. 466-467].

Злочинець став значно більш обізнаним і ним (особливо професіоналами) здійснюються різнобічні та вмілі дії щодо незалишення слідів своєї злочинної діяльності, їх приховання, маскування та фальсифікації [439, с. 30–33; 440, 441, 442]. Але знаючи вид комп'ютерної мережі, що стала знаряддям злочину, що зберегла електронно-цифрові сліди, що здатні послужити засобами для виявлення злочину й встановлення обставин вчиненого, слідчому буде досить легко визначити провайдера послуг Інтернету, географічне місце знаходження робочої станції мережі, встановити особистість абонента - користувача, з яким укладений договір при виділенні для надання послуг абонентського номера або унікального коду ідентифікації. В одержанні доказової інформації йому допоможе дослідження «доріжки електронно-цифрових слідів», під якою В.Б. Вехов пропонує розуміти систему утворення слідів у комп'ютерній мережі, що складається з декількох послідовно розташованих за часом і логічно взаємозалежних записів про проходження комп'ютерної інформації з ліній зв'язку через комутаційне встаткування операторів зв'язку від комп'ютера злочинця до комп'ютера потерпілого, і розкриває її зміст, що включає дев'ять елементів [443, с. 78-85]. Отже, для виявлення злочинців та їх викриття

наприклад, розвал таких злочинних утворень, створення умов для їх розпаду. У противному разі зазначена боротьба буде неефективною, бо виявлені та покарані члени таких злочинних організацій без якихось складнощів заміняються іншими, і злочинна організація продовжує існувати й здійснювати свою злочинну діяльність [190, с. 106]. У зв'язку з цим слід відзначити, що останнім часом ряд учених-кримінологів (західні – Н. Крісті, Х. Зер, російські – Я. Гілінський, Г. Забрянський, Л. Карнозова, Р. Максудов, М. Флямер) вказують на "кризу покарання" як такого, а тому необхідність пошуку альтернатив кримінальної юстиції. Ці вчені вважають, настав час перегляду усталених поглядів на засоби протидії злочинності, зміни парадигми [191, с. 42].

Отже, можна сказати, що політика в наш час стає сферою інтересів кримінальних структур, а тому потребує уваги вчених, правоохоронних органів, ЗМІ. На думку Г.Н. Горшенкова, ЗМІ, в силу їх суспільно-політичного призначення, просто зобов'язані інформувати населення про факти, які заслуговують на суспільну увагу, особливо про ті з них, котрі мають важливе значення для формування органів влади, державного та регіонального управління, вибору у владу гідних громадян, які претендують на суспільну довіру, політичне визнання, на владу [192, с. 152, 193, 194]. Враховуючи неможливість у деяких випадках кримінально-процесуальної реалізації інформації про протиправну діяльність або належність до організованих злочинних угруповань кандидатів до органів влади, вважаємо за потрібне розробку тактичного, а також удосконалення нормативно-правового механізму взаємодії правоохоронних органів із ЗМІ для формування належної суспільної думки з метою недопущення кримінальних структур до органів влади. Постає завдання розробки теоретичних та практичних рекомендацій ситуативного попередження проникнення членів ОЗУ до органів державної влади, що направлене на обмеження можливостей здійснення намірів таких осіб [195, с. 37]. Відмітимо можливості українського законодавства щодо непроцесуального використання оперативної інформації, яким може бути її оприлюднення в ЗМІ. Так ст. 26 Закону України "Про друковані засоби масової інформації (пресу) в Україні" дозволяє журналісту поширювати підготовлені ним повідомлення й матеріали під умовним ім'ям (псевдонімом) або без підпису (анонімно), а також збереження таємниці авторства джерел інформації, за винятком випадків, коли ці таємниці обнародуються на вимогу суду. Це дозволяє слідчим і оперативним органам готувати разом із працівниками ЗМІ під виглядом журналістських розслідувань матеріали викривального характеру (які перед цим повинні бути процесуально задокументовані), дифамацію (за умови розголошення лише правдивих свідчень, які дискредитують іншу особу) для формування підґрунтя викриття злочинців.

Серед можливих шляхів створення заслону від проникнення представників організованих злочинних груп до органів державної влади, а також для виявлення та оперативного реагування на факти корупційних дій необхідно розглядати і можливості взаємодії між працівниками ЗМІ та співробітниками правоохоронних органів. Нерідко журналісти отримують інформацію такого характеру, про яку правоохоронцям на той час мало що відомо. Російський учений Н.Є. Павлов відмічає, що по інформованості відносно корупційних дій ЗМІ можуть сповна конкурувати з оперативними підрозділами органів, які здійснюють оперативно-розшукову діяльність; повідомлення про хабарництво досить часто з'являються в періодичних виданнях, передаються по радіо й телебаченню [196, с. 142]. Поряд із великою кількістю повідомлень про невизначені факти корупції у ЗМІ можна зустріти повідомлення про вчинення корупційних діянь конкретними посадовими особами, які є наслідком журналістських розслідувань.

Нових підходів вимагає й ставлення до можливостей залучення ЗМІ у профілактиці проявів корупції. Про необхідність залучення ЗМІ з превентивною метою усунення тиску на органи правосуддя відмічає доктор юридичних наук, професор, народний депутат України В. Сіренко який зазначає, що "будь-які "вказівки" суддям, від кого б вони не виходили, необхідно розглядати як корупційні дії з усіма наслідками прокурорського розслідування і юридичної відповідальності. Такі випадки мають обговорювати у ЗМІ з подробицями журналістського розслідування" [197,198]. Суспільно небезпечні симбіози державної влади та злочинності потребують нових нетрадиційних підходів до розробки та створення способів протидії злочинності в Україні. Серед них належне місце можуть зайняти і ЗМІ: взаємодія органів дізнання і досудового слідства із ЗМІ ефективна для формування належної суспільної думки про учасників організованих злочинних груп, дифамації відносно них, отримання нової криміналістично значимої інформації, непроцесуального використання оперативної інформації, попередження тиску впливових посадових осіб на слідчі та судові органи та інших напрямків, які ще потребують свого обговорення.

2.2. Конфіденційність даних досудового слідства та діяльність засобів масової інформації

У Законі України "Про державну таємницю" від 21 січня 1994 р. (ст. 8) указується, яка інформація може бути віднесена до державної таємниці [199; 200].

різні права доступу і користування інформацією, яка необхідна для виконання задач правоохоронної діяльності. Вказані розходження в даний час є перешкодою не тільки для створення інтегрованої інформаційно-аналітичної системи правоохоронних органів, але й ускладненням обміну оперативною інформацією між оперативними підрозділами [437].

У деякій мірі правоохоронні органи України займаються моніторингом повідомлень ЗМІ. Так у структурі Департаменту зв'язків з громадськістю МВС України функціонують відділ моніторингу та роботи з мережею Інтернет, сектор моніторингу, що займаються виявленням інформації про діяльність ОВС. Департамент інформаційних технологій МВС України, управління (відділи) інформаційних технологій ГУМВС, УМВС, УМВСТ здійснюють інформаційно-пошукові заходи у мережі Інтернет для встановлення осіб, які вчинили злочини, що залишаються нерозкритими. Але доцільно розширити їх функції з метою проведення моніторингу мережі Інтернет і засобів масової інформації (повідомлення в пресі, телебаченню, радіо та ін.) для пошуку відомостей щодо кримінальної активності осіб та груп; нагромадження, первинний аналіз та систематизація інформації, отриманої в ході комп'ютерної розвідки, з метою її подальшого використання зацікавленими оперативними підрозділами; за завданнями оперативних підрозділів та з дозволу суду здійснення негласного отримання доступу через комп'ютерну мережу до певного віддаленого комп'ютера шляхом зламу системи логічного захисту та дистанційному знятті або знищенні (спотворенні) інформації, яка міститься в ньому та розробка пропозицій щодо вдосконалення механізмів дотримання прав і свобод людини в ході підготовки і проведення оперативно-технічних заходів.

Ці обставини, природно, виділяють комп'ютерну розвідку в самостійний напрямок діяльності правоохоронних органів, а у сполученні із аналітичною розвідкою дають можливість говорити про комплекс розвідувальних заходів, що здійснюються на сучасних інформаційних технологіях.

Науково-технічні досягнення останніх років стали основою розвитку й удосконалення тактики застосування спеціальної техніки в ОРД. Потужні можливості криються у поєднанні технічних засобів розвідувального призначення з тактичними завданнями, серед яких найбільш популярними є: контроль психофізіологічного стану людини, негласний акустичний контроль помешкань без розміщення в них будь-якої апаратури, негласний електронний контроль пересування об'єктів у складних міських умовах і т.ін. А такі позитивні зрушення, як застосування цифрових методів опрацювань даних, мініатюризація технічних засобів, нові фізичні принципи дії, не тільки підвищують ефективність вирішення традиційних задач, а й

даткові пільги) і деякі інші. Однак, доступ до цих ресурсів неможливо назвати ефективним і оперативним, тому що його реалізація передбачає складання письмових запитів, надання їх у відповідні організації і витребування відповідей. З огляду на те, що передбачений чинним законодавством термін надання таких відповідей складає один місяць (ч.ч.3 і 4 ст.33 Закону України «Про інформацію»), використання інформаційних ресурсів для виявлення і розслідування злочинів у термін до 3 чи 10 діб (ст. 97 КПК України) не є можливим. Виключенням, зазначеним у ст. 33 Закону України «Про інформацію», є діяльність підрозділів по боротьбі з організованою злочинністю, що відповідно до п.б) ч. 2 ст. 12 Закону України «Про організаційно-правові основи боротьби з організованою злочинністю», мають право одержувати інформацію негайно, або в термін до 10 діб. Таким чином, можна констатувати відсутність реальної можливості забезпечити оперативно-розшуковий супровід, повноту та всебічність розслідування інформації про інформаційні злочини.

Практично оперативні підрозділи в даний час самостійно формують розрізнені масиви відомостей, які використовуються в ході оперативно-розшукової діяльності, застосовуючи як правову основу п. 17 ч. 1 ст. 8 Закону України «Про оперативно-розшукову діяльність». Пошук або формування баз даних здійснюється з ініціативи безпосередніх суб'єктів оперативно-розшукової діяльності, несистемно і тому не дозволяє включати в дані масиви інформацію більшості сфер суспільних відносин, що в сукупності може представляти значний оперативний інтерес у наступному.

Зазначена фрагментарність масивів інформації є наслідком впливу «фактора власника», що значно ускладнює взаємний обмін наявною інформацією навіть у рамках єдиного регіону, і практично виключає міжрегіональний обмін такою інформацією серед оперативних структур. Розглядаючи можливості організації інтегрованої інформаційно-аналітичної системи правоохоронних органів, необхідно відзначити особливості юридичного статусу інформації, що повинна скласти основу інформаційних масивів системи: така інформація, в основному, є конфіденційною, належить до інформації про особистість, і може знаходитися в розпорядженні суб'єктів різних форм власності.

На практиці зазначені особливості впливають на формування правового поля правоохоронної діяльності, що проявляється в неузгодженості законодавчих і нормативно-правових актів. Так, Закони України і нормативно-правові акти, якими визначений статус Державної служби по боротьбі з економічною злочинністю, податкової адміністрації, підрозділів боротьби з організованою злочинністю, Служби безпеки, передбачають

"Таємниця – один із найважливіших інститутів, які визначають співвідношення інтересів особи, суспільства та держави, приватної і публічної основи права, підстави та межі втручання держави у недержавну сферу, ступінь інформаційної захищеності…" [201, с. 124].

Таємниця безпосередньо пов'язана з інформаційною безпекою, під якою розуміється стан захищеності інформаційного середовища суспільства, що забезпечує його формування та розвиток в інтересах громадян, суспільства і держави [202, с. 8].

Державна таємниця – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки й техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди життєво важливим інтересам України, а також ті, що визнанні в порядку, установленому Законом України «Про державну таємницю».

Зі змістовного боку таємниця може бути позначена як блок секретної або конфіденційної інформації (відомостей), що особливим чином охороняється законом, яка відома або довірена вузькому колу суб'єктів у силу виконання службових, професійних та інших обов'язків або окремих доручень, розголошення якої може спричинити юридичну відповідальність.

Разом із терміном "таємниця" у літературі часто трапляється словосполучення "конфіденційна інформація". Етимологічно слово "конфіденційний" походить від латинського confidentia – довіра і в сучасній мові означає довірчий, той, що не підлягає розголошенню, секретний [203, с. 359]. До речі, треба зазначити, що відповідно до ст. 30 Закону України "Про інформацію", інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну і таємну.

Конфіденційна інформація – це відомості, які перебувають у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов. З наведеного випливає, що термін "конфіденційний" має таке ж значення, як і термін "таємниця". Ці поняття – конфіденційний і таємниця – трактуються як рівнозначні і в інших словниках [204, с. 199, 320, 484; 205, с. 95].

Термін "таємниця досудового слідства" не використовується в чинному законодавстві. У статтях 121 КПК і 387 КК України йдеться про дані досудового слідства (дізнання). Цього терміну ми не знаходимо ні в юридичних, ні в енциклопедичних, ні в інших словниках. Але, виходячи з наведених висловлювань учених-юристів щодо таємниці досудового слідства, можна зробити висновок, що він широко використовується у наукових працях. Цей термін трапляється на сторінках періодичної преси [206, с.13; 207, с. 7], його застосовують працівники правоохоронних органів [208, с.

5; 209, с. 2]. Про таємницю досудового слідства писали як вітчизняні, так і зарубіжні вчені-юристи. Це питання висвітлювалося у працях Т.В. Авер'янової, В.П. Бахіна, Р.С. Бєлкіна, О.Д. Бойкова, І.О. Биховського, В.Є. Даліна, А.В. Дулова, І.О. Копилова, В.С. Кузьмічова, В.П. Лаврова, О.М. Ларіна, В.Г. Лісогора, Є.Д. Лук'янчикова, П.Д. Нестеренка, І.Л. Петрухіна, М.В. Салтевського, І.В. Смолькової та ін.

І.О. Биховський указує на те, що тактичні прийоми, застосовані без урахування конкретної слідчої ситуації, можуть спричинити знищення доказів, розголошення таємниці слідства. Він також підкреслює, що до числа загальних тактичних положень, що мають значення для всіх слідчих дій, належить урахування протидії встановленню істини з боку заінтересованих осіб, що зумовлює, зокрема, вживання заходів щодо збереження слідчої таємниці [210, с. 16, 18].

"Слідча таємниця, – зазначає В.Є. Далін, – надає можливість слідчому бути ініціативним навіть у тих випадках, коли інформаційних передумов для цього ще немає. Здатність діяти раптово (діяти несподівано), формувати відомі уявлення у свідомості допитуваного та тому подібні уміння прямо зумовлені можливостями слідчого діяти ініціативно, готуючись таємно від протидіючих осіб" [211, с.102].

Про таємницю досудового слідства пише Є.Д. Лук'янчиков та В.С. Кузьмічов, "Розслідування злочинів передбачає не тільки нерозголошення відомостей про подію злочину та засоби розслідування, а й різноманітну систему заходів, що сприяють вирішенню зазначеного завдання" [212, с. 34-35].

У праці "Тактика использования внезапности в раскрытии преступлений органами внутренних дел" 1990 р. В.П. Бахіна, В.С. Кузьмічова, Є.Д. Лук'янчикова, вказано: "Виходячи з обставин справи, слідчий сам вирішує, які матеріали справи слід зробити надбанням гласності, а які зберегти у таємниці" [213, с. 48]. Далі: "…раптові дії можуть бути засобом збереження слідчої таємниці або запобігання негативним наслідкам її розголошення" [199, с. 49].

Під редакцією Т.В. Авер'янової та Р.С. Бєлкіна у 1997 р. вийшла праця "Криминалистическое обеспечение деятельности криминальной милиции органов предварительного расследования". У ній зазначено, що однією з безпосередніх цілей тактичної комбінації може бути забезпечення слідчої таємниці, у тому числі збереження у таємниці джерел інформації, що має доказовий та орієнтуючий характер [214, с. 82].

Питання, пов'язані з таємницею досудового слідства, висвітлюються й у багатьох інших наукових працях учених-юристів.

Важливість збереження таємниці досудового слідства пов'язана з тим,

орган є спроможним виконувати функції Національного контактового пункту, створення якого передбачено Конвенцією про кіберзлочинність (ст..35). Хоча справедливо відмітити, що спроба створення в Україні міжвідомчої інтегрованої інформаційно-аналітичної системи (МІІАС) правоохоронних органів уже була. З ініціативою про створення такого підрозділу МВС України зверталось до інших правоохоронних органів. Проект створення МІІАС правоохоронних органів міститься у вказівці МВС України від 25.09.1997. У ній, зокрема, зазначається, що головною метою функціонування МІІАС є всебічне інформаційне забезпечення діяльності оперативних служб, експертно-криміналістичних та слідчих підрозділів МВС, СБУ, Генеральної прокуратури, Державної податкової інспекції, Держкомкордону, Міністерства оборони, Державної митної служби та інших зацікавлених відомств під час розслідування злочинів і в розшуковій роботі, підготовка для державних органів інформації по цим питанням та інтеграція у відповідні інформаційні системи [435]. Однак ідея створення такого підрозділу залишилась до кінця не реалізованою. Відсутність інтегрованої інформаційно-аналітичної системи правоохоронних органів, створення якої було передбачено у Законі Україні «Про концепцію національної програми інформатизації» [436] необхідність запровадження національної інформаційної мережі відомостей про осіб, події і факти, що мають значення для проведення оперативно-розшукової діяльності, надзвичайно актуальна для правоохоронних органів України.

Передумови створення централізованої інформаційної мережі сьогодні з'являються в практичній діяльності. На практиці зазначені правовідносини між регіональними підрозділами ОВС і суб'єктами, що володіють необхідною інформацією, здійснюються неформально, в основному, на рівні міжособистісних відносин, а на рівні міністерств і відомств - носять одиничний характер (наприклад, Угода № 3/2340 від 30.09.1998 р. «Про передачу інформації», укладена між МВС України і Державним комітетом статистики України), угоди про обмін інформацією між Державною податковою адміністрацією і митними органами.

На сьогоднішній день правоохоронна діяльність оперативних працівників районного чи міського підрозділу забезпечена інформаційними ресурсами підрозділів оперативної інформації УМВС та обласного адресно-довідкового бюро, до яких мається ефективний оперативний доступ. Крім того, в їх розпорядженні - масиви інформації про реєстрацію суб'єктів підприємницької діяльності, наявність ліцензій на здійснення окремих видів підприємницької діяльності, різні юридичні факти, що характеризують підприємницьку діяльність (наприклад, про факти банкрутства, по-

формації, вже зроблено. У Департаменті ДСБЕЗ МВС України створено відділ боротьби з правопорушеннями у сфері високих технологій. Серед його завдань – здійснення моніторингу мережі Інтернет із метою виявлення розповсюдження інформації злочинного змісту [433]. Відділом по боротьбі з правопорушеннями у сфері високих технологій Департаменту ДСБЕЗ МВС України постійно здійснюється робота у напрямку протидії злочинам, що підготовлюються або вчиняються з використанням комп'ютерних Інтренет-технологій та телекомунікаційних систем – у тому числі екстремістської та терористичної спрямованості. Співробітниками підрозділів по боротьбі з правопорушеннями у сфері високих технологій проводиться постійний моніторинг мережі Інтернет з метою встановлення фактів розміщення інформації екстремістської, терористичної та іншої злочинної спрямованості. Позаштатні негласні працівники також зорієнтовані на висвітлення такої інформації, перш за все, з середовища хакерів та постійних користувачів мережі Інтернет. Співробітниками відділу по боротьбі з правопорушеннями у сфері високих технологій ведеться постійна допомога іншим підрозділам та службам в антитерористичній та антиекстремістській діяльності як інформаційного, так і практичного характеру [434]. . Так, у січні 2002 р., співробітниками відділу надано допомогу у розслідуванні терористичного акту в аеропорту м. Одеси, внаслідок чого викрито злочинне угрупування, яке підготовило цей терористичний акт від імені "хунти Піночета" та висловлювало загрози в разі невиконання їх вимог підірвати в повітрі літак рейсу Одеса-Відень. До Департаменту захисту національної державності та боротьби з тероризмом СБ України надіслано інформацію щодо наявності в Українській складовій всесвітньої інформаційної мережі Інтернет сайтів терористичної спрямованості, отриману за результатами діяльності негласного апарату. Також за допомогою позаштатних негласних працівників отримано інформацію щодо осіб, які за допомогою мережі Інтернет шукають клієнтів, які могли б сплатити за вчинення будь-яких замовлених злочинів на території країн СНД та близького зарубіжжя. Такі підрозділи мають бути створені в інших містах України, крім того, вони мають здійснювати моніторинг ще й інших ЗМІ. Також, на базі Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ України, створено Державну службу спеціального зв'язку та захисту інформації україни, на яку покладено функції реалізації державної політики у сфері захисту державних інформаційних ресурсів у мережах передачі даних, криптографічного та технічного захисту інформації, а також забезпечення захисту державних інформаційних ресурсів у мережах передачі даних. Уявляється, що саме цей

щоб у практиці правоохоронних органів уникнути випадків, які мають місце, коли внаслідок невжиття заходів щодо її збереження була розголошена інформація, отримана у ході слідства, що у свою чергу призводило до значних збитків і компрометації людей, заподіяння їм моральної шкоди. Недодержання таємниці спричиняє небажані наслідки, знижує ефективність процесу розслідування, ставить під загрозу осіб, які сприяли розкриттю злочину [215, с. 189; 216, с. 3; 217, с.96]; попередні рішення та висновки можуть вплинути на формування показів свідків і суспільної думки, завдати незаслуженої шкоди репутації людей [218, с.58]; ускладнити роботу слідчого з розслідування злочинів, стати на перешкоді отримання необхідної інформації, збільшити обсяг проваджуваних слідчих дій – і строк, установлений для досудового слідства, буде порушеним. Особам, які вчинили злочини, часто вдається знищити сліди злочину, сховати майно, на яке міг бути накладений арешт, приховатися від слідства, підготувати докази своєї "невинуватості", здійснювати вплив на потерпілих, свідків із метою схилити їх до давання завідомо неправдивих показань тощо. Кримінальні справи ще на стадії досудового слідства, не доходячи до суду, закриваються.

Успіх проведення розслідування залежить від нерозголошення отриманої інформації, збереження у таємниці дій, що плануються та проводяться. Відповідно до цього слідчий під час здійснення тактичних комбінацій, а також загалом у ході розслідування має дотримуватись збереження таємниці досудового слідства, повідомляти інших осіб лише про необхідне для виконання тієї чи іншої дії, вживати заходів щодо забезпечення нерозголошення інформації, що становить цю таємницю, та обмеження кола осіб, які могли б отримати її, щоб інформація не була використана з метою, яка суперечить завданням процесу розслідування. Як підкреслює Ю.П. Аленін, "важливою гарантією успіху розслідування є і дотримання учасниками слідчих дій вимог про неприпустимість розголошення даних досудового слідства (ст. 121 КПК). У ході слідчої дії можуть бути отримані важливі дані, розголошення яких неприпустимо до певного моменту з тактичних або інших міркувань" [219, с. 58].

Плануючи такі дії, необхідно зберігати таємницю їх підготовки, виходячи з того, наскільки повно вони можуть бути збережені у таємниці від обвинуваченого або підозрюваного.

Збереження таємниці досудового слідства, дозволяє слідчому володіти тактичною ініціативою, що, у свою чергу, сприяє можливості оперативно отримувати інформацію, діяти несподівано, готувати свої дії таємно від підозрюваного, обвинуваченого, а також осіб, які можуть вчинювати про-

тидію слідству, формувати в обвинуваченого необхідне слідчому уявлення про хід розслідування, дозволяє слідчому приховати свою необізнаність про певні деталі події злочину, а також створювати необізнаність у підозрюваного, обвинуваченого чи осіб, які протидіють розслідуванню [220, с. 95].

Таємниця досудового слідства належить до професійних таємниць, в основі яких лежать особисті таємниці.

Проблемами особистих і професійних таємниць займалось широке коло правознавців. Серед них можна назвати М.С. Алексєєва, О.Д. Бойкова, В.Є. Гулієва, Л.Д. Кокорєва, В.О. Коновалову, В.М. Корнукова, Л.О. Красавчикову, С.М. Логінову, П.І. Люблінського, З.В. Макарову, М.С. Малеїна, Г.Д. Мепаришвілі, Я.О. Мотовиловкера, І.Л. Петрухіна, Ф.М. Рудинського, І.В. Смолькову, Ю.І. Стецовського, Н.В. Устименко та ін.

До особистих таємниць Г.Д. Мепаришвілі відносить таємницю житла й особистих документів, зміст листування, телеграфних повідомлень та телефонних переговорів, а до професійно довірених – адвокатську таємницю, лікарську таємницю, таємницю грошових вкладів, таємницю нотаріальних дій, таємницю усиновлення, таємницю сповіді [221, с.9].

І.Л. Петрухін до особистих таємниць відносить таємницю творчості і спілкування, таємницю сімейних та інтимних взаємин, таємницю житла, щоденників, особистих паперів, таємницю поштово-телеграфної кореспонденції і телефонних переговорів. До професійних таємниць належать медична таємниця, таємниця судового захисту та представництва, таємниця сповіді, таємниця усиновлення, таємниця попереднього слідства, таємниця нотаріальних дій і записів актів громадянського стану. В основі професійних таємниць лежать особисті таємниці, захищені від розголошення правовими заборонами, що адресовані тим, кому ці таємниці за необхідністю довірені [222, с.15].

Як правильно зауважує Н.В. Устименко, під таємницею особистого життя розуміє відомості конфіденційного характеру про різноманітні сторони індивідуальної життєдіяльності людини, розголошення яких завдає або може завдати людині шкоду [223, с. 11].

У ст. 9 Закону України "Про оперативно-розшукову діяльність" вказано: забороняється передавати й розголошувати відомості про нерозкриті злочини або такі, що можуть зашкодити слідству чи інтересам людини, безпеці України. Також у ній зазначено, що не підлягають передачі й розголошенню відомості, що стосуються особистого життя, честі, гідності людини [224]. Так у ході проведення тактичних комбінацій при ознайомленні з документами, змістом листування, може стати відомою інформа-

протидії, правоохоронні органи України практично не займаються виявленням ознак злочинів із повідомлень ЗМІ для оперативного реагування. Це пов'язано з тим, що специфіка основної роботи оперативного уповноваженого, слідчого, прокурора не містить у собі елементу пошуку інформації з газет, журналів, теле- та радіопередач, Інтернет-ЗМІ. Звичайно, що слідчий після ознайомлення з матеріалами різних кримінальних справ, в яких для вчинення злочинів злочинцями були використані повідомлення ЗМІ, може виявити схожі обставини вчинення злочинів. Установлення їх подібності дозволить зробити висновок про діяльність однієї особи або групи. Однак проведення такого порівняльного аналізу слідчим або слідчо-оперативною групою обмежується лише територією міста, району, у крайньому разі області чи регіону. Охопити весь масив інформації, що міститься у повідомленнях ЗМІ від загальнодержавних до регіональних людина фізично не в змозі. Не повинні цим займатись і працівники ЗМІ. Тому шляхом вирішення цієї проблеми, на нашу думку, повинне стати створення загальнодержавних спеціальних інформаційно-аналітичних підрозділів, які б займалися моніторингом повідомлень ЗМІ. Після виявлення потрібної інформації вони б передавали її відповідним підрозділам для перевірки та реагування.

Підрозділи, що здійснюють моніторинг відкритих джерел інформації з метою виявлення криміналістично значимої інформації, вже давно існують у США, ФРН та багатьох інших країнах. Так фахівці ФБР запевняють, що до 90% інформації стратегічного характеру можна взяти з відкритих джерел: газет, журналів, телебачення, радіо, комп'ютерів [428, с. 109]. Спеціальні підрозділи комп'ютерної розвідки США (ФБР) та ФРН (ВКА) відслідковують кримінальні явища в мережі Інтернет [429, с. 325].

Відмітимо, що відповідно до Законів України "Про організаційно-правові основи боротьби з організованою злочинністю" (ст. 9) та "Про Службу безпеки України" (ст. 10) в МВС та Службі безпеки України створено інформаційно-аналітичні підрозділи. Серед їх завдань відзначено і викриття та припинення діяльності організованих злочинних груп. Останніми роками в науковій літературі дедалі більше відзначається про необхідність формування та розвитку нових напрямків інформаційного забезпечення протидії злочинності, у тому числі через розвиток аналітичних служб [430, с. 118; 431, с. 13; 432, с. 232 та інші]. Ця ідея, на думку автора, може бути перспективною стосовно проведення аналізу повідомлень ЗМІ з метою виявлення криміналістично значимої інформації.

Перші кроки у створенні в Україні підрозділів, що проводять моніторинг повідомлень ЗМІ з метою виявлення криміналістично значимої ін-

спеціалізованих підрозділів ОВС України названо виявлення учасників організованих злочинних угруповань. Прямі вказівки на вжиття органами дізнання необхідних оперативно-розшукових заходів із метою виявлення ознак злочину й осіб, які його вчинили, містить ст. 103 КПК України. Про пошук і фіксацію фактичних даних про протиправну діяльність окремих осіб та груп, як завдання оперативно-розшукової діяльності говориться в ст. 1 Закону України "Про оперативно-розшукову діяльність".

Потреба у проведенні спеціальних заходів щодо виявлення та розкриття злочинів виникає як наслідок об'єктивних, так і суб'єктивних причин. По-перше, це пов'язано із тим, що особами, які вчиняють злочин, виконуються дії щодо приховування його слідів. Іншою причиною потреби проведення спеціальних заходів щодо виявлення та розкриття злочинів є те, що окремі суспільно небезпечні діяння характеризуються високим ступенем латентності.

Виявлення та розкриття злочинів потребує використання криміналістичних знань не лише на стадії їх розслідування, а й під час проведення організаційних та оперативно-розшукових заходів до порушення кримінальної справи. Із цього можна зробити висновок, що під час проведення оперативно-розшукових заходів щодо виявлення злочинів не лише можна, а й вкрай необхідно застосовувати напрацювання криміналістичної науки щодо характеристики способів підготовки вчинення злочину, приховування його слідів, характеристики поведінки злочинця тощо. Тобто процес виявлення та розкриття злочинів повинен мати відповідне криміналістичне забезпечення (техніко-криміналістичними засобами, тактичними прийомами, методичними рекомендаціями) [424, с.212-213, 425]. Традиційними формами виявлення злочинів органами дізнання і досудового слідства є: 1) розгляд заяв та повідомлень про злочини; 2) безпосереднє виявлення ознак злочину. На думку В.М. Григор'єва діяльність правоохоронних органів із виявлення ознак злочину починається з отримання та перевірки інформації щодо протиправності певної події і завершується прийняттям рішення стосовно порушення або відмови у порушенні кримінальної справи [426, с. 40]. Однак попри значну увагу законодавця питання, пов'язані з виявленням злочинів, не достатньо висвітлені в юридичній літературі. В.В. Степанов справедливо зазначає, що виявленню злочинів у криміналістиці приділялось явно недостатньо уваги, не дивлячись на те, що своєчасна поінформованість компетентних органів про скоєний злочин дозволяє ефективно організувати роботу по його розкриттю [427, с. 147].

Не маючи належних теоретичних напрацювань та правових засобів

ція, що становить особисту таємницю його й інших осіб. У силу своїх обов'язків, слідчий стає власником отриманої інформації і повинен забезпечувати конфіденційність відомостей.

Саме на це спрямовані норми Конституції України (ст. 31), які гарантують кожному таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом [225].

Досить проблематичним залишається правове забезпечення нерозголошення даних досудового слідства стосовно діяльності ЗМІ.

В.Г. Лісогор справедливо відзначає, що у наш час ЗМІ стали одним із способів розголошення таємниці досудового слідства [226, с. 9].

Положення ст. 121 КПК України відобразились у Законах України "Про інформацію" (ст. 46), "Про друковані засоби масової інформації (пресу) в Україні" (ст. 3), "Про інформаційні агентства" (ст. 2), "Про телебачення і радіомовлення" (ст. 2), "Про міліцію" (ст. 3), "Про прокуратуру" (ст. 7), "Про Службу безпеки України" (ст. 7). У зазначених нормах забороняється розголошення передбаченої законодавством таємниці. У Законі "Про інформацію" серед основних принципів інформаційних відносин названо відкритість та доступність інформації, а також гарантованість права на інформацію, яке забезпечується обов'язком органів державної влади інформувати про свою діяльність та прийняті рішення (ст. 10). Право громадськості на інформацію про діяльність правоохоронних органів забезпечується Законами України "Про міліцію" (ст. 3), "Про прокуратуру" (ст. 6), "Про Службу безпеки України" (статті 3 і 7). Норми цих законів зобов'язують інформувати державні органи влади, громадські організації, населення про свою діяльність через ЗМІ. У такий спосіб реалізується принцип гласності в діяльності правоохоронних органів України. Стаття 32 Закону України "Про інформацію" надає право журналісту звернутись з інформаційним запитом про діяльність органів виконавчої влади та їх посадових осіб. На що ті зобов'язані надати інформацію, що стосується їх діяльності, письмово, усно, по телефону чи використовуючи публічні виступи своїх посадових осіб. Однак ст. 37 гарантує збереження в таємниці даних досудового слідства. У ній зазначено, що не підлягають обов'язковому наданню для ознайомлення за інформаційними запитами офіційні документи, які містять інформацію про оперативну роботу органів прокуратури, МВС, СБУ, роботу органів дізнання та суду у тих випадках, коли її розголошення може зашкодити оперативним заходам, розслідуванню чи дізнанню, порушити право людини на справедливий та об'єктивний судовий розгляд її справи, створити загрозу життю або здо-

ров'ю будь-якої особи. Заборона журналістам розголошувати дані досудового слідства та право слідчого відмовити журналістам у висвітленні подій кримінального характеру гарантується ст. 15 Закону "Про державну підтримку засобів масової інформації та соціальний захист журналістів", яка покладає на журналіста обов'язок дотримуватись вимог щодо нерозголошення планів спеціальних підрозділів, відомостей, що є таємницею слідства, не створювати штучної психологічної напруги в суспільстві. Про необхідність співробітництва між правоохоронними органами та ЗМІ за умови дотримання вимог нерозголошення даних досудового слідства йдеться в Указі Президента України від 9 грудня 2000 р. "Про додаткові заходи щодо безперешкодної діяльності засобів масової інформації, подальшого утвердження свободи слова в Україні" [227, с. 40].

Право ЗМІ висвітлювати всі аспекти діяльності правоохоронних органів, а також обов'язок останніх по відношенню до ЗМІ в наданні повної інформації про свою діяльність закріплено в ст. 2 Закону України "Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації". Правоохоронні органи як органи державної влади зобов'язані надати ЗМІ повну інформацію про свою діяльність через відповідні інформаційні служби, забезпечувати журналістам вільний доступ до неї, крім випадків, передбачених Законом України "Про державну таємницю". У свою чергу ЗМІ можуть проводити власне дослідження й аналіз діяльності зазначених органів, їх посадових осіб, давати їй оцінку, коментувати [228, с. 311].

Деякі автори вказують: "Значна кількість опитаних слідчих (43%) негативно ставляться до повідомлень засобів масової інформації про розслідування і його результати до вступу вироку в законну силу. Кожний десятий слідчий відзначив, що повідомлення про те, як іде розслідування у кримінальній справі, заважає його об'єктивному проведенню" [229, с.62].

Однією з причин порушення вимог щодо розповсюдження інформації про процес розслідування є прогалини у галузевому законодавстві. У законодавстві недостатньо чітко регламентовано правила розповсюдження інформації про кримінальний процес, а також немає санкцій за порушення заборони на розповсюдження такої інформації. Прогалиною законодавства можна назвати і те, що у ньому бракує норм, які встановлюють порядок висвітлення засобами масової інформації матеріалів певних кримінальних справ до вступу вироків у них у законну силу [230, с.142].

Недієвість ст. 121 КПК України по відношенню до працівників ЗМІ, які безпосередньо не були попереджені слідчим про нерозголошення даних досудового слідства, а також вказаних положень інформаційного за-

3.2. Виявлення ознак злочинної діяльності організованих злочинних угруповань із використанням інформаційних технологій

Важливим елементом роботи органів дізнання та досудового слідства є діяльність із виявлення злочинів, що зумовлює можливість ефективної протидії сучасній злочинності, швидкого й повного розкриття злочинів, викриття винних, а також припинення та попередження протиправних дій. Під виявленням злочинів, на думку І.П. Герасимова, слід розуміти поінформованість компетентних органів про вчинення протиправного діяння [416, с. 28]. В.О. Ледащев розуміє під цим виявлення ознак злочину в результаті пізнавальної діяльності органів дізнання та досудового слідства, що здійснюється криміналістичними методами та документально зафіксована [417, с. 20].

У криміналістиці цей напрямок діяльності органів дізнання та досудового слідства ще називають пошуковим. Так М.Г. Шурухнов відмічає, що пошукова діяльність слідчого – це комплекс процесуальних і непроцесуальних засобів, які реалізовує слідчий при розслідуванні злочину з метою забезпечення збирання доказів і пізнання всіх обставин, які мають значення для правильного вирішення кримінальної справи [418, с. 261]. В.Л. Васильєв пише, що основна сутність пошукової діяльності полягає у виявлені із зовнішньої середи інформації, значимої для розкриття злочинів даної категорії [419, с. 88]. Про пошуковий аспект діяльності слідчого відзначає В.І. Галаган [420, с. 129]. Однак пошукова діяльність є також складовою ОРД. Так, І.П. Козаченко під пошуковими заходами ОРД розуміє "дії оперативних працівників по встановленню ще невідомих подій злочину і винних осіб, злочинів, що готуються або вчинені невстановленими особами" [421, с. 15]. Про пошукову діяльність оперативних служб ОВС, направлену на виявлення злочинів та осіб, які готують або вже вчинили злочини відзначають ряд російських учених [422, с. 52]. На думку Д.І. Сулейманова, основу пошуку джерел криміналістично значимої інформації складає комплекс слідчих і оперативно-розшукових дій [423, с. 25].

Варто відзначити, що на важливість виявлення злочинів у діяльності правоохоронних органів зазначається у положеннях ряду нормативно-правових актів. Так на виявлення злочинів як обов'язок ОВС, що випливає з основних завдань міліції, вказує Закон України "Про міліцію" (ст. 10), як обов'язок СБУ – Закон України "Про Службу безпеки України" (ст. 24). У ст. 6 Закону України "Про організаційно-правові основи боротьби з організованою злочинністю" серед основних напрямків діяльності

ваного укріплення оперативних позицій в середовищі організованої злочинності та спрямованість оперативно-агентурного апарату не тільки на тактичне документування конкретних злочинів, що як правило вчиняють низові ланки організованих злочинних груп, а й на стратегічні цілі злочинних економічних схем, викриття лідерів, їх корумпованих зв'язків, реального, а не задекларованого підриву економічної основи; ініціювати прийняття низки нормативних внутрішньовідомчих і міжвідомчих нормативних актів та відповідних змін до чинного законодавства, спрямованих на безумовне забезпечення комплексної системи інформаційно-аналітичного забезпечення. Система розвідувально-інформаційного та аналітичного забезпечення підрозділів БОЗ повинна бути створена для підвищення ефективності й цілеспрямованості протидії організованим злочинним угрупованням шляхом використання всіх наявних у системі МВС України, інших державних і недержавних структурах сил та засобів для збирання, оброблення, накопичення та аналізу інформації щодо проявів організованої злочинності й корупції в державі.

конодавства зумовлена невизначеністю поняття "дані досудового слідства", порядку попередження про недопустимість розголошення, отримання дозволу, межа дозволеного та ряд інших, про які вже неодноразово зазначали вчені-юристи. Намагання злочинців отримати відомості, що складають таємницю слідства, значно збільшуються при розслідуванні діяльності ОЗУ. Спільниками злочинців, як випадково, так і навмисно, в цьому відношенні нерідко виступають ЗМІ [231, с. 327]. Випадки передчасного оприлюднення в ЗМІ повідомлень, що могли завадити проведенню оперативних та слідчих заходів, вже мали місце в практиці правоохоронних органів України. Так 6 квітня 2003 р. невідомі викрали директора Новоселицького лікеро-горілчаного заводу І.А. Нежурбіду. Наступного дня вони зателефонували його сім'ї, вимагаючи 300 тис. дол. США за його звільнення, а також застерегли від звернення в міліцію. Прослуховування телефонних розмов дозволило встановити місце перебування викрадачів і заручника, але ЗМІ оприлюднили чутки про викрадення директора. Після цього викрадачі змінили місце схованки. Співробітникам міліції знадобилось кілька додаткових днів, щоб його встановити, затримати 5 викрадачів і звільнити І.А. Нежурбіду. У затриманих вилучили 300 набоїв до пістолета ТТ, нарізну та гладкоствольну вогнестрільну зброю. З цього можна зробити висновок, наскільки реальною була загроза життю потерпілого і наскільки непродуманими були намагання працівників ЗМІ висвітлити цю подію кримінального характеру. Відмітимо, що через подібні обставини у вересні 1977 р. німецькі журналісти утримались від висвітлення звільнення Президента спілки підприємців ФРН Ханса-Мартіна Шляйєра, аби не зашкодити його звільненню. Тоді федеральний уряд прийняв рішення в інтересах потерпілого та його розшуку не давати ніякої інформації про ведення переговорів із терористами та процес розслідування цієї справи. Заборона на передачу інформації відносилась лише до державних відомств. Журналістам, із правової точки зору, не заборонялось повідомляти громадськість про цей злочин. Однак більшість із них добровільно відмовилась поширювати інформацію, якою володіли, не зважаючи на мовчання із цього приводу державних органів [232, с. 5].

В.П. Бахін, І.В. Гора, П.В. Цимбал, говорячи про проблеми взаємовідносин правоохоронців із ЗМІ зазначають: "У своїй більшості практичні працівники розглядають "участь" преси як перешкоду, "вторгнення" в закриту зону, а допомогу бачать лише в передачі розшукової інформації. Дійсно, бажання журналістів "знайти все" і безконтрольне висвітлення того, що стало відомим та "своїх прогнозів", може стати суттєвою перешкодою розслідуванню. …Для попередження цього потрібно не "відмахуватися від

преси", а за власною ініціативою повідомляти журналістам можливе, у потрібному ракурсі і з вказівкою на ті аспекти, які на даний час не слід зачіпати. Причому найкраще передавати пресі офіційні письмові заяви та повідомлення, щоб виключити можливість перекручування усних заяв" [233, с. 301]. Згідно з Положенням про Центр громадських зв'язків МВС, ГУМВС, УМВСТ, затверджене наказом МВС України № 1357 від 31 жовтня 2003 р. [234], на центри покладається забезпечення організації взаємодії із ЗМІ, населенням, трудовими колективами, громадськими організаціями з метою інформування про стан правопорядку в державі, заходи ОВС щодо його зміцнення, формування позитивного іміджу міліції України, аналіз розміщених у ЗМІ матеріалів щодо діяльності ОВС, своєчасне інформування про них керівництва, забезпечення акредитації журналістів, організація їх участі у брифінгах, прес-конференціях тощо. Відповідно до наказу МВС України від 25 березня 2004 р. № 330 у складі Міністерства на базі Центру громадських зв'язків (на правах управління) створено Департамент зв'язків з громадськістю [235]. . Також, Наказом МВС України від 30 квітня 2004 р. № 458 затверджено Положення про основи організації розкриття органами внутрішніх справ України злочинів загальнокримінальної спрямованості. Відповідно до пунктів 2.3.7 і 4.1.2 цього наказу організацію використання ЗМІ з метою встановлення і затримання злочинців покладається на начальників ГУМВС, УМВС, УМВСТ, міськ-, рай-, лінорганів. На жаль, створення груп громадських зв'язків лише за необхідності не завжди позитивно відбивається на рівні інформаційного супроводження розкриття та розслідування злочинів, адже на ці посади можуть призначатись співробітники без належної професійної підготовки. Центр виконує загальні функції щодо інформування населення про діяльність ОВС. Саме тому, з метою створення чіткої системи взаємодії слідчого з іншими учасниками розслідування, подолання управлінських та організаційних труднощів у слідчій діяльності, інформування щодо ходу і результатів розслідування справи, проведення інформаційно-тактичних операцій та інших напрямків що зазначаються в роботі, і потрібна взаємодія слідчого з засобами масової інформації.

Справедливою також є думка В.С. Кузьмічова про те, що взаємодію слідчого з представниками ЗМІ слід будувати на чіткій та гнучкій системі випереджувального інформування журналістів про обставини, що на даний момент можуть і повинні стати надбанням гласності. Це ґрунтується на тому, що в умовах розвитку демократії факт вчинення й розкриття злочину повинен бути оприлюднений. Особливого значення це набуває тоді, коли скоєні тяжкі злочини, котрі викликали великий суспільний і психологічний резонанс [236, с. 32].

техніки в навчанні слідчих, що здійснюється шляхом використання: імітаційно-навчальних програм-тренажерів; контрольно-навчальних і інших програм.

Стосовно оперативно-розшукових підрозділів, з огляду на світовий досвід, інформаційне забезпечення повинно здійснюватися шляхом формування електронних досьє за такими пов'язаними між собою основними базами даних, як злочинні групи; події та злочини; особи оперативна та інша інформація; кримінальні та оперативні справи; об'єкти; транспортні засоби; документи на основі накопичення та систематизації в електронному вигляді всієї інформації, здобутої як у результаті оперативно-службової діяльності безпосередньої підрозділів БОЗ та інших служб і органів внутрішніх справ (внутрішні джерела інформації), так і наданої (або здобутої із застосуванням гласних і негласних методів оперативних методів оперативної роботи) іншими державними і недержавними структурами оперативної, облікової, статичної та аналітичної інформації (зовнішні джерела інформації).

До найвагоміших зовнішніх джерел інформації слід віднести такі автоматизовані обліки: абонентів телефонної та інших телекомунікаційних мереж (організації зв'язку); суб'єктів господарської діяльності та їх засновників (Держкомстат); фізичних та юридичних осіб платників податків (ДПА), суб'єктів зовнішньоекономічної діяльності (МЗС); вантажні митні декларації (Митна служба); власників нерухомості (БТІ); зареєстрованого АМТ, зброї, охоронних структур, закордонних паспортів (ОВС); інформація по великомасштабних та сумнівних операціях по рахунках клієнтів (НБУ, комерційні банки), проплата з пластикових карток (процесингові центри); Інтернет та інші відкритті джерела інформації.

Запровадження такої системи дасть змогу виявляти нові злочинні та корупційні зв'язки, схеми, економічне підґрунтя та відмивання коштів накладання та аналізу оперативної інформації та довідкових обліків [415, с. 353-355].

З метою створення єдиної загальнодержавної, комплексної системи розвідувально-інформаційного та аналітичного забезпечення необхідно здійснити такі заходи: у рамках концепції кримінальної розвідки розробити та затвердити положення про систему інформаційно-аналітичного забезпечення; створити схему та налагодити надходження інформаційних потоків з внутрішніх та зовнішніх джерел як по офіційних каналах, так і за допомогою гласних та негласних методів оперативно-розшукової діяльності; провести відповідні та організаційно-штатні зміни в ГУБОЗ МВС України та його регіональних підрозділах; провести заходи із цілеспрямо-

банків даних в умовах інформаційної невизначеності [414].

При плануванні слідчим розслідування цих видів злочинів можливо також використання інформаційних технологій: наукової, довідкової й методичної інформації, що зберігається на магнітних носіях; даних загальноправових довідкових систем; інформації, що зосереджена в загальнодержавних, відомчих або регіональних банках даних; баз даних установ, підприємств, організацій і інших юридичних осіб; баз даних Інтернету, а також локальних мереж. Використання електронної пошти для листування по кримінальних справах дозволяє автоматизувати: напрямок запитів, листів, повідомлень і іншої інформації із кримінальних справ на адресу установ, підприємств, організацій і інших юридичних осіб; одержання інформації від установ, підприємств, організацій і інших юридичних осіб відповідно до спрямованих запитів на їх адресу по електронній пошті або в інший спосіб.

Застосування слідчим комп'ютерних технологій при плануванні розслідування по кримінальних справах і здійсненні контролю за виконанням запланованих слідчих дій, оперативно-розшукових, організаційних і інших заходів можливо у випадку використання: баз даних у вигляді таблиць текстових процесорів (редакторів); баз даних, створених за допомогою редакторів електронних таблиць; власних баз даних, розроблених за допомогою найпоширеніших систем управління базами даних; спеціально розроблених підсистем АРМ слідчого (по розслідуванню злочинів окремих видів); комплексної автоматизованої інформаційної системи слідчого.

Використання слідчим комп'ютерних баз даних для контролю за дотриманням процесуальних термінів затримання підозрюваних, утримання під вартою обвинувачуваних (підозрюваних), досудового слідства й інших, передбаченим кримінально-процесуальним законодавством, термінів, можливо шляхом використання, наприклад: списків кримінальних справ, підготовлених у формі таблиць текстових редакторів; списків кримінальних справ, підготовлених за допомогою редакторів електронних таблиць; картотек і списків кримінальних справ, підготовлених за допомогою систем управління базами даних; баз даних спеціально розроблених підсистем автоматизованого місця слідчого (по розслідуванню окремих видів злочинів).

Застосування комп'ютерних технологій слідчим при оцінці наявних у справі доказів, у тому числі отриманих або виготовлених іншими учасниками кримінального процесу з використанням комп'ютерних технологій можливо, наприклад, коли слідчим застосовуються комп'ютерні програми, ідентичні тим, які використовувалися експертом при провадженні експертизи.

Крім цього можливе ефективне використання засобів комп'ютерної

Суперечливим у сфері кримінального судочинства залишається положення щодо допустимості під час досудового слідства виступів співробітників правоохоронних органів у ЗМІ, а також публікацій та коментарів журналістів із приводу кримінальних справ, що розслідуються. Важливості визначення критеріїв допустимості таких виступів додає те, що у цьому випадку правоохоронні органи та ЗМІ обов'язково повинні додержуватись принципу презумпції невинуватості. Зміст цього принципу викладений у ст. 62 Конституції України та ст. 15 КПК України і полягає у тому, що будь-яка особа вважається невинною у вчиненні злочину і не може бути піддана кримінальному покаранню, доки її вину не буде доведено в законному порядку і встановлено обвинувальним вироком суду.

Варте уваги рішення Євросуду у справі "Аллене де Рібемон проти Франції" від 10 лютого 1995 р. у частині, яка стосується допустимості заяв працівників правоохоронних органів про винність особи у вчиненні злочину. У світлі зазначеної проблеми щодо виступів співробітників правоохоронних органів не зайвим буде привести положення цивільного законодавства. Так, відповідно до ст. 296 ЦК України використання імені фізичної особи з метою висвітлення її діяльності, що ґрунтується на відповідних документах (звіти, стенограми, протоколи, аудіо-, відеозаписи, архівні матеріали тощо), допускається без її згоди. Ім'я фізичної особи, яка затримана, підозрюється чи обвинувачується у вчиненні злочину може бути обнародуване лише у разі набрання законної сили обвинувальним вироком суду. Ім'я потерпілого від правопорушення може бути обнародуване лише за його згодою. Використання початкової літери прізвища фізичної особи у ЗМІ не є порушенням її права [237].

Можливість оприлюднення через ЗМІ імен осіб, які підозрюються у вчиненні злочину, ставить питання про допустимість використання у кримінальному судочинстві дифамації. Адже оприлюднення імені особи, яка є підозрюваною у кримінальній справі, може дискредитувати її. Крім того, не поодинокими є випадки, коли особи, стосовно яких були висунені обвинувачення у вчиненні злочину, боячись громадського осуду, накладали на себе руки. Якщо звернутись до судової практики та рішень Євросуду щодо допустимості використання дифамації, то можна побачити, що Суд неодноразово висловлював свою думку про те, що журналіст має право не розкривати свої джерела (наприклад справа Гудвін проти Об'єднаного Королівства [238] та користуватись будь-якими з них, у тому числі й чутками. Судові рішення, які стосуються діяльності журналістів, свідчать, що важливішим виглядає соціальне значення оприлюдненої інформації, ніж формальне порушення закону, а компенсація за дифамацію

може бути присуджена тільки у випадку, якщо особа доведе злий умисел.

Законом не забороняється оприлюднювати інформацію через ЗМІ щодо особи запідозреної (обвинуваченої) у вчиненні злочину за наявності відповідних кримінально-процесуальних документів, окрім відносно неповнолітніх.

Крім того, працівники ЗМІ мають право самостійно збирати, а потім поширювати інформацію про злочин, по якому проводиться досудове розслідування. Цей вид діяльності журналістів отримав назву "журналістське розслідування" і останнім часом набув великої популярності. Зауважимо, що вплив ЗМІ у будь-якій формі на працівника правоохоронного органу з метою перешкодити виконанню ним службових обов'язків або добитися прийняття незаконних рішень тягне за собою відповідальність, передбачену ст. 343 КК України [239]. З огляду на результати опитування суддів, проведеного Ю.М. Грошевим (нагадаємо, 20% суддів відповіли, що оцінка ЗМІ вплинула на формування їх внутрішнього переконання. Треба зазначити: не лише ЗМІ своїм "розслідуванням" і своїми публікаціями сприяють розголошенню таємниці досудового слідства, а й окремі співробітники ОВС. Журналіст і ЗМІ у цьому випадку лише подають інформацію, повідомлену співробітником.

Також важливе значення має законодавче врегулювання порядку висвітлення ЗМІ процесу розслідування у кримінальній справі та його результатів до вступу вироку в законну силу, на що звертають увагу працівники слідчих підрозділів. Зокрема пропонується обов'язкове погодження зі слідчим тексту майбутньої публікації, що ґрунтується на матеріалах кримінальної справи, й отримання від нього письмового дозволу на висвітлення певної інформації.

Система забезпечення безпеки злочинного угруповання включає у себе використання корумпованих зв'язків. Загроза, яка виходить не ззовні, а зсередини, має особливо небезпечний характер для процесу розслідування у кримінальній справі. Основне призначення корумпованих співробітників полягає у забезпеченні безпеки існування та діяльності ОЗУ – саме шляхом використання корумпованих співробітників правоохоронних органів досягається найбільший ефект гарантування їх безпеки. Результати дослідження показують: 20% із виявлених організаторів злочинних угруповань мали радників із числа працівників правоохоронних органів [240, с. 147].

З приводу корумпованості працівників правоохоронної сфери В.П. Бахіним і Н.С. Карповим були опитані начальники районних відділів внутрішніх справ, слідчі й оперативні працівники. Наведемо окремі дані проведеного опитування. Так на питання: чи зустрічались з випадками надання неправо-

вно-розшукову діяльність", нормою, яка б конкретно регулювала застосування технічних засобів взагалі і поліграфу –зокрема, при проведенні опитування громадян.

2. Видати наказ МВС України «Про забезпечення впровадження поліграфа в діяльність органів внутрішніх справ» та спільну інструкція МВС, СБУ та Генеральної прокуратури України «Про порядок застосування поліграфа при опитуванні громадян».

3. Доповнити КПК України ст.. 85^3 «Застосування спеціального психофізіологічного обстеження з використанням поліграфа при провадженні досудового слідства», зміст, якої викласти в наступній редакції «Психофізіологічне обстеження з використанням поліграфа може використовуватись при проведенні обшуку, відтворення обстановки та обставин події, допиту та при проведенні інших слідчих дій. Особа, відносно, якої проводиться психофізіологічне обстеження з використанням поліграфа, повинна до початку цієї дії бути проінформована о сутності цього дослідження, і дати письмову згоду. Після цього таке тестування здійснюється поліграфологом (спеціалістом), а розшифрована ним поліграма повинна приєднуватися додатком до протоколу слідчої дії, який підписується всіма учасниками слідчої дії.»

4. Доповнити ст. 128^1 КПК України правом застосування спеціалістом (поліграфологом) спеціального психофізіологічного обстеження з використанням поліграфа.

На завершення слід констатувати, що інформаційне забезпечення слідчої діяльності здійснюється із різних джерел і в різноманітних формах., так з використанням комп'ютерних технологій можуть бути: витребування й прилучення в передбачених законодавством порядку до кримінальної справи інформації, що зберігається в комп'ютерних базах даних (відомості про судимість, про знаходження в розшуку осіб, предметів і т. ін.); одержання безпосередньо або через оператора, інформації, необхідної для розкриття злочинів; виїмка й прилучення до кримінальної справи інформації, що зберігається на магнітних носіях; одержання по електронній пошті документів, засвідчених цифровим підписом, при подальшій передачі документів у натуральному вигляді відповідно до вимог чинного кримінально-процесуального законодавства. Такі заходи потрібні, впершу чергу, з метою оперативності обміну інформацією і прийняття своєчасних рішень.

Перспективним є одержання слідчим з комп'ютерних баз даних, інформації, й використання її при плануванні роботи при розслідуванні злочинів, учинених ОЗУ. Зокрема, заслуговують на увагу пропозиції про використання автоматизованих інформаційних систем, комп'ютеризованих

шенням суду, прийнятим за поданням керівника відповідного оперативного підрозділу або його заступника. Застосування цих заходів проводиться виключно з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншим способом одержати інформацію неможливо. На нашу думку, тут мова йде не про поліграф і ті ситуації, в яких він застосовується. Отже, в Законі України "Про оперативно-розшукову діяльність" відсутній дозвіл на використання поліграфу органами дізнання.

В підзаконних актах органів виконавчої влади України немає чітких вказівок про його використання при розкритті й розслідуванні злочинів. Тому на стадії порушення кримінальної справи органи дізнання мають користуватися нормами частин четвертої та п'ятої статті 97 КПК України і передбаченим чинним законодавством переліком перевірочних дій.

В юридичній літературі висловлені пропозиції про залучення поліграфіста до участі в проведенні допиту. Слідчий в такому випадку обов'язково має здійснити ряд дій, зокрема, запросити адвоката і поліграфіста (як спеціаліста), отримати письмову згоду особи на проведення поліграфічного тестування тощо. Після цього таке тестування здійснюється оператором, а розшифрована ним поліграма повинна приєднуватися додатком до протоколу допиту, який підписується всіма учасниками слідчої дії. Зазначена думка, на наш погляд, має право на існування, однак вона не узгоджується з чинним законодавством України. Спеціаліст дійсно може залучатися до участі в проведенні окремих слідчих дій відповідно до статті 128^1 КПК України. Він зобов'язаний, зокрема, використовувати свої спеціальні знання і навички для сприяння слідчому у виявленні, закріпленні та вилученні доказів; звертати увагу слідчого на обставини, пов'язані з виявленням та закріпленням доказів; давати пояснення з приводу спеціальних питань, які виникають при проведенні слідчої дії. Отже, спеціаліст не проводить самостійного дослідження, а виконує свої функції під керівництвом слідчого у ході проведення слідчої дії. Натомість поліграфіст отримані результати фіксує в окремому висновку, який, як показано вище, до матеріалів кримінальної справи не прилучається.

Виходячи з вищевикладеного, пропонуємо внесення наступних змін до чинного законодавства України стосовно нормативного закріплення проведення спеціального психофізіологічного обстеження з використанням поліграфа при провадженні досудового слідства, а також участі спеціаліста-поліграфолога у слідчих діях:

1. Доповнити статтю 8, що називається "Права підрозділів, які здійснюють оперативно-розшукову діяльність" Закону України "Про операти-

мірної допомоги підозрюваним (обвинуваченим) – 59% опитаних начальників РВВС, 28,7% слідчих, 33,7% оперуповноважених відповіли "так". 33,3% опитаних начальників РВВС, 7,3% слідчих, 15% оперуповноважених вказали, що їм відомі факти прямого співробітництва зі злочинними формуваннями. На питання: чи відомі випадки зриву заходів, намічених проти злочинних груп – 70,7% опитаних начальників РВВС, 39,2% слідчих, 67,5% оперуповноважених відповіли "так" [241, с. 85-86]. Ці заходи здійснюються за допомогою розвідки, контррозвідки, з використанням сучасних технічних засобів [242, с. 44]. Наймогутніші угруповання мають у своєму складі підрозділи розвідки та контррозвідки [243, с.27; 244, с.135; 245, с.149]. І.П. Козаченко зазначає: 32% викритих злочинних угруповань вживали контррозвідувальних заходів [246, с. 144]. Як показують дані досліджень окремих учених, злочинна діяльність характеризується таким елементом як тактика, яка є ознакою професійності [247, с.11]. За даними дослідження, проведеного Н.С. Карповим, 65,7% респондентів указали: тактика злочинців містить у собі методи збору інформації про засоби й методи діяльності правоохоронних органів [248, с.31].

Ми також поділяємо точки зору щодо потреби притягнення до кримінальної відповідальності журналістів за зловживання своїми професійними обов'язками [249, с. 29]. Ряд учених-криміналістів нашої держави, серед яких В.П. Бахін, І.В. Гора, П.В. Цимбал, М.А. Михайлов, відзначають, що закріплені в Конституції України свобода слова і друку не можуть бути безконтрольними без шкоди для громадян. Вони виступають за законодавче впровадження відповідальності за розповсюдження та використання інформації зі злочинною метою [250, с. 324].

У науковій літературі зазначається: "В Україні зафіксовані випадки спроб проникнення в інформаційні системи правоохоронних органів. Прикладом того може послужити спроба вторгнення у базу даних НЦБ Інтерполу України у 1994 р." [251, с.144]. Відомі й інші факти негласного доступу до інформації, що зберігається у комп'ютерах.

Значного поширення набули технічні пристрої, які дозволяють знімати інформацію з каналів зв'язку, прослуховувати розмови у кабінетах, квартирах, автомобілях, на вулиці, по телефону тощо. Як зазначає О.Ф. Долженков, "…на технічне оснащення організованих злочинних формувань затрачується до 30% злочинних прибутків. За кордоном закуповуються першокласні засоби зв'язку, стеження, звукоуловлювальна та звукозаписувальна апаратура, інша новітня техніка, яка потім нелегально привозиться в Україну" [252, с.200]. Новим напрямком у діяльності правоохоронних органів є забезпечення інформаційної безпеки. Задача захисту

комп'ютерних систем від «інформаційної зброї» останнім часом кількістю відомостей про розробку зарубіжними країнами концепцій ведення «інформаційної війни». Сьогодні «інформаційні зброя», що становить собою скоординовану діяльність щодо використання інформації для ведення «бойових дій» у будь-якій сфері у буд-якій сфері чи на реальному полі бою є однією з основних загроз інформаційній безпеці держави.

Загрози інформації здебільшого спрямовані на її негласне отримання, знищення (поновлення) чи внесення певних змін (модифікацію) [253, с.9, 254].

Постановою Кабінету Міністрів України № 1126 від 8 жовтня 1997 р. затверджено Концепцію технічного захисту інформації в Україні, що визначає основи державної політики у сфері захисту інформації інженерно-технічними заходами [255]. Згідно з Указом Президента України "Про заходи щодо посилення контролю за розробленням, виготовленням і реалізацією технічних засобів негласного отримання інформації" № 1346/98 від 14 грудня 1998 р. метою цих заходів є запобігання безконтрольному розповсюдженню та застосуванню спеціальних пристроїв для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації [256].

Указом Президента України № 1229/99 від 27 вересня 1999 р. затверджено Положення про технічний захист інформації в Україні, що визначає правові й організаційні засади технічного захисту важливої для держави, суспільства та особи інформації, охорона якої забезпечується державою відповідно до законодавства [257].

13 березня 2002 р. прийнято постанову Кабінету Міністрів України № 281 "Про деякі питання захисту інформації, охорона якої забезпечується державою" [258]. На даний час у СБУ функціонує Департамент спеціальних і телекомунікаційних систем та захисту інформації. Хоча нормативні акти СБУ потребують включення спеціальних ділянок захисту інформації в складі її підрозділів, органів та установ. Нещодавно такі структури з'явилися і в Департаменті контррозвідувального захисту економіки держави СБУ, завданням яких є захист інформації, що обробляється відомчими автоматизованими системами, від злочинних посягань.

Безпосередньо на збереження таємниці досудового слідства спрямована дія статей 121 КПК і 387 КК України.

Питанням забезпечення інформаційної безпеки органів внутрішніх справ у цілому та збереження таємниці досудового слідства зокрема присвячено і ряд відомчих актів МВС України [259, 260, 261].

Захист секретної інформації при обробці її на засобах ЕОТ забезпечується комплексом організаційно-режимних, технічних, програмних і

нями і реакцією на них зі сторони особи. Встановити такий зв'язок потрібно працівникові органу дізнання чи слідчому після аналізу результатів поліграфічного дослідження. Отримана при цьому інформація є орієнтуючою і сприяє у підготовці слідчих дій з метою перевірки висунутих версій. В реалізації тактичного аспекту застосування контактного поліграфу, таким чином, є істотні запитання.

Сутність етичного аспекту проблеми полягає в тому, щоб уникнути порушення конституційних прав громадян, насамперед – на недоторканість особи. З метою усунення можливих порушень норм статей 19, 22, а також частини третьої статті 28 Конституції України про те, що жодна людина без її вільної згоди не може бути піддана медичним, науковим чи іншим дослідам, розроблений текст письмової заяви про згоду на проведення поліграфічного екзамену. Відмова від такого тестування не може розглядатися як прояв чи ознака винності особи у скоєнні злочину. Існує також ряд умов, при наявності яких відмова розглядається як така, що основана на поважних причинах. Серед них – погане самопочуття, стан пригніченості, наявність в недалекому минулому стресів та хвилювань, неприємності на роботі, в сім'ї тощо. Таким чином, особа дає свою згоду на проведення поліграфічного тестування, користуючись при цьому лише своїм власним бажанням.

Найскладнішим є процесуальний аспект проблеми. Застосування поліграфу в КПК не врегульоване і до процесуальних дій не відноситься. Вбачається, що призначати поліграфічне тестування мають працівники органів дізнання – карного розшуку, державної служби по боротьбі з організованою злочинністю, управління по боротьбі з незаконним обігом наркотиків тощо. Правовою підставою для таких дій мали б бути Закон України "Про оперативно-розшукову діяльність" та відомчі накази й інструкції. Але у статті 2 вказаного Закону, яка іменується "Поняття оперативно-розшукової діяльності", лише згадується про застосування оперативно-технічних засобів. Деяка конкретизація мала б бути у статті 8 цього Закону, що називається "Права підрозділів, які здійснюють оперативно-розшукову діяльність". Однак, по-перше, у цій нормі йдеться уже не про оперативно-технічні, а технічні засоби; по-друге, там відсутня норма, що конкретно регулювала б застосування таких засобів взагалі і поліграфу – зокрема, при проведенні опитування громадян. Щоправда, у пункті 9 статті 8 Закону України "Про оперативно-розшукову діяльність" йдеться про можливість знімати інформацію з каналів зв'язку, застосовувати інші технічні засоби отримання інформації. Однак в подальшому у частині другій статті 8 цього Закону зазначається, що такі дії проводяться за рі-

док отримання інформації за допомогою технічних засобів, на відміну від законодавства РФ, немає чітких вказівок про використання поліграфа в кримінальному судочинстві за ініціативою ОВС чи за замовленням захисника або підозрюваного. Таким чином, міркування О.О. Пунди щодо можливості використання захисником зазначеного технічного засобу є довільними і не основаними на чинному законодавстві України.

Використовуючи як контактний (в західних країнах), так і безконтактний поліграф в Україні при розслідуванні злочинів, при істотній різниці в порядку застосування цих технічних засобів, в обох випадках отримується практично однаковий результат. Його сутність полягає в розпізнаванні емоційної напруги, стану емоційного стресу при приховуванні інформації або неправдивій відповіді допитуваного на поставлені запитання. Висновки щодо фізіологічного стану особи при проведенні її допиту і відповіді на поставлені запитання можливо отримати і завдяки використанню безконтактного поліграфа після проведення судової експертизи.

Проблему можливості використання поліграфу потрібно розглядати в чотирьох аспектах: технічному, тактичному, етичному і процесуальному.

Стосовно першого аспекту, немає сумнівів у тому, що сучасні поліграфи завдяки науково-технічному прогресу значно вдосконалені, серійно випускаються різноманітні моделі комп'ютерного поліграфа. Ці прилади мають незаперечну перевагу щодо найбільш досвідченого, тонкого спостерігача в особі людини. Крім цього, що особливо важливо, застосування поліграфа дає безперервну і системно-цілісну картину одночасної динаміки цілого ряду процесів, що відбуваються в організмі допитуваної людини. Але отримані дані потрібно належним чином проаналізувати і пояснити наявність змін у стані людини. Тому технічний аспект тісно пов'язаний з тактичним. Його сутність полягає в наступних положеннях.

В залежності від ситуації, яка склалася на певний час, при застосуванні поліграфу можуть бути використані різні методи. Головна мета при цьому – виявити наявність у особи "слідів пам'яті", тобто тієї інформації, яку вона в силу різноманітних причин не бажає надати слідчому. Такі дослідження мають діагностичний характер і висновки спеціалістів на сучасному етапі розвитку науки є ймовірними. На основі вивчення змін у фізіологічних показниках особи з великою ймовірності робиться висновок про правдивість отриманої при опитуванні інформації. Однак не виключено, що питання, які задають особі, дійсно її хвилюють. Але вони можуть пов'язуватися не з подією злочину, а, наприклад, з приємними або неприємними спогадами минулих життєвих подій. Тому важливого значення набуває наявність причинного зв'язку між поставленими запитан-

конструкторських заходів, які спрямовані на запобігання випадків та спроб несанкціонованого доступу до секретної інформації, її витоку та втрат. Конкретні заходи та засобів технічного захисту інформації визначається залежно від ступеня секретності інформації, яка обробляється, розміру контрольованої зони, присутності віддалених терміналів, складу та типів засобів ЕОТ, результатів їх спеціального дослідження.

Передаються, пересилаються секретні замовлення (завдання, запити), секретні машинні носії інформації (магнітні носії, друковані машинні документи з секретною інформацією) оператору засобу ЕОТ тільки через РСП (режимні секретні підрозділи) з дотримання вимог Інструкції про заходи забезпечення режиму секретності у системі МВС України. Секретна інформація може передаватися на засоби ЕОТ по каналах зв'язку тільки за умови обладнання цих каналів засекречувальною сертифікованою апаратурою гарантованої стійкості або із застосуванням шифрованого зв'язку.

Розвиток інформаційних та телекомунікаційних технологій, дослідження у природничих науках, пов'язаних з відкриттям нових фізичних та хімічних ефектів, розроблення новітніх способів математичної обробки сигналів стають перспективною теоретичною та технічною базою для розроблення нових видів оперативно-технічних засобів. За результатами опитування оперативних працівників, 67% з яких назвали оперативну техніку засобом, який найбільше впливає на удосконалення тактики та становлення нових методів оперативно-розшукової діяльності [262, с.11]. У сучасному суспільстві рівень вирішення проблем захисту інформації, поряд із прогресом комп'ютерних технологій, став фактором, що визначає швидкість і ефективність впровадження інформаційних технологій в усі сфери життя. Більше того, від якості застосовуваних технологій захисту інформації залежить зараз не тільки збереження у таємниці конфіденційних відомостей, але й взагалі існування конкретних інформаційних і телекомунікаційних сервісів, послуг і додатків.

У цей час, активно розвиваються й впроваджуються криптографічні комп'ютерні технології, спрямовані на забезпечення працездатності таких комплексних і масштабних мережних додатків, як електронний банк (e-banking), електронна торгівля (e-commerce) і електронний бізнес (e-business). Із цілком зрозумілих причин серед цих технологій визначну роль відіграють криптографічні протоколи аутентифікації, розподілу ключів і системи електронного цифрового підпису.

Важливою проблемою є забезпечення ефективного відображення арсеналу існуючих і нових перспективних криптографічних рішень (алгори-

тмів, протоколів, ключових систем) на прикладні програмні продукти, мережних операційних систем і апаратних платформ, на яких базуються згадані вище інформаційні системи й ресурси. У цьому зв'язку, необхідна розробка, удосконалювання й впровадження наступних найважливіших технологій захисту інформації: нових стандартів електронного цифрового підпису; масштабованої системи електронних цифрових сертифікатів з використанням центрів довіри; криптографно захищених корпоративних (віртуальних) комп'ютерних мереж і засобів міжмережевого екранування; засобів антивірусного захисту й засобів захисту від несанкціонованого доступу до інформації для неоднорідних розподілених інформаційних систем; моніторингу й аудиту безпеки мережних інформаційних ресурсів; захищених програмно-апаратних засобів для IP-Телефонії; засобів захисту мереж мобільного зв'язку й персональних комунікацій; засобів біометричної ідентифікації й аутентифікації на базі інтелектуальних карт і інших малогабаритних технічних засобів обробки інформації.

Розвиток зазначених перспективних технологій захисту інформації вимагає, з одного боку, застосування нових математичних і криптографічних рішень (наприклад, криптоалгоритмів на основі еліптичних кривих, методів квантової криптографії, фрактальних алгоритмів стиску даних), а, з іншого боку, істотно залежить від прогресу в рівні розвитку мікропроцесорних, алгоритмічних, програмістських і інших суміжних технічних рішень. Сконцентрувати інформаційний масив даних про об'єкти пошуку, здійснюваних у процесі ОРД, дозволяють банки даних управлінь інформаційних технологій різних рівнів. Для обміну інформацією з інформаційними банками даних повинна бути надана можливість використання виділеної мережі передачі даних.

Перспективними системами захисту інформації є, також, впровадження біометричних технологій ідентифікації; мікрочипи радіочастотної ідентифікації (RFID), технології спостереження і обробки бездротових сигналів, нанотехнології й вивчення генома людини та інші [263].

Одна з найважливіших проблем, пов'язаних з Інтернет, полягає в тому, щоб забезпечити конфіденційність користувачів, тобто запобігти прихованому збиранню даних досудового слідства та персональних даних. Інтернет за своєю суттю не передбачає забезпечення анонімності. Навпаки, сім'я комунікаційних протоколів TCP/IP базується на тому, що кожен підключений до Інтернет комп'ютер має постійний або тимчасовий ідентифікатор - IP-адресу, яка дає змогу відправляти і приймати інформацію. У разі звернення до будь-якого Web-сайту IP-адреса комп'ютера, з якого робиться запит, обов'язково заноситься до лог-файлу - спеціального текс-

використанням сучасних комп'ютерних технологій.

Вирішення вказаних питань можливе лише за умови використання знань відповідних спеціалістів у формі судових експертиз.

Останнім часом про такий безконтактний поліграф згадують досить рідко. По-перше, дослідження на ньому практично не проводяться з об'єктивних причин; по-друге, в літературі висловлена інша думка щодо безконтактного поліграфу. П.І. Гуляєв і І.Є. Биховський у своїх роботах показали можливість реєстрації змін фізіологічних характеристик організму людини на відстані на основі вимірів змін слабких електромагнітних полів, які існують у просторі навколо людини, за допомогою спеціальних датчиків. Таким чином, стала можливою одночасна реєстрація електрокардіограми, сейсмокардіограми, пневмограми, фонограми та інших параметрів діяльності організму [412, с. 107-108]. Про такий різновид поліграфа відомо вузькому колу спеціалістів-криміналістів, широкого поширення його застосування також не набуло.

По-друге, це дослідження реакції мозку людини на поставлені запитання за допомогою спеціальних датчиків, які прикріплюються до тіла і реагують на зміни внутрішнього стану людини (хвилювання, знервованість, збентеженість тощо). Використання з указаною метою технічних засобів контактного характеру поширено в західних (США, Канада, Польща, Чехія) і східних країнах (Індія, Китай, Південна Корея, Японія), а також в РФ.

В обох випадках технічні засоби іменуються однаково – поліграф. Тому з метою недопущення їх суміщення доцільно постійно вживати відповідні прикметники – контактний і безконтактний. У першому випадку при застосуванні контактного поліграфа за допомогою датчиків безпосередньо досліджується сама особа і її функціональний стан. Указані дослідження як на поліграфі контактному, так і безконтактному, мають виражений діагностичний характер.

У спеціальній літературі висловлено думку щодо принципової можливості використання захисником у кримінальному судочинстві таких діагностичних засобів. Їх застосування, як зазначає О.О. Пунда, вже знаходить своє місце в процесі реалізації оперативно-розшукової діяльності. Тобто цей автор уважає, що таке дослідження за допомогою тестів можливе або за клопотанням самого підозрюваного або захисника за згодою підозрюваного вони можуть використовуватись, як непроцесуальні засоби одержання інформації про причетність певної особи до розслідуваного злочину [413, с. 383-384]. Ні в наказі МВС України №743-2001 року, ні в інших інструкціях, положеннях чи настановах, які регламентують поря-

чать зміст одних і тих же проявів емоційної напруги допитуваної особи. Для уникнення такої суб'єктивності й отримання об'єктивної можливості виявлення і фіксації вербальної інформації в даний час пропонуються два шляхи, пов'язані з використанням приладів.

По-перше, це опосередковане дослідження таких біологічних властивостей людини, як мова та голос. Такі дослідження знаходяться у повній відповідності з чинними кримінально-процесуальними нормами. Адже статті 851, 852 КПК України дозволяють застосовувати звуко- і відеозапис при проведенні слідчих дій, а ст. 128^1 КПК України передбачає можливість запрошення спеціаліста для участі у проведенні слідчої дії, в тому числі експерта-криміналіста чи іншого фахівця для надання допомоги в якісній фіксації ходу та результатів слідчої дії за допомогою вказаних додаткових засобів [411, с. 70].

Усне мовлення допитуваної особи, записана на звукозаписуючий пристрій, може досліджуватися експертами за допомогою спеціальних приладів – спектрографів, сонографів. Цей напрям пов'язаний з використанням технічних засобів, однак які-небудь датчики, що прикріплюються до тіла людини, не застосовуються. На сучасному етапі за усним мовленням, може бути встановлена емоційна напруженість в мовних сигналах, при відповіді на певні питання, що може говорити про причетність особи до визначених подій або про її поінформованість про факти й обставини, які мають значення для встановлення істини по справі. Усне мовлення являє собою упорядковану систему акустичних сигналів, розгорнутих у часі й сприйманих як звуковий образ, що має семантичне й емоційне навантаження. Такі дослідження стали доступнішими і достовірнішими завдяки використанню даних фонетики і фонології, що знайшли своє втілення в методиці судово-фонетичної експертизи, розробленої українськими вченими-криміналістами П.Ю. Тимошенком, Ю.Ф. Жаріковим і М.В. Салтевським, ще на початку 90-х років.

Зараз продовжуються наукові дослідження в напрямку удосконалення даної методики такими вченими, як Біговим Д.Д., Грабовським В.Д., Носенко Є.Л., Карповим О.М., Чугай А.А., О.М. Кравчуком, Жаріковим Ю.Ф., Кучеренко В.А., Струк І.А. та іншими. Наприклад, з метою використання для визначення емоційного стану людини в криміналістичних цілях Д.Д. Біговим досліджено параметри усного мовлення та проаналізовано можливість діагностики змінювання емоційного стану людини за відповідними зсувами на психічному рівні, які відображаються на її усному мовленні. Запропоновано систему діагностики емоційного стану людини, побудовану на аналізі акустичних характеристик усного мовлення із

тового файлу протоколу роботи серверу, на якому розміщено цей сайт, - звідки його легко можна вибрати.

Ще одна проблема щодо забезпечення конфіденційності пов'язана з «cookies» (мета цих файлів, ідентифікація користувача і персональне настроювання Web-сторінок. Такі файли, одержані від певного Web-сервера, записуються на комп'ютер користувача і надсилаються цьому серверові під час подальших запитів інформації з нього. При цьому сервер точно знає, «хто до нього прийшов і що йому треба показати) — невеликими файлами зі службовою інформацією, які на комп'ютер користувача без його дозволу може записати будь-який сервер Інтернет. Файли cookies не дають змоги встановити особу користувача, але під час їх використання можна відстежити його поведінку в Інтернет. Браузери мають опції відмови від одержання файлів cookies, але це унеможливлює роботу з деякими сайтами. Аналіз слідчої практики показав, що процесуальні документи досудового слідства, в переважній більшості, були підготовлені за комп'ютерами підключеними до Інтернету та не обладнані необхідними програмними продуктами з захисту інформації.

З другого боку оперативні підрозділи в ході проведення тактичної комбінації можуть встановлювати контроль над чужим комп'ютером і знаходитись в Інтернеті від його імені. Цим незаконним способом користуються хакери під час атак у мережі, використовуючи локальну мережу або прокси-сервер чи передаються через множину серверів, якими керують провайдери-партнери, приховуючи маршрути передавання з шифруванням пакетів даних. Але цим принципом можна скористатися й цілком легально. Досвід поліції світу дозволяє зробити висновок про необхідність розроблення організаційно-тактичних основ огляду або вилучення інформації з віддаленого комп'ютера, який є заходом щодо безпосереднього негласного проникнення у закриту комп'ютерну мережу або окремій віддалений комп'ютер, ознайомлення та копіювання інформації, що представляє оперативний інтерес за конкретно оперативно-розшуковою справою, відносно конкретної особи або конкретних осіб, за конкретний період часу або її перетворення чи знищення, якщо ця інформація була отримана несанкціоновано, з обмеженим доступом користування. Ми поділяємо точку зору Хараберюша І.Ф., який пропонує ввести до переліку методів ОРД оперативно-технічний метод «отримання інформації за допомогою засобів спеціальної техніки» та оперативно-технічні заходи «моніторинг телекомунікаційних мереж» і «огляд або вилучення інформації з віддаленого комп'ютера»[264, с.19].

Своєрідність тактики й використання технічних засобів виявлення й ви-

лучення інформації, що зберігається в оперативній пам'яті комп'ютера або на фізичних носіях, дозволяє, також, виділити новий різновид обшуку - обшук засобів комп'ютерної техніки. Докладно техніка такого обшуку викладена в працях В.В. Крилова, І.А Ніколайчука, В.Б. Вехова й ін. вчених.

Забезпечення конфіденційності даних досудового слідства повинна здійснюється з урахуванням всіх можливих напрямків, це стосується не тільки заборони передачі й розголошення цих відомостей, а й забезпечення інформаційної безпеки носіїв цієї інформації, які мають доступ в мережу Інтернет, це також стосується і питань забезпечення захисту в мережі, конспірації фактів негласного доступу, щодо отримання чи спотворення інформації.

2.3 Тактика використання повідомлень засобів масової інформації при розслідуванні злочинів, учинених ОЗУ

Сучасний стан криміналістичної тактики характеризується необхідністю підвищення її ефективності і потребує подальшого вдосконалювання. Тенденції розвитку теорії криміналістичної тактики пов'язані з можливістю розроблення тактичних прийомів із використанням інформаційних технологій, визначенням аспектів їх практичного використання в судово-слідчій практиці.

Багато вчених серед специфічних завдань криміналістики відзначають розробку нових і вдосконалення існуючих тактичних прийомів, тактичних операцій і рекомендацій, направлених на їх ефективне використання в слідчій практиці [265, с. 228; 266, с. 22; 267, с. 15]. Окремі проблеми тактики стали розглядатися й у спеціальних наукових виданнях системи МВС. З'явилися відповідні теоретичні напрями наукових досліджень – проблем оперативно-розшукової тактики. Так, наприклад, А.Г. Лєкар досліджував тактику попередження злочинів органами охорони громадського порядку; [268] В.А. Лукашев – тактику розшуку злочинців [269].

С.С. Овчинський – тактику інформаційного забезпечення оперативно-розшукової діяльності; В.Г. Бобков, Е.О. Дідоренко – тактику оперативної розробки; [270] І.П. Козаченко – тактику оперативно-розшукової профілактики злочинів, застосування засобів і методів оперативно-розшукової діяльності [271] І.І. Басецький – тактику агентурної роботи [272].

Тактичний прийом є основним елементом криміналістичної тактики. У юридичній літературі визначення поняття тактичного прийому дотепер є

Склад та порядок розміщення обов'язкових реквізитів електронних документів визначається законодавством. Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму. Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною.

Окрім цього визначення електронного документа як інформації в електронній формі не вказує на специфічність форми: будь-який документ, у тому числі й на паперовому носії, пов'язаний з електронами або заснований на їх властивостях (виходячи з її молекулярного складу). При цьому для кваліфікації «електронної» інформації як документа, матеріальний носій не має якого-небудь істотного значення.

Схожа ситуація існує й щодо визначень «інформація», «відомості» і «комп'ютерна інформація» [408]. Відзначені питання заслуговують самостійного дослідження. Отже, вірніше буде використання для позначення матеріалів, здатних містити відомості, що мають значення при встановленні обставин, що підлягають доказуванню, термін «носій даних». Відповідно до офіційного визначення «носій» - це фізичне тіло або середовище, використовувані для запису й зберігання інформації в системах автоматизованої обробки інформації. Під це визначення підпадають тільки ті носії даних, на які інформація записується способом зміни їх форми, магнітних, оптичних або інших властивостей. Перелічити ряд властивостей, при зміні яких відбувається відбиття сигналів у вигляді інформації на носії, досить важко, насамперед, через появу нових технологій і тих, які ще будуть з'являтися (квантові й нейрокомп'ютери). Таким чином, під терміном носій даних слід розуміти носій як фізичну основу, адекватної критеріям довговічності й безпеки, призначеної для відображення на ній інформації.

У ході розслідування злочинів іноді виникає необхідність виявлення у свідка, потерпілого, підозрюваного або обвинуваченого інформації, яку вони з різних причин не вважають за необхідне повідомити слідчому. Для зміни такої негативної позиції допитуваного в деяких випадках корисне стимулювання його позитивних особистих якостей, які основані на прийомах логічного і емоційного впливу, часта постановка найменш очікуваних питань з вимаганням негайних відповідей на них тощо. Ці та інші тактичні прийоми досить повно описані в спеціальній літературі [409, с. 322–325; 410, с. 48–54]. Однак органолептичні засоби пізнання суб'єктивні, сприйняття отриманої під час спілкування інформації залежить від особливостей організму, загальної сенсорної культури, наявних спеціальних знань. Цілком природно, що два слідчі неоднаково розтлума-

особливого відношення до них при їх відтворенні та зберіганні.

Пропонується доповнити КПК процедурою зберігання таких доказів як інформації, представленої в електронному виді, і передбачити, що інші носії прилучаються до справи, які отримані із застосуванням інформаційних технологій, що містять інформацію, яку можна аутентифікувати та (або) ідентифікувати.

Інформація, що міститься в електронному вигляді може використовуватися як доказ, але сумісно з носієм, в якому вона міститься. Вказаний носій виступає речовим доказом.

Таким чином, при розслідуванні злочинів у сфері комп'ютерної інформації можуть бути вилучені докази, що обґрунтовують винність особи, але представлені у вигляді сигналів в аналоговій цифровій формі або іншій формі, що не може бути представлена в доступному для сприйняття виді через відсутність спеціального програмного забезпечення, що може мати вирішальне значення при розслідуванні даних справ. На думку Р.С.Бєлкіна, сигнал є матеріальний носій і засоби передачі інформації, це «зміна, що наступила у зв'язку з подією злочину, сигнал може виступати в предметній формі і у вигляді уявних образів, фактів-відображень» [407]. Причому в КПК відсутня процедура прилучення до матеріалів справи документів, представлених на носіях інформації. Проведений аналіз статей дозволяє дійти висновку про те, що електронно-цифровий вид подання доказів не може бути віднесений до доказів, оскільки немає законодавчого процесуального закріплення такого виду. КПК також містить недогляд, що укладається в тому, що учасникам кримінального судочинства надається право збирати тільки документи, представлені в писемній формі й тільки предмети як докази. При існуючому принципі рівності всіх доказів, ці положення суперечать іншим нормам КПК, що регулюють процес доказування, оскільки не дозволяє збирати і представляти носії й саму інформацію, представлену на них в електронному виді. Це варто виправити шляхом внесення відповідних змін в КПК.

Своєрідність тактики й використання технічних засобів виявлення й вилучення інформації, що зберігається в оперативній пам'яті комп'ютера або на фізичних носіях, дозволяє виділити новий різновид обшуку - обшук засобів комп'ютерної техніки. Докладно техніка такого обшуку викладена в працях В.В. Крилова, І.А Ніколайчука, В.Б. Вехова й ін. вчених.

Відповідно до ст..5 Закону України «Про електронні документи та електронний документообіг» від 22.05.2003 р. Електронний документ - документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.

спірним і викликає неоднозначне розуміння й застосування.

У широкому значенні під тактичним прийомом розуміють найбільш раціональний, найбільш ефективний засіб дії або найбільш раціональну лінію поведінки особи, яка здійснює процесуальні дії [273, с. 4; 274, с. 168]. А.О. Філющенко зазначає, що тактичний прийом є результатом розумової діяльності, змістом якої є оцінка конкретної ситуації, вибір найбільш ефективного способу дії з інших варіантів поведінки [275, с. 6-8].

Не досить чітким до цього часу залишається відмежування тактичного прийому від тактичної рекомендації. Деякі вчені ці поняття не розділяють. Так О.М. Васильєв зазначає, що всякий тактичний прийом розслідування є рекомендація, застосування якої залежить від слідчого, від його оцінки обстановки, що склалася [276, с. 276]. На думку І.П. Герасимова, тактичні рекомендації суттєво не відрізняються від прийому і можуть вважатись тактичними прийомами. Також він уважає, що найчастіше різниця зводиться до того, що рекомендації направлені на підвищення ефективності тактичного прийому, а прийом здебільшого представляє конкретну дію або лінію поведінки [277, с. 229]. І.Є. Биховський вважає тактичними прийомами розроблені криміналістичною наукою рекомендації про способи дії, використання яких з урахуванням конкретної слідчої ситуації і вимог процесуального закону забезпечує найбільш ефективне і швидке виконання окремих слідчих завдань і досягнення загальної мети розкриття злочину [278, с. 282]. В.І. Комісаров вважає, що поняття "тактичний прийом" і "рекомендація" хоч і не тотожні, однак настільки пов'язані, що розділяти їх недоцільно [279, с. 59]. В.Ю. Шепітько розділяє ці поняття таким чином. Тактичний прийом – спосіб здійснення процесуальної дії, направлений на досягнення її конкретної цілі; тактична рекомендація – науково обґрунтована і апробована практикою порада, що стосується вибору і застосування засобів, прийомів і форм поведінки [280, с. 15].

А. Ф. Волобуєв уважає, що поняття «тактичний прийом» і «тактична рекомендація» є різнопорядковими й при їх використанні повинно дотримуватися умови - аспект розгляду слідчої тактики. Поняття «тактичний прийом» відображає насамперед практичну спрямованість слідчої тактики. оскільки це спосіб цілеспрямованої практичної діяльності при розслідуванні злочинів. Поняття ж «тактичної рекомендації» як і «криміналістичної рекомендації» взагалі належить до наукознавчої сфери криміналістики [52, с. 30.31].

Ми цілком згодні з таким визначенням тактичної рекомендації і вважаємо, що під тактичним прийомом слід розуміти найбільш раціональний і ефективний спосіб дії в даних умовах. Ці поняття не слід ототожнювати

оскільки вони мають різну етимологічну та змістовну сутність і направленість.

Розробка тактики слідчих дій передбачає необхідність розгляду їхнього взаємозв'язку, визначення найбільш доцільних їх комплексів. У процесі розслідування злочинів слідчі дії використовуються не ізольовано, а у зв'язку з іншими діями і заходами для вирішення певного завдання, в необхідній послідовності їхньої реалізації.

З початку 70-х років і до теперішнього часу триває створення нової конкретної криміналістичної теорії тактичних операцій. Цій науковій проблемі присвятили свої праці А.В. Дулов [281], Л.Я. Драпкін [282], О.С. Подшибякін [283], В.О. Образцов, А.А. Протасевич [284], П.Д. Біленчук, В.І. Перкін [285], С.І. Цвєтков [286], В.І. Шиканов [287], С.Ф. Здоровко [288] та інші науковці.

Термін "операція" походить від латинського operatio – дія й означає діяльність по виконанню якого-небудь завдання. Під тактичною операцією в криміналістиці розуміють комплекс слідчих дій, оперативно-розшукових, превентивних, організаційно-технічних та інших дій, об'єднаних для вирішення окремого завдання розслідування і проводяться по єдиному для них плану [289, с. 431]. У 1979 р. Р.С. Бєлкін запропонував іншу назву – "тактична комбінація". На його думку існує два види тактичних комбінацій: прості – комбінації тактичних прийомів і складні – комбінації дій та заходів [290, с. 88]. Отже, суттєвих відмінностей між складними тактичними комбінаціями, зазначені Р.С. Бєлкіним, та тактичними операціями немає. Хоча окремі вчені розділяють ці поняття (А.В. Дулов [291, с. 45], В.І. Шиканов [292, с. 44], О.О. Михальчук [293, с. 59]).

Постановка проблеми тактичних операцій у криміналістиці належить до початку 70-х рр. В одній із своїх робіт А. В. Дулов вперше звертається до проблеми розробки тактичних операцій як систем слідчих дій у розслідуванні злочинів [294, с. 23-26]. У подальшому проблеми теорії тактичних операцій досліджувалися в роботах О.Я.Баєва, Р.С.Бєлкіна, Л.Я.Драпкіна, В.О.Князєва, В.О. Коновалової, В.О.Образцова, В.І.Шиканова та інших учених [295, с. 215-219; 296, с. 202-243; 297, с. 219; 298, с. 4; 299; 300; 301, с. 282-284; 302, с. 16-19; 303, с. 54-60; 304, с. 86-93; 305; 306; 307, с. 193-195].

Сьогодні проблема тактичних операцій у криміналістиці є недостатньо розробленою і дискусійною. Щодо практичної діяльності, на нашу думку, О. Ю. Булулуков справедливо зазначає, що в практичній діяльності органів, які здійснюють боротьбу зі злочинністю, тактичні операції проводились і раніше, але через відсутність належної теоретичної розробки і відповідних реко-

ряється задопомогою відкритого ключа;Електронний підпис є обов'язковим реквізитом електронного документа, який використовується для ідентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу.

Накладанням електронного підпису завершується створення електронного документа.

Відносини, пов'язані з використанням електронних цифрових підписів, регулюються законом.

Використання інших видів електронних підписів в електронному документообігу здійснюється суб'єктами електронного документообігу на договірних засадах [406].

Відповідно до статті 83 КПК України (в редакції Закону N 807-VI (807-17) від 25.12.2008 р.) Документи є джерелом доказів, якщо в них викладені або засвідчені обставини, які мають значення для справи. Документами є предмети, на яких за допомогою письмових знаків, звуку, зображення тощо зафіксована певна інформація.

До документів можуть належати матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі електронні), які містять відомості про обставини, встановлені в ході кримінального судочинства органом дізнання, слідчим, прокурором чи судом у порядку, встановленому цим Кодексом.

Документи мають бути досліджені та приєднані до справи постановою особи, яка проводить дізнання, слідчим, прокурором, ухвалою суду і зберігатися весь час при справі.

За клопотанням власника, а також інших осіб, які за законодавством мають право користуватися цими документами, вилучені та приєднані до кримінальної справи документи або їх копії можуть бути надані їм у порядку, встановленому КПК.

У тих випадках, коли документи мають ознаки, зазначені в статті 78 КПК, вони є речовими доказами.

При віднесенні носіїв інформації до інших документів, як письмові докази., наприклад отримані за допомогою факсимільного, електронного або іншого зв'язку, а також документи, підписані ЕЦП, КПК важливе значення має технології їх зберігання. Так у випадку проведення в рамках ОРД оперативно-технічних заходів їх результати можуть бути зафіксовані на матеріальних (фізичних) носіях інформації (фонограмах, відеограмах, кінострічках, фотоплівках, фотознімках, магнітних, лазерних дисках, злітках і т.ін.). Так матеріали відеозапису відтворюються (прослуховуються, переглядаються і т.ін.) відразу ж після вилучення. Але вони потребують

а) повним або неповним номером відповідно до Рекомендацій МСЕ Е.164, Х.121;

б) ідентифікатором вхідного напрямку пучка каналів;

в) ідентифікатором лінії (каналу);

г) ідентифікатором ознаки номера (міжнародний, національний, міжміський, внутрішньо зоновий та місцевий);

д) ідентифікатором напрямку з'єднання (вхідне, вихідне);

е) MSISDN — міжнародним ISDN номером рухомої станції (у тому числі роумінгових);

ж) IMSI — міжнародним ідентифікатором рухомого абонента спостереження;

и) IMEI — міжнародним ідентифікатором (повним або скороченим) обладнання рухомої станції;

к) TMSI — тимчасовим міжнародним ідентифікатором рухомого абонента спостереження;

л) LAC, CELL ID — ідентифікаторами зони розташування;

м) CLASS MARK — ідентифікатором технічних можливостей рухомої станції;

н) ідентифікаційним кодом мережі. [405].

Ще одним прогресивним методом аналізу оперативно-розшукової інформації є застосування комп'ютерних систем візуалізації інформації. Це дозволяє відображати на екрані монітора зв'язки між об'єктами, представляти картини цих зв'язків у різних масштабах, більш наочно структурувати схеми легалізації коштів, здобутих злочинним шляхом і ін. Зазначене дозволяє застосовувати не тільки логічний аналіз ситуації, але й оперувати деякими образами (тобто включати образне мислення слідчого) і, отже, одержати більш ємну інформацію.

Є можливість скоротити строк проходження окремих документів, так застосуванні технології електронного цифрового підпису дозволяє спростити процедуру передачі електронної версії документів, у тому числі висновків експертів, що приведе до скорочення термінів розслідування. Використання інформаційних технологій можливо за допомогою матеріалів, що ілюструють висновок експерта, які додаються до висновку експерта й служать його складовою частиною.

Електронний цифровий підпис - вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіmендацій слідчі і оперативні працівники органів внутрішніх справ здійснювали їх, спираючись лише на власний досвід, досвід своїх колег або на обмежені відомості, що є в криміналістичній літературі [308, с. 166].

Питання про поняття тактичної операції є дискусійним у теорії криміналістики. Так А. В. Дулов указує, що тактична операція є сукупністю слідчих, оперативних, ревізійних та інших дій, які розробляються і виконуються у процесі розслідування за єдиним планом під керівництвом слідчого з метою реалізації такого тактичного завдання, яке не може бути вирішене провадженням у справі окремих слідчих дій [309, с. 44].

Іншою є точка зору Р. С. Бєлкіна. На його думку, сукупність слідчих дій у рамках окремого акта розслідування є тактична комбінація. Автор вважає, що тактична комбінація – це певне сполучення тактичних прийомів або слідчих дій, що переслідують мету вирішення конкретного завдання розслідування й зумовлені цією метою і слідчою ситуацією [310, с. 139, 145]. Р. С. Бєлкін розглядає "слідчі хитрощі" або "психологічні пастки" як різновид тактичних комбінацій. На його думку, потрібний вплив ці прийоми справляють, як правило, не своїм змістом, а часом, місцем, послідовністю застосування. По суті вони являють собою комбінації прийомів, об'єднані однією метою і рамками однієї слідчої дії [311, с. 204].

Оперативна комбінація є складовою оперативно-розшукової тактики, тобто сукупність тактичних заходів, які здійснюються у визначений послідовності за єдиним задумом [312]. Як правильно зазначають Е.О. Дідоренко, М.М. Польською та інші автори, оперативна комбінація – це сукупність дій, що підтверджують легенду і створюють сприятливі умови для здійснення оперативно-розшукових заходів [313].

З урахуванням аналізу сутності такої категорії як тактична комбінація, спробуємо запропонувати таке поняття, - це визнана обставинами справи ефективна сукупність тактичних прийомів або слідчих дій, яка проводиться з метою зміни слідчої ситуації, поведінки чи позиції підозрюваних, обвинувачених та інших осіб і створюють сприятливі умови для виконання конкретного завдання розслідування.

На нашу думку, мають рацію криміналісти, які розглядають тактичну операцію як самостійну категорію криміналістики. Зокрема, А. Є. Михальчук вважає, що категорія тактичної операції ширше, ніж тактична комбінація, і являє собою оптимальне сполучення тактичних прийомів, застосовуваних у процесі провадження окремої слідчої дії, спрямоване на вирішення конкретного проміжного завдання розслідування й зумовлене слідчою ситуацією, що склалася [314, с. 59]. М. П. Яблоков відносить тактичну операцію до основних понятійних категорій криміналістичної так-

тики [315, с. 189-193].

На думку М. В. Салтевського, тактична операція – це засіб діяльності слідчого, що використовується для вирішення тактичних завдань, які виникають при розкритті, розслідуванні і попередженні злочинів [316, с. 79]. При формулюванні поняття тактичної операції становить інтерес акцент автора на її дієвості. Проте вказаних ознак недостатньо для розкриття сутності даного поняття.

Більш ємними визначеннями тактичної операції є ті, що відбивають найбільш істотні ознаки. Тому видаються точнішими визначення поняття тактичної операції як "сполучення однойменних і різнойменних слідчих дій, а іноді й організаційно-технічних заходів, спрямованих на виконання завдання розслідування в даній слідчій ситуації" [317, с. 82], або як "комплекс зумовлених слідчою ситуацією взаємозалежних, скоординованих слідчих дій, оперативно-розшукових та інших заходів, проваджених правомочними посадовими особами під керівництвом слідчого з метою вирішення тактичного завдання як проміжної мети розслідування" [318, с. 67; 319, с. 127-129].

У криміналістичній літературі висловлюється думка, що тактична операція завжди являє собою об'єднання декількох різнорідних за своїм призначенням слідчих і оперативно-розшукових дій, підпорядкованих виконанню поставленої задачі [320, с. 284]. Така позиція є не зовсім чіткою, оскільки тактична операція може об'єднувати також декілька однойменних дій (наприклад, серію допитів або групу обшуків).

У сучасній криміналістичній теорії пропонується термін "спеціальна операція". Спеціальна операція не збігається з тактичною операцією. На думку С. Б. Россинського, ознаками спеціальної операції є: 1) спеціальна операція при провадженні слідчої дії – це не тактичний прийом і не процесуальний вид, а організаційна форма здійснення слідчої дії. Від звичайної форми проведення слідчої дії спеціальна операція відрізняється особливостями організації і планування; 2) спеціальна операція полягає в збиранні і дослідженні багатьох об'єктів, що несуть криміналістично значущу інформацію та розташовані на достатньо широкій території; 3) при проведенні спеціальної операції завжди задіяна велика кількість співробітників: слідчих, оперативних працівників, спеціалістів, співробітників силових підрозділів та інших учасників; 4) проведення спеціальної операції пов'язано з протидією осіб, не зацікавлених у належному здійсненні слідчої дії [321, с. 187].

Таким чином, спеціальна операція – це організаційна форма проведення слідчої дії. Незважаючи на те, що у ній задіяна велика кількість учас-

б) фізичне місцезнаходження (номер у мережі фіксованого телефонного зв'язку, доступ до якої здійснюються із застосуванням стаціонарного кінцевого обладнання тощо);

в) логічне місцезнаходження (IP адреси для мереж передачі даних, єдиний UPT номер для універсального персонального зв'язку тощо).

Визначення місцезнаходження проводиться як при повному, так і при статистичному режимах спостереження, як при здійснені сеансу зв'язку, надання послуги, так і незалежно від цього.

Визначення географічного, фізичного або логічного місцезнаходження абонента спостереження має здійснюватися ЗУСП у випадках:

а) успішної або неуспішної спроби встановлення сеансу зв'язку для вихідного виклику від абонента спостереження, та успішної спроби встановлення сеансу зв'язку для вхідного виклику до абонента спостереження;

б) обміну службовими повідомленнями між терміналом та обладнанням телекомунікаційної мережі;

г) надання послуги, що асоціюється з місцезнаходженням абонента спостереження;

д) передачі спеціального запиту від ЗУСП щодо визначення місцезнаходження абонента спостереження.

Визначення місцезнаходження проводиться як при повному, так і при статистичному режимах спостереження, як при здійснені сеансу зв'язку, надання послуги, так і незалежно від цього.

Визначення географічного, фізичного або логічного місцезнаходження абонента спостереження має здійснюватися ЗУСП у випадках:

а) успішної або неуспішної спроби встановлення сеансу зв'язку для вихідного виклику від абонента спостереження, та успішної спроби встановлення сеансу зв'язку для вхідного виклику до абонента спостереження;

б) обміну службовими повідомленнями між терміналом та обладнанням телекомунікаційної мережі;

в) надання послуги, що асоціюється з місцезнаходженням абонента спостереження;

г) передачі спеціального запиту від ЗУСП щодо визначення місцезнаходження абонента спостереження.

Технологія комутації каналів використовується в мережах фіксованого і рухомого зв'язку та дозволяє передавання: мовної інформації; тональної інформації; інформації даних;- факсимільних повідомлень; коротких повідомлень (SMS (ПКП)); мультимедійних повідомлень (MMS (ПММП)).

Кожний з об'єктів перехоплення має бути описаний однією або сукупністю із наступних ознак:

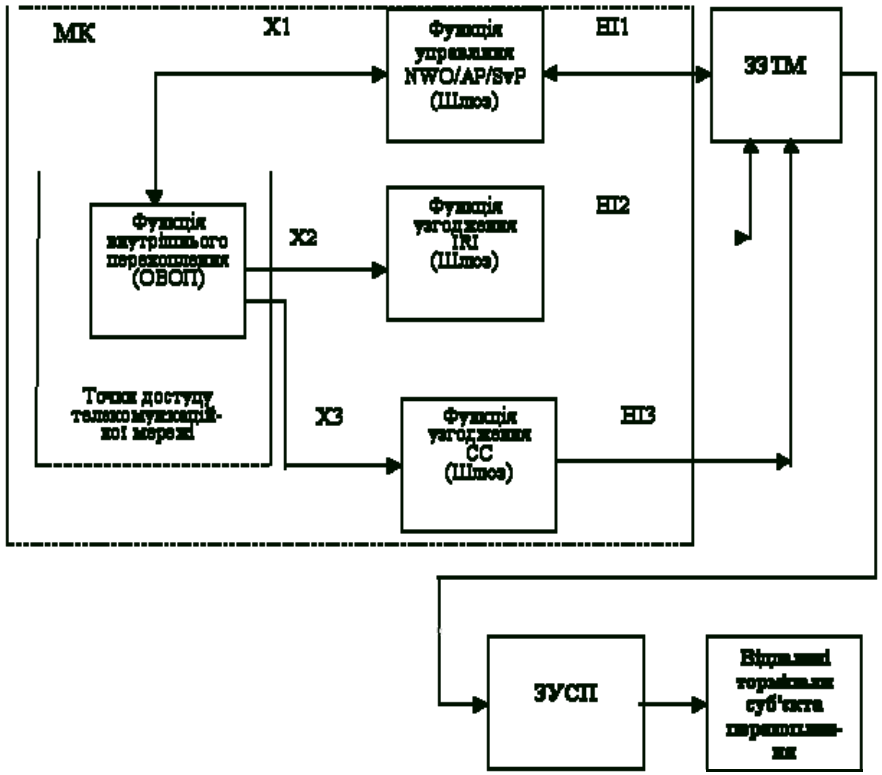

Схема функціонування інтерфейсів

Крім того, технічні властивості телекомунікаційних мереж надають оперативним працівникам додаткові оперативні можливості щодо створення закладних пристроїв на базі мобільних терміналів, застосування мереж стільникового зв'язку для передачі оперативної інформації, а також відстеження маршруту переміщення певних об'єктів із використанням мереж стільникового зв'язку та GPS-технологій.

Визначення місцезнаходження абонента спостереження застосовується у телекомунікаційних мережах (підсистемах мереж), в яких абонент спостереження може здійснювати переміщення.

Залежно від типу телекомунікаційної мережі визначення місцезнаходження термінала абонента спостереження поділяється на:

а) географічне місцезнаходження (ідентифікатори країни, міста або оператора телекомунікацій, зони приймання для мереж рухомого зв'язку тощо);

ників і вона має високий рівень організації і забезпечення, спеціальна операція обмежується однією слідчою дією.

У криміналістичній літературі досить часто використовуються різноманітні терміни, що позначають поняття тактичної операції. Іноді її іменують системою слідчих дій, або тактичним (криміналістичним) комплексом, або криміналістичною операцією. Така термінологічна нечіткість є не випадковою, вона пов'язана з етапом становлення категорії, з можливістю надання певного акценту сукупності тих чи інших дій або заходів.

Сьогодні в криміналістиці виникає питання про місце тактичної операції в її структурі. Ідеться про те, якою категорією є тактична операція – категорією криміналістичної тактики або категорією методики розслідування окремих видів злочинів. Тут необхідно виходити з загальних принципів співвідношення криміналістичної тактики і методики. Тому видається непереконливою точка зору Г. А. Матусовського [322] про віднесення тактичної операції до категорій криміналістичної методики, навіть якщо назвати її криміналістичною операцією [323, с. 177-179; 324, с. 149-156] Необхідно виходити з того, що положення криміналістичної тактики реалізуються в житті, на практиці тільки через криміналістичну методику, набуваючи тих специфічних особливостей, що відбивають їх пристосування до умов і завдань боротьби з конкретним видом злочинів [325, с. 295].

Таким чином, тактична операція являє собою категорію криміналістичної тактики. Вона може бути визначена таким чином: тактична операція – це система процесуальних і непроцесуальних дій і заходів (слідчих і оперативно-розшукових, організаційних), тактичних прийомів, комбінацій, яка зумовлена ситуаційною необхідністю взаємодії посадових осіб різних служб правоохоронних органів і спрямована на виконання проміжного завдання розслідування.

Однією з окремих завдань криміналістики є постійне відслідковування за новітніми досягненнями наукових дисциплін різних галузей знань. Завдяки їм збільшується та вдосконалюється науковий апарат розслідування. Ряд учених (І.П. Герасимов, М.О. Селіванов [326, с. 9], М.П. Яблоков [327], Л.Я. Драпкін [328, с. 27] та інші) наголошує, що криміналістика покликана використовувати й пристосовувати для потреб розслідування злочинів досягнення сучасних природничих, технічних і суспільних наук.

Р.С. Бєлкін відмічає, що загальнонаукові тенденції диференціації та інтеграції наукового знання проявляються в криміналістиці з моменту її зародження як науки [329, с. 34]. Новому баченню стосовно існуючих, а також створенню нових тактико-криміналістичних засобів протидії злочинності можуть допомогти й досягнення наукових дисциплін, які вивча-

ють комп'ютерні технології та засоби масової комунікації. До того ж, сучасна слідча діяльність потребує залучення й використання можливостей ЗМІ у процесі розслідування злочинів. Це викликано не лише потребою розвитку демократичних засад суспільства, але й наступом сучасних форм злочинних проявів. Крім того, В.Є. Коновалова справедливо відмічає, що в наш час криміналістична тактика переростає свій традиційний потенціал, який вимагає не тільки його поновлення, але й побудови систем тактичних прийомів, глибокого дослідження закономірностей, що лежать в основі формування останніх, а також розроблення нових прийомів та їх систем [330, с. 149].

Серед ознак тактичного прийому, що відмежовують його від інших способів дії слідчого В.Ю. Шепітько відмічає його психологічну направленість та ситуаційну зумовленість [331, с. 22]. Слід погодитись з цим твердженням, а тому при розробці тактичних прийомів використання інформаційних технологій та ЗМІ особливої уваги заслуговують досягнення психології, соціальної психології та соціології. Це дозволить слідчому більш диференційовано вибрати важелі впливу на конкретних осіб, усунути амбівалентність (суперечливість) відношення аудиторії до події злочину, віднайти засоби активізації до вчинення потрібних слідчому дій, усунути психологічний бар'єр, що заважає повідомити потрібну слідчому інформацію, створити належний психологічний клімат під час розслідування злочину. Належна увага має також відводитись можливостям рефлексивного управління, завданням якого є переграти супротивника [332, с. 23]. В.Ю. Шепітько вважає, що необхідно більш широко використовувати елементи рефлексивного мислення у процесі побудови окремих тактичних прийомів, їх систем, прогнозування можливостей їх ефективної реалізації [333, с. 39]. Тобто слідчий може використовувати ЗМІ як канал психологічного впливу на учасників кримінального процесу, який здійснюється шляхом передачі значимої для адресата інформації.

До тактичних прийомів використання ЗМІ під час проведення тактичних операцій при розслідуванні злочинів слід віднести інформаційні заходи, пов'язані з методами правомірного психологічного впливу на підозрюваного або обвинуваченого. До типових тактичних прийомів здійснення комп'ютерної розвідки - пошуку та отримання відкритої інформації з комп'ютерних систем та мереж, які не пов'язані з обмеженням прав особи і не потребують дозволу суду на її проведення слід віднести: прийоми, спрямовані на здійснення в комп'ютерній мережі активних заходів щодо здобуття інформації: створення сайтів-пасток для виявлення осіб, причетних до злочинної діяльності, а також моделювання певної ситуації на фо-

— програмне забезпечення (ПЗ) технічних засобів;
— експлуатаційна та програмна документація технічних засобів;
— комплект запасних інструментів та приладів (ЗІП).

Функціональне поєднання цих засобів утворює систему перехоплення телекомунікацій (СПТ).

Мережний комплект МК для здійснення перехоплення телекомунікацій призначені для розпізнавання і відгалуження об'єктів перехоплення, відбору та передачі даних до ЗУСП.

До складу МК має входити обладнання відбору об'єкта перехоплення (ОВОП) та шлюз, що повинні бути установлені в телекомунікаційній мережі.

- Організація взаємодії ОВОП та шлюзу здійснюється по інтерфейсу перехоплення.
- Шлюз має здійснювати взаємодію із ЗУСП по інтерфейсу управління та передачі.
- Для організації доступу до будь-якого об'єкта перехоплення з урахуванням технічних характеристик та особливостей побудови телекомунікаційної мережі можуть використовуватися технологічні можливості мережі при відгалуженні об'єкта перехоплення. Організація доступу передбачає локальну чи розподілену структуру МК на площах оператора телекомунікацій (провайдера послуг).
- МК при здійсненні перехоплення телекомунікацій не повинні погіршувати якість послуг, що їх надає телекомунікаційна мережа.
- Відповідність МК у складі телекомунікаційного обладнання стандартам та цим ЗТВ має бути підтверджена у встановленому законодавством порядку.

загального користування України. Загальні технічні вимоги», який поширюються на технічні засоби для здійснення уповноваженими органами оперативно-розшукових заходів у телекомунікаційних мережах загального користування України в порядку, визначеному законодавством України і є обов'язковими:

— для операторів (провайдерів) телекомунікації;

— для проектувальників та виробників зазначених технічних засобів;

— для проектувальників телекомунікаційних мереж та виробників обладнання телекомунікацій;

— для органів, уповноважених на здійснення оперативно-розшукових заходів;

— для органів сертифікації, що здійснюють діяльність з підтвердження відповідності технічних засобів.

Система перехоплення телекомунікацій (СПТ), яка призначена для оперативного отримання інформації стосовно об'єкта перехоплення і має забезпечувати:

а) можливість доступу до будь-якого об'єкта перехоплення без зниження якості телекомунікаційних послуг, що надаються абонентам спостереження, та/або внесення змін та завад до роботи телекомунікаційної мережі;

б) відповідність функціональних можливостей СПТ рівню розвитку телекомунікаційних технологій, які використовуються у телекомунікаційних мережах;

в) можливість здійснення модернізації СПТ відповідно до розвитку телекомунікаційної мережі при впровадженні нових телекомунікаційних технологій та послуг;

г) можливість ініціювання перехоплення телекомунікацій та незалежного використання отриманої інформації кожним суб'єктом перехоплення;

д) технічні можливості організації контролю використання СПТ за призначенням згідно з законодавством України.

До складу технічних засобів для здійснення уповноваженими органами оперативно-розшукових заходів у телекомунікаційних мережах загального користування України відносяться:

— мережний комплект (МК) для здійснення перехоплення телекомунікацій;

— засоби управління системою перехоплення телекомунікації (сервери, станції, термінали та інші — ЗУСП);

— засоби захищеної телекомунікаційної мережі спеціального призначення (ЗЗТМ);

румі, який відвідує особа, що становить оперативний інтерес, з метою здійснення її зашифрованого оперативного опитування; прийоми, що спрямовані конспірації в ході комп'ютерної розвідки: застосування proxy-серверу; застосування сучасних технологій стільникового зв'язку з мережею Інтернет; легендування належності IP-адреси комп'ютера, що використовується для здійснення розвідки; прийоми подолання протидії пошуку і отримання інформації [334, с. 22-23].

Повідомлення ЗМІ можуть впливати на психічний стан підозрюваного у потрібному слідчому напрямку – визвати стан емоційної напруженості, страху, пригніченості, відчаю, фрустрації тощо, з метою викликати бажання здійснити певні дії, які прогнозуються слідчим в рамках проведення операції при розслідуванні злочину. Типовими тактичними операціями з використанням ЗМІ повинні бути такі: під умовною назвою «свідок», «підозрюваний».

Тактична операція «свідок» має на меті за допомогою ЗМІ активізації вольових якостей громадян, які з тих чи інших причин уникають можливості повідомити слідчому відому їм інформацію, якою вони володіють, і можуть сприяти розкриттю злочину. Тактична операція «підозрюваний» з використанням ЗМІ проводиться для впливу на суб'єкта злочину з метою активізації його діяльності, яка може призвести до здійснення помилок, на користь досудового слідства. Розголошення тривожної інформації для особи, яка вчинила злочин, може змінити поведінку цієї особи, здійснити певні вчинки, залишити сліди, речові докази. Серед прикладів активізації діяльності вказаних осіб шляхом розголошення тривожної для них інформації можна привести розслідування ряду тяжких злочинів в АРК у 1999 р. [335].

Різновидом тактичної операції «підозрюваний» може бути операція «полювання за жертвою», коли для встановлення та затримання особи, що вчинила злочин, потрібно поширити інформацію, яка її цікавить, у тому числі у зв'язку з подією злочину. Серед прикладів проведення тактичної операції із застосуванням тактичного прийому по активізації діяльності осіб, що вчинили злочин із використанням можливостей ЗМІ – розслідування двох подібних вбивств у м. Київ. Співробітниками прокуратури та міліції було встановлено, що обидві жертви помістили в рекламній газеті оголошення про продаж шуби з натурального хутра. Для виявлення та затримання осіб, що вчинили ці подібні злочини, правоохоронці помістили в ту ж саму рекламну газету, що й потерпілі, оголошення про продаж шуби. У результаті проведення тактичної операції правоохоронцям вдалося затримати двох осіб, які вибирали жертв із числа осіб, що подавали оголошення про продаж дорогих речей у рекламну газету [336].

З наведених прикладів видно, що в основі тактичної операції по активізації особи, яка вчинила злочин, лежить можливість рефлексивного управління слідчим її поведінкою. Р.С. Бєлкін зазначає, що в криміналістиці рефлексія є базою для передбачення поведінки та дій учасників кримінального процесу, протидіючих розслідуванню, а також основою для розробки та вибору тих чи інших тактичних прийомів, визначення напрямків розшуку осіб та предметів [337, с. 67]. Тактична операція «підозрюваний» не тільки з використанням ЗМІ, а здійснюючи аналітичну роботу з вивчення повідомлень ЗМІ, так правоохоронці можуть реалізовувати тактичні операції по виявленню та затриманню осіб, що скоїли злочини, і до порушення кримінальної справи. Наприклад, у 2002 році в м. Хмельницький працівники міліції, виявивши в рекламній газеті оголошення "Привабливі активні дівчата шукають роботу. Телефонувати цілодобово за номером…", провели ряд оперативно-розшукових заходів із використанням оперативної відеозйомки. У результаті цього були виявлені та затримані троє жінок віком від 17 до 21 року, які набрали групу інших дівчат для надання сексуальних послуг. Щодо них були порушенні кримінальні справи за звідництво для розпусти [338]. Ефективним може бути і такий різновид тактичної операції «підозрюваний» під умовною назвою «імітація», яка ґрунтується на формуванні у підслідного помилкового уявлення про хід розслідування кримінальної справи або дій слідчого. З допомогою повідомлень ЗМІ слідчий створює умови, при яких формування уявлення підслідного здійснюється в потрібному для слідчого напрямку. Прикладом використання тактичної операції "імітація" можна назвати виявлення та затримання правоохоронцями м. Одеси замовника вбивства за 1000 дол. США К. Уборіна в січні 2003 р. Вбивство замовив його конкурент. Він заплатив виконавцю завдаток, однак той замовлення не виконав, а повідомив про це правоохоронців. Ними була спланована тактична операція по затриманню замовника вбивства. Щоб переконати його в тому, що вбивство вже скоєне, злочин було імітовано – по місцевому телебаченню показали розстріляний автомобіль К. Уборіна, який насправді в цей час перебував в обумовленому місці. Повіривши повідомленню ЗМІ, замовник вийшов на контакт із "виконавцем", після чого його було затримано.

Наступним різновидом тактична операції є «Міраж», яка також направлена на формування у особи, яка вчинила злочин, помилкового уявлення про хід розслідування кримінальної справи. Установивши, наприклад, із допомогою оперативно-розшукових заходів, її особу та, передбачаючи, що в разі притягнення її до відповідальності вона може знищити важливі речові докази, слідчий передчасно не розголошує про це. Він навіть може

гій у розслідуванні є застосування апаратно-програмних засобів із використанням сучасних методів кореляційного, факторного й регресного аналізу, методів аналітичного й імітаційного моделювання, методів, що включають подання складних систем і зв'язків, що складаються з окремих елементів з індивідуальними властивостями, зв'язками й станами, що дозволяє отримувати оперативно-розшукову інформацію й прогнозувати розвиток різних ситуацій у злочинних групах і співтовариствах. Використання програмних продуктів для прогнозування розвитку ситуацій у злочинних співтовариствах, які складаються в результаті тих або інших дій правоохоронних органів, відкриває можливість планувати й робити на них цілеспрямовані інформаційно-психологічні впливи, як у ході оперативних заходів, так і в ході слідчих дій і судових розглядів.

Так, моделювання дорожньо-транспортних випадків дозволяє вирішувати багато завдань: відновити границі місця події, визначити лінію зіткнення й положення транспорту щодо перешкоди в момент контакту, відтворити основні фази й елементи механізму дорожньої події [403, с.51].

Ми згодні з Орловим Ю.Ю. [404, с.15] щодо перспективності напрямків розвитку розвідувальної техніки і застосування телекомунікаційних технологій з метою оперативного перехоплення та прослуховування переговорів певного абонента, отримання інформації щодо факту його телефонних розмов, визначення місця його знаходження, а також блокування переговорів абонента задля унеможливлення вчинення злочину.

З урахуванням рекомендацій Резолюції Ради Європи ЕС COM 96/C329/01 „Про законне перехоплення телекомунікацій" і ENFOPOL 55 „Про оперативні потреби правоохоронних органів стосовно телекомунікаційних мереж загального користування та послуг зв'язку" визначає загальні технічні вимоги до технічних засобів для здійснення уповноваженими органами оперативно-розшукових заходів у телекомунікаційних мережах загального користування України. Перехоплення телекомунікації є оперативно-технічним заходом, що здійснюється відповідно до законодавства України суб'єктами перехоплення, який полягає у спостереженні, відборі за визначеними ознаками та фіксації сеансів зв'язку із застосуванням системи перехоплення.

Відповідно до статті 15 Закону України «Про телекомунікації», статті 5 Указу Президента України від 07.11.2005 N 1556 «Про додержання прав людини під час проведення оперативно-технічних заходів», затверджений нормативний документ Наказом Мінтрансзв'язку та СБУ від 11 грудня 2007 року N 1140/882 «Технічні засоби для здійснення уповноваженими органами оперативно-розшукових заходів у телекомунікаційних мережах

чно змінюються, із вказівкою назв вулиць, відстаней до найближчого перехрестя або кінцевої точки маршруту. Система може подавати інші дані, важливі для кожної конкретної служби (склад екіпажу, його озброєння й ін.).

Специфіка використання комп'ютерних технологій у процесі розкриття й розслідування злочинів зумовлена тим, що їх впровадження можливо на будь-якій стадії провадження по кримінальних справах - від одержання інформації і її реєстрації до стадії судового розгляду з використанням систем відеоконференцій, коли його учасники можуть перебувати в різних географічних точках, і вести безпосередній аудіовізуальний діалог з учасниками в залі суду.

Якщо для оперативних заходів неминуче застосування сучасної спеціальної й комп'ютерної техніки, сучасних інформаційних нововведень в галузі фіксації інформації й т.ін., на думку Р.С. Бєлкіна, застосування їх у слідчій роботі досить сумнівне [402].

На наш погляд, залучення інформаційних технологій у процес розслідування кримінальних справ, особливо для звільнення від численної технічної рутинної роботи з текстовими файлами, досить виправдано, а їх застосування в процесі розслідування, при якому комп'ютер підмінює інтелектуально-розумову діяльність слідчого, повинне розвиватися по досить вузьких ділянках такого процесу, наприклад, на деяких методичних, тактичних, організаційних аспектах слідчих дій і процесу розслідування в цілому.

Тому ведення сучасного розслідування кримінальних справ вимагає від слідчого інноваційних підходів, зокрема стає актуальним питання про програмування дій слідчого за допомогою комп'ютерних технологій. Комп'ютерні технології в діяльності слідчого – це сукупність відповідних законодавству й заснованих на застосуванні засобів комп'ютерної техніки прийомів, методів і методик збору, обробки, зберігання й використання інформації, спрямованих на ефективне використання програмного забезпечення при реалізації процесуальних, організаційних і тактичних рішень, збиранні, перевірці й використанні доказів по кримінальній справі.

Завдання вдосконалювання інформаційного забезпечення слідчо-оперативних груп при проведенні слідчих дій вирішуються за допомогою створення мобільного АРМ. Останнє повинне містити у собі портативну ЕОМ із необхідним програмним забезпеченням і периферійним устаткуванням, а також засобу зв'язку й передачі даних.

У наших умовах розвитку інформаційних технологій перспективно використовувати АРМ як ефективного «помічника», процесу розслідування, своєрідного сателіта розумової діяльності слідчого.

Перспективним напрямком у галузі розвитку інформаційних техноло-

не оголошувати серед висунутих версій ту, на яку вказують обставини скоєння злочину. А через ЗМІ повідомляється про безпорадність слідчого про те, що досудове слідство зайшло в глухий кут і не має перспектив. Тим самим в особи, яка його вчинила, створюється помилкове враження про хід розслідування злочину, вона перестає вживати заходів конспірації, що дозволяє слідчому виявити та зібрати докази скоєння нею злочину.

Схожою за змістом є тактична операція "витік інформації". Різниця полягає в тому, що вплив на формування помилкового уявлення особи, яка скоїла злочин про хід розслідування, здійснюється не через оприлюднення в ЗМІ повідомлень слідчого, керівника або інших співробітників органу, який проводить досудове слідство, а під виглядом журналістського розслідування. За змістом цей тактичний прийом близький до прийому "створення умов для інформаційної необізнаності підозрюваного" під час проведення слідчих дій. Таку назву пропонує Л.Я. Драпкін [339, с. 24]. Наприклад, коли є інформація про те, що особа, яка скоїла злочин, володіє знанням про методи роботи правоохоронних органів і може не повірити офіційним повідомленням правоохоронців, слідчий за допомогою працівників ЗМІ може організувати ряд публікацій у газеті під виглядом журналістського розслідування цього злочину. В цій статті від імені журналіста може подаватись добута ним інформація про хід розслідування, а також та, що "стала відома з джерел у правоохоронних органах". Слідчому після виходу таких публікацій слід передбачити можливість контакту особи, яка скоїла злочин, або за її вказівками інших осіб із журналістом.

Продуманий та організований "витік" вигідних для слідства відомостей у ЗМІ М.П. Яблоков називає серед психологічних засобів регулювання складних ситуацій розслідування організованої злочинної діяльності [340, с. 142]. З цією думкою погоджуються В.І. Бояров [341, с. 127], В.П. Бахін, І.В. Гора, П.В. Цимбал [342, с. 301].

Поділяючи думки вчених, акцентуємо на доречність використання можливостей ЗМІ як одного зі способів та методів подолання протидії розслідуванню [343, с. 255; 344, с. 159]. Типовою тактичною операцією з використанням ЗМІ може бути операція з умовною назвою «протидія», направлена на подолання протидії розслідуванню. В умовах конфліктної ситуації досягнення слідчим позитивного результату при проведенні тактичної операції, направленої на попередження можливої протидії розслідуванню, слід очікувати за умов використання: 1) рефлексивного управління; 2) фактора раптовості; 3) непоінформованості протидіючих осіб про наявність доказів, результатах слідчих дій, намірах слідчого; 4) наданої особам, що протидіють розслідуванню, можливості вибору рішення при дефіциті інформації;

5) інертності мислення, стандартності рішення особою, що має намір, або вже вчиняє протидію розслідуванню, завдання, яке виникло внаслідок інформаційного висвітлення події злочину [345, с. 175].

Різновидом тактичної операції «протидія» може бути операція під умовною назвою “дифамація”. Дифамацією (від лат. diffamatio – ганьблення) називається розголошення свідчень (правдивих чи неправдивих), які ганьблять іншу особу [346, с. 520]. К.І. Бєляков пропонує розглядати поняття «дифамація» в межах українського інформаційного права як інформаційний делікт, дію, в основі якої лежить зловживання свободою слова та масової інформації, спрямоване на приниження честі, гідності та ділової репутації особи в очах громадськості, шляхом поширення про неї відомостей, що не відповідають дійсності. Запровадження у науці інформаційного права однозначно визначення поняття «дифамація» дозволяє коректно сформулювати зміст інституту дифамації як сукупність доктринальних положень науки інформаційного права, інформаційно-правових норм і механізмів охоронного характеру, які забезпечують судовий захист честі і гідності та ділової репутації особи від розповсюдження відомостей, що не відповідають дійсності за умовами строгого дотримання конституційного права на свободу слова і масової інформації [347, с. 211]. Використання цього тактичного прийому пов’язане з криміналістичним вивченням особистості підозрюваного (обвинуваченого), інших осіб, здатних чинити протидію розслідуванню. На можливість цілеспрямованого дозованого поміщення в ЗМІ оперативної інформації з метою дискредитації лідерів злочинного світу та їх заступників із числа чиновників владних структур указує С.С. Овчинський [348, с. 328]. Інший російський учений В. Васильєв, даючи оцінку висвітлення діяльності терористів у ЗМІ, зазначає про необхідність додавати до виступів терористів по телебаченню коментар осіб, “знайомих” із терористами з повідомленням інформації, що викликає фізіологічну огиду до терористів, про деякі подробиці з їх інтимного життя [349, с. 592]. Для подолання протидії розслідуванню злочину допустимим є розголошення і поширення правдивих відомостей, що можуть дискредитувати особу, яка намагається протидіяти слідчому в проведенні досудового слідства, а також прізвища та посаду особи, яка намагається втрутитись у процес досудового слідства.

Особливої уваги з приводу дотримання багатьох видів критеріїв допустимості вимагає планування та проведення тактичних операцій по встановленню та затриманню осіб, підозрюваних у вчиненні різних злочинів. Сучасний рівень доступності розміщення повідомлень у ЗМІ надає злочинцям нові можливості для вчинення суспільно небезпечних дій. А це, у

даних підвідомчої території; сервер оперативної бази даних; модуль оперативного керування ситуацією на підвідомчій території з АРМ оперативного чергового та АРМ збирання інформації та обліку конкретних подій; модуль розв’язування аналітичних задач та упорядкування звітів.

До складу функціональних модулів можуть входити підмодулі: картографічної інформації (бази додаткових даних про територію); доступу до спеціальної інформації (органів МВС, СБУ, податкової міліції, митниці, Міністерства надзвичайних ситуацій тощо) баз даних території (прикордонні райони, морські об’єкти тощо); відстеження і зв’язку з мобільними об’єктами; прогнозування і моделювання.

Під час роботи з ГІС з бази даних керування територією інформація надходить до модуля оперативної бази даних, звідки передається до функціональних модулів. У модулі оперативного керування територією відбувається координатна прив’язка подій до геокодованої картографічної електронної основи. У результаті на екрані АРМ оперативного чергового на електронній карті автоматично з’являється умовне позначення події. Далі залежно від виду події (рухливі — викрадення або статичні — пограбування, пожежа тощо) починає працювати АРМ вирішення оперативних задач: визначення особливостей місця події; визначення найкоротшого шляху для патрульної мобільної групи; визначення зон перехоплення; виділення в зоні спостереження особливих об’єктів (кількість жителів будинку, селища, наявність піднаглядних осіб тощо); оперативне формування протоколу події і проектів наказів оперативного чергового для керування силами і засобами.

Особливу увагу необхідно приділити переходу до наукомістких космічних технологій і новітнім комп’ютерним геоінформаційним системам у процесі керування рухливими об’єктами оперативних служб. Наприклад, системи автоматичного визначення місця розташування транспортних засобів з метою запобігання їх викраденню; пости оснащуються апаратурою, що дозволяє примусово зупинити викрадений автомобіль щойно він з’явиться в зоні радіовидимості. Недоліком даної системи є те, що викрадач автомототранспорту може об’їжджати такі пости.

У системах моніторингу для спостереження за службовими транспортними засобами органів внутрішніх справ на них установлюється приймач. Потім через УКВ-радіоканал, стільникову мережу або глобальну систему супутникового зв’язку координати передаються на диспетчерський пункт тієї чи іншої служби. На диспетчерському пункті технологія переводить інформацію про координати, швидкість і її напрямок в «картинку» на електронній карті міста. На ній з’являються текстові повідомлення, що динамі-

томатичному режимі, так і з пульта термінала чергової частини оператором; наявність у комплексі розширеної бази даних із можливістю звертання до власників інформаційних послуг для оперативного встановлення координат абонента стільникового зв'язку або стаціонарного таксофону; використання функції розширеного пошуку й швидкого пошуку географічних координат абонента; застосування елементів космічної (супутникової) навігації для керування службовими транспортними засобами й установлення координат місць злочинів.

Виконання завдання підвищення оперативності дій слідчо-оперативних груп вимагає автоматизованої обробки географічно прив'язаної інформації, зокрема, географічних інформаційних систем (ГІС). ГІС ОВС України розробляються Інститутом передових технологій разом з УОІ УМВС на основі програмного продукту американського Інституту спостереження за навколишнім середовищем (Environmental Systems Research Institute, ESRI, http://www. esri.com/) ArcView.

У системах використовуються цифрові бази та електронні карти, розроблені в Укргеодезкартографії. Можливі актуалізація і спостереження за картографічною базою даних із використанням космічних знімків високого дозволу (2 – 3 м). Доречі, досить цікаві перспективи відкриває нова інформаційна технологія, іменована дистанційним зондуванням Землі. Відповідно до Конвенції про передачу й використання дистанційного зондування Землі з космосу, воно здійснюється в різних діапазонах електромагнітних хвиль і сприяє визначенню місцезнаходження, опису характеру й змін не тільки природних, але й антропогенних об'єктів. Ця дистанційна апаратура, розташовувана на різних літальних устроях: літаках, космічних супутниках, уже досить активно використовується в розкритті й розслідуванні злочинів, пов'язаних з незаконним оборотом наркотиків [400]. Комплекс дистанційного зондування Землі складається із системи технічно взаємозалежного й постійного інформаційного обміну, що перебувають у режимі, сегментів космічного й наземного базування. Об'єкт ідентифікації характеризується тим, що він являє собою цифровий відбиток досліджуваної проекції як віртуальна математична позиційна модель. У практиці вже мали місце випадки використання таких фотознімків як докази, що фігурували в суді по справах про знищення й ушкодження лісів, незаконному культивуванні наркомістких рослин, вбивствах, незаконному видобутку й контрабанді тварин і рослин, викраденнях автотранспорту й ін. Карти електронних знімків забезпечують достатню точність відображення характерних ознак об'єкта [401].

До складу ГІС ОВС України входять такі функціональні модулі: бази

свою чергу, вимагає від правоохоронних органів адекватних заходів реагування. Відмітимо досвід діяльності правоохоронців інших країн. Наприклад, у США агенти ФБР активно проводять операцій щодо виявлення через мережу Інтернет осіб, схильних до вчинення сексуальних злочинів, у тому числі щодо неповнолітніх. Протягом восьми років, починаючи з 1995 р., ФБР було здійснено близько двох тисяч арештів таких осіб у рамках операції "Невинні особи". Адвокати затриманих, вважаючи такі методи роботи ФБР незаконними, подавали апеляції. Тому у деяких штатах судові власті, аби запобігти розголошенню конфіденційної інформації про приватне життя підозрюваних, заборонили публікувати в Інтернеті адреси й імена сексуальних злочинців. Інтернет-пастки використовуються у діяльності правоохоронних органів й інших країн. При цьому нерідко проводяться такі операції правоохоронцями різних держав. Так у 2001 р. працівниками російської міліції та американської митної служби в рамках спільної операції було викрито злочинну групу, члени якої займались виготовленням та поширенням дитячої порнографії у мережі Інтернет.

Досвід подібних тактичних операцій, на нашу думку, корисно перейняти й правоохоронним органам України. Про необхідність криміналістичного розгляду питання допустимості "оголошень-пасток" відзначають В.П. Бахін, І.В. Гора, П.В. Цимбал [350, с. 302], І.В. Строков [351, с. 112]. Щоправда, деякі сумніви щодо правомірності їх проведення породжує давня полеміка з приводу допустимості "слідчих хитрощів" та "психологічних пасток" при розслідуванні злочинів. Слід нагадати, що радянські вчені-криміналісти, які займались розробленням та вивченням часткової криміналістичної теорії тактичних операцій, неоднозначно висловлювались стосовно допустимості тактичних прийомів, проведення яких пов'язане із слідчими хитрощами та психологічними пастками. Противниками концепції "слідчих хитрощів", "психологічних пасток", "пасток" виступали М.С. Строгович, І.Д. Перлов, С.П. Стремовський, І.Ф. Пантелеєв, В.К. Гавло та інші. Характеризуючи погляди вчених, що є прихильниками чистоти процесуальної форми І.Є. Биховський, Ф.В. Глазирін і С.К. Пітерцев відмічають, що деякі вчені настільки гіпертрофують і формалізують, відриваючись від реальних умов життя, питання про гарантії прав обвинуваченого, що, по суті, обеззброюють слідчого в його діяльності щодо встановлення об'єктивної істини [352, с. 40]. Інші вчені, які виступають за розширення засобів і прийомів слідчої діяльності, допускають можливість використання "слідчих хитрощів" та "психологічних пасток" у ролі тактичних елементів слідчих дій, хоча й відмічали етимологічну невідповідність цих термінів. Серед них – В.П. Бахін [353, с. 126], Р.С.

Бєлкін [354, с. 114], І.П. Герасимов [355, с. 232], О.М. Ларін [356, с. 147], Г.Ф. Горський, Л.Д. Кокорєв, Д.П. Котов [357, с. 72] та інші.

Так В.П. Бахін, В.С. Кузьмічов і В.К. Весельський замічають, що "тактика необхідна там, де зустрічається протидія цілям даної діяльності або досягненню конкретного результату, і спрямована вона на подолання або нейтралізацію такої протидії. Тактика, в найбільш загальному вигляді, полягає у вмінні перехитрити протидіючу сторону за рахунок маскування своїх намірів, шляхом введення в оману, на основі спонукання до певних дій".

Тактичні аспекти діяльності, на їхню думку, виникають за наявності: а) протилежності інтересів взаємодіючих сторін; б) складних екстремальних ситуацій; в) необхідності вибору найдоцільнішого рішення з ряду можливих варіантів дій; г) тактичного ризику при подібному виборі та вмінні (здібності) приймати відповідні рішення [358, с.217–225].

На вибір тактичних засобів впливає слідча ситуація, тобто обстановка, в якій відбувається процес доказування [359, с.5].

Стосовно допустимості використання тих чи інших тактичних засобів слідчої діяльності В.П. Бахін, І.В. Гора, П.В. Цимбал вважають: "При проведенні розслідування будь-яка дія і будь-яка інформація, що отримана в його ході, одночасно захищають права та інтереси одних осіб і зачіпають права та інтереси інших. Отже, і законодавець, і вчений, і практик, вирішуючи будь-яке конкретне питання, повинні враховувати цей взаємозв'язок (взаємовплив) і відповідно до цього визначатися, чому саме віддати пріоритет у кожному конкретному випадку" [360, с. 186]. Дещо категоричнішу позицію, з огляду на сучасний стан протидії злочинності, займають О.Ф. Волинський і Д.П. Поташник. Зокрема, вони відмічають, що в умовах зростаючої небезпеки, суспільство неминуче буде вимушено йти (і це треба усвідомити) на розумні поступки у частині прав та свобод особистості. Це самообмеження кожного необхідно для контролю над злочинністю, для безпеки всіх. Злочинність дедалі більше стає фактором, спроможним дезорганізувати економіку й політичне життя всього суспільства [361, с. 62]. Для того, щоб спираючись на використання юридичних засобів, відвернути економічні злочини, обмежити «чорну» диверсифікацію, треба проблему попередження економічної злочинності розглядати не просто у кримінально-правовому полі, тобто з позицій покарання або посилення карних санкцій за вчинені злочини, а передусім в господарсько-правовому полі [362, с.153].

Полеміка з приводу допустимості використання у стадії досудового розслідування "пасток" свідчить про наукову та практичну значимість цього питання в діяльності органів дізнання та слідства. Воно прямо стосується

Значна частка заяв про здійснення злочинів доводиться на телефонне джерело первісної інформації про злочини. Згідно із чинним законодавством такі відомості належать до іншої інформації про правопорушення, що надійшли по телефону, телеграфу, факсимільним зв'язком або іншим видом зв'язку. На наш погляд, у перелік даних джерел на правовому рівні варто додати й електронну пошту, що прийшла на зміну традиційної. Стосовно до сказаного вимагає окремого пророблення механізм реєстрації й прийому таких заяв, а також вироблення джерел оперативного одержання й обробки інформації про відправника електронних повідомлень. Для початку повинен бути сайт відповідної чергової частини з електронною адресою, яку необхідно перевіряти кожному чергову на предмет існування повідомлень, які потребують перевірки або реєстрації і прийняття необхідних рішень.

У рамках комп'ютеризації чергових частин пропонується модернізація апаратно-програмного комплексу чергової частини ОВС шляхом об'єднання АОН абонента, багатофункціонального цифрового реєстратора сигналів, що функціонує відповідно до відомчих наказів у кожній черговій частині ОВС, із цифровою картою міста й базою даних по телефонних номерах різних абонентів. Основні компоненти такого вдосконаленого комплексу включають: наявність детальної електронної карти з масштабом не більше 1: 10000- 25000; розміщення маршрутів проїзду патрулів і дислокації постів на цифровій карті методом нанесення міток; комп'ютерну програму, однією з функцій якої є формування найкоротшого шляху руху патрулів до того, хто зателефонував.

Крім того, існує можливість оснащення створеної програми додатковими функціями, деякі з яких реалізовані в подібних системах, наприклад: оснащення радіомаяками піших і автомобільних патрулів; можливу інтеграцію комплексу з аналогічними, що вже існують в екстрених службах, наприклад, службі невідкладної медичної допомоги, МНС і ін.; підтримку автоматизованої функції прийняття рішень про зразкове розташування сил і засобів, необхідних для забезпечення комплексу невідкладних оперативно-розшукових заходів і слідчих дій стосовно до характеру події; додаткове оснащення такої системи пристроями експрес-аналізу фоноскопічних ознак осіб, що звертаються по телефону й ін.; реалізацію комплексної інфраструктури інформаційного захисту; зокрема варто передбачити можливість на основі конкретного випадку, використовуючи банк даних по аналогічним випадкам, рекомендувати хід і напрямок комплексу невідкладних слідчих дій і оперативно-розшукових заходів і інших дій із самостійним запитом у базу даних. Запит повинен здійснюватися як в ав-

помогою засобів он-лайного спілкування, оперативніше вирішував поточні справи.

Тут могла б міститися й інформація про розшук злочинця, який переховується, і звернення до громадськості щодо встановлення очевидців та інших свідків події, а також оголошення про винагороду за корисні для розслідування відомості. На цих сторінках відвідувачі могли б довідатися про те, як уберегти себе від дій злочинця, причини й умови, що сприяють скоєнню злочинів. Інтернет-сайт органів розслідування міг би сприяти викриттю перекручування інформації про розслідування, що надається журналістами та захисниками у пресі.

На практиці при передачі «орієнтувань» в інші ОВС є загальний недолік - неповнота й недосконаліть наявних у них відомостей, використання ж комп'ютерів, повне й грамотне кодування наявних даних дозволяють зафіксувати значно більшу кількість ознак і тим самим підвищити їх криміналістичну значимість. Вирішити проблему дефіциту часу, на наш погляд, можуть спеціальні системи сторожових запитів, за допомогою яких установлюється автоматичний контроль за проходженням інформації в АБД різних рівнів на конкретних осіб або об'єктів, що представляють оперативний інтерес. У випадку виявлення в інтегрованому банку даних об'єктів, що цікавлять, система сама сповістить ініціатора постановки об'єкта.

Одним із підходів до виконання перелічених завдань може бути створення й використання спеціалізованих автоматизованих робочих місць (АРМ) співробітників чергових частин ОВС, об'єднаних у локальну обчислювальну мережу, що дозволить зосередити інформацію оперативно-розшукового характеру, специфічного й профілактичного призначення, криміналістичні, аналітико-статистичні дані, проводити аналіз минаючих інформаційних потоків. У даних системах важливо забезпечити повноту відомостей, що надходять, тобто поставити "на потік" збір фактів криміногенного характеру. Вони концентруються в пам'яті комп'ютера за принципом електронного досьє на осіб, події, предмети. При цьому комп'ютер здійснює набір операцій із застосуванням структур логічних алгоритмів, дозволяючи споживачам прогнозувати події й потім приймати рішення.

Також, на наш погляд, необхідне створення АБД про: а) послідовність початкових дій співробітників чергової частини при нестандартних ситуаціях (наприклад хімічній, радіаційній, токсичній і інших погрозах і т.д.), б) заявників, які зверталися до чергової частини, крім існуючих відомчих інструкцій, для оптимізації пошуку, з метою одержання в разі потреби анкетних і інших даних про заявників.

використання повідомлень ЗМІ при проведенні тактичних операцій. Адже заходи, пов'язані з використанням ЗМІ в тактичних операціях, здійснюються у комплексі з проведенням слідчих дій, оперативно-розшукових та інших заходів. Метою тактичної операції завжди є вплив на слідчу ситуацію в цілому або на її компоненти. Такий вплив у кінцевому рахунку завжди являє собою вплив на людей, які так чи інакше пов'язані з розслідуванням кримінальної справи. Правомірність такого впливу і є основною умовою допустимості проведення тактичної операції [407, с. 172]. Свобода вибору позиції, вибір визначеної лінії поведінки, наявність умов для її вибору – це ті ознаки правомірності використання повідомлень ЗМІ при проведенні тактичної операції для встановлення особи підозрюваного у вчиненні злочину та його затримання. Таким чином, можна запропонувати інформаційно-тактичну операцію – це система тактичних прийомів, комбінацій, слідчих дій, оперативно-розшукових заходів з використанням сучасних інформаційних технологій або ЗМІ, яка є ситуаційною потребою взаємодії посадових осіб різних служб правоохоронних органів і спрямована на виконання проміжного завдання розслідування.

На нашу думку, використання Інтернет-пасток є допустимим тактичним прийомом при проведенні тактичної операції по виявленню та затриманню особи, яка підозрюється у вчиненні злочину. Провокування особи до вчинення злочину за таких умов відкидається, бо таке затримання не може бути підставою притягнення її до кримінальної відповідальності. Крім того, зберігається така умова допустимості використання тактичного засобу впливу, що визначає його як правомірний, – вибірковість впливу. Мається на увазі направленість впливу лише на окремих осіб і його нейтральність щодо інших. Таким чином, допустимість використання Інтернет-пасток визначається метою проведення такої тактичної операції – виявлення та затримання особи, підозрюваної у вчиненні дій, що мали місце до моменту її затримання і містять ознаки злочину [363, с.142-143]. Однак при цьому обов'язковим є збереження у таємниці подробиць приватного життя громадян, які при проведенні перевірки попали у поле зору правоохоронців, але виявились не причетними до вчинення злочинів.

Виступаючи за допустимість використання слідчих хитрощів та пасток О.М. Ларін відмічає, що мистецтво слідчого полягає у тому, щоб продумано, точно вирішувати, яка інформація, в якому об'ємі і в який момент може стати відомою злочинцю і пов'язаним із ним особам, аби це не тільки не зашкодило, а й допомогло досягненню істини [364, с. 49]. Інший російський учений-криміналіст М.П. Яблоков допускає використання повідомлень ЗМІ для дезінформації членів організованої злочинної групи

про найближчі плани слідства як елемент реалізації тактичних операцій у ході розслідування [365, с. 160]. За допустимість використання обману при розслідуванні злочину виступає Р.С. Бєлкін. Зокрема, він уважає, що пора відкрито визнати, що й держава визнає допустимість обману в правоохоронній сфері: вона узаконила ОРД, яка багато у чому ґрунтується на дезінформації, обмані як засобу виявлення й розкриття злочинів. Обман протидіючої оперативному співробітникові особи не вважається аморальним; не вдаючись до обману, неможливо впровадитись в злочинне угруповання, піймати на гарячому хабарника, вимагача тощо. Соромливе маскування слова "обман" спеціальним терміном "легендування" сутності справи не міняє. На думку вченого, треба або визнати, що в правоохоронній діяльності обман допустимий, або його заборонити; принципове рішення цього питання може бути тільки однозначним. Інша справа, що, допустивши можливість обману, можна його певним чином обмежити, вказати, на чому він ніколи не може ґрунтуватись, які засоби обману будуть визнаватись безумовно недопустимими, абсолютно аморальними [366, с. 104]. У цьому світлі варто згадати вислів американського криміналіста Ч. Сакамі, який відмічає парадокс у тому, що зі злочинністю XXI ст. доводиться боротися на підставі законів XIX ст. [367, с. 62].

Таким чином проблема допустимості тактичних засобів, які прямо не зазначені, однак і не заборонені законом, переноситься із правової сфери до моральної. Перед слідчим постає питання співвідношення інтересів окремих громадян (підозрюваного та потерпілого), а також суспільних інтересів. Досить категоричну відповідь на це питання дає В.І. Бакштановський. Зокрема, він вважає моральним і доцільним той засіб, який є необхідним і достатнім для досягнення моральної мети, який у той же час не суперечить більш високій і вищій меті, не змінює їх характер [368, с. 49]. М.П. Хайдуков із цього приводу відмічає, що якщо при виборі прийомів і засобів впливу виникло протиріччя між двома окремими цінностями й зберегти їх обидві при досягненні процесуально й тактично значимої мети не представляється можливим, то доцільним і морально виправданим буде моральний компроміс, тобто таке тактичне рішення, яке направлене на збереження найбільш значимої у даній ситуації цінності [369, с. 72]. З ним погоджується Р.С. Бєлкін, який як моральний компроміс допускає застосування "меншого зла", тобто обману, у слідчій діяльності. Однак він категорично зазначає, що подібні компроміси є допустимими лише в об'єктивно вимушених випадках [370, с. 112].

Планування та проведення пасток для виявлення й затримання осіб, які вчинили злочини, можливе як із використанням Інтернет-ЗМІ, так і повід-

На наш погляд, частково цю проблему могло б вирішити безпосереднє використання можливостей мережі Інтернет як слідчим, так і експертом. Будучи, по суті, недосконало упорядкованим сховищем найрізноманітнішої інформації, це джерело могло б, при вмілому звертанні до нього, допомагати в роботі з кримінальної справи, а також у провадженні експертиз та досліджень.

Багато установ і організацій розмістили у всесвітній мережі свої сторінки (сайти), ознайомившись з якими можна довідатися про адреси, телефони й інші відомості, як про сам об'єкт, так і про керівників та співробітників, інформацію про характер діяльності, партнерах і продукції, що випускається.

Вже не вважається новиною розміщення особистої інформації (біографії, візитної картки, фотознімка) на персональному сайті тієї чи іншої особи в мережі. Численні електронні ЗМІ й електронні копії газет і журналів, можуть містити інформацію про осіб, що цікавлять слідчого, підприємства або установи [398].

Нарешті, починаючи розслідування злочину, учиненого із застосуванням нових для слідчого знань, або в незнайомій для нього галузі людської діяльності, він може поповнити свої знання про це, також за допомогою інформації з мережі Інтернет. Інтернет-сторінки, створювані окремими експертними підрозділами могли б містити інформацію про їх експертні можливості, допомогти слідчим у виборі певної експертної установи та конкретного експерта. Не має ніяких перешкод для того, щоб експерти розміщали на своїх сторінках інформацію про порядок підготовки об'єктів для експертизи, одержання зразків для порівняльного дослідження, формулювання питань експерту. Такі сторінки могли б служити і для професійного спілкування фахівців, які працюють у різних відомствах і навіть країнах.

Одним із чинників, який впливає на ефективність протидії злочинності, є організація співробітництва, взаємодії та координації діяльності різних державних органів. Спільна діяльність щодо протидії злочинності знаходить безпосереднє вираження в таких напрямах взаємодії: виявлення, припинення, розкриття та розслідування злочинів; профілактика злочинів та інших правопорушень; розшук та затримання злочинців, (осіб, які переховуються від слідства та суду); удосконалення правової бази у сфері протидії злочинності в цілому та окремих злочинних проявів [399].

Імовірно, і слідчим було б що сказати зі сторінок Інтернет-сайту свого слідчого підрозділу, де він маючи право обмеженого адміністративного доступу до сайту розміщував би певну інформацію, редагував її, та за до-

не дозволяє здійснювати централізоване управління системою. АДІС, яку слід створити, повинна охоплювати всі дактилоскопічні обліки органів внутрішніх справ України, і тому вже за своїм значенням вона є національною системою. Крім цього, проект створення національної АДІС повинен розроблятися відповідно до вимог постанов Кабінету Міністрів України та бути узгодженим з Державним комітетом зв'язку та інформатизації України, а відбір та придбання засобів обчислювальної техніки, оргтехніки, телекомунікаційного обладнання тощо, необхідних для функціонування системи, має визначатися на тендерній основі [395; 396; 397].

Перспективним на наш погляд являється і можливість автоматизувати облік об'єктів, отриманих із застосуванням сучасних методів голографії, які починають впроваджуватися в процес розслідування злочинів, що дозволяють фіксувати більші обсяги криміналістично значимої інформації про об'єкт обліку. Голографія, пише Р.С. Бєлкін, - метод стійкий до втрати значної частини інформації у відбитку пальців і дозволяє використовувати всю інформацію про папілярний візерунок, у тому числі особливості його будови. Голографія може бути зіставлена з відбитками пальців з картотеки, а сполучення голографії й ПЕОМ забезпечить автоматичний пошук матеріалу для такого порівняння. Даний метод дозволяє запам'ятовувати зовнішність особи, що перевіряється по обліку, з максимальною повнотою. Зазначене потребує від криміналістичної реєстрації повного й багатогранного аналізу потенціалу технічних і методичних можливостей, що відповідав би передовим науковим знанням, а також перетворення отриманих у результаті такого аналізу даних у криміналістично значиму інформацію для потреб правоохоронних органів.

Слідчий нерідко має потребу в інформації про географічне розташування того чи іншого місця, розклад руху транспорту, поштової індексації, телефонах і адресах. При складанні процесуальних документів може бути затребувана лінгвістична інформація про значення терміна, синоніми, орфографію. Слідчому необхідне залучення різноманітних правових актів, які постійно змінюються й удосконалюються. У роботі експерта довідкова інформація має навіть ще більше значення.

Сьогодні методами одержання такої інформації є традиційне використання книжкових довідників, звертання до джерела по телефону, направлення поштових письмових запитів. Варто визнати, що ці можливості вже не можуть повною мірою задовольнити вимог слідчого й експерта в силу своєї неоперативності (поштові запити), недостатньої динамічності відновлення відомостей і дефіцитності (книжкові довідники), недостатнього обсягу (відомості, одержувані за допомогою телефону).

омлень друкованих ЗМІ, телебачення та радіомовлення. Досвід правоохоронних органів України у проведенні таких тактичних операцій дещо більший ніж у мережі Інтернет. Щоправда, результати не завжди збігаються з очікуваними. Так негативної критики у багатьох ЗМІ зазнали імітації правоохоронними органами вбивств (з поміщенням відповідних повідомлень у ЗМІ) депутата Верховної Ради Криму М. Котляревського (листопад 2002 р., м. Євпаторія), а також директора фірми "Арго" Дніпропетровського лікеро-горілчаного заводу К. Крупеникова (лютий 2003 р., м. Дніпропетровськ). Зазначені приклади наводять на думку про недостатній рівень теоретичного опрацювання питань, пов'язаних із можливостями та допустимістю використання повідомлень ЗМІ у діяльності правоохоронних органів і, зокрема, органів досудового слідства. Складається враження, ніби наука або залишила поза увагою потреби практики, або не встигає за пошуком шляхів їх вирішення. Очевидно, що розвиток ситуації не можна упускати з-під контролю. Означені проблеми торкаються не лише діяльності органів досудового слідства та ЗМІ. Вищевикладене засвідчує, що ці проблеми пов'язані з правами та свободами громадян, а тому їх вирішення є важливим для розвитку в Україні громадянського суспільства.

Висновки до розділу 2

Виконання завдань зміцнення правопорядку та боротьби зі злочинністю повинно бути тісно пов'язане з формуванням належної суспільної думки в нашому суспільстві, що вимагає збільшення обсягу та інтенсивності взаємодії посадових осіб оперативно-розшукових та слідчих підрозділів із різними соціальними групами та верствами населення, соціальними інститутами, серед яких важливе місце займають ЗМІ.

Серед засобів протидії злочинності належне місце повинні зайняти ЗМІ, для формування належної суспільної думки про учасників організованих злочинних груп, дифамації відносно них, створенні умов отримання нової криміналістично значимої інформації, непроцесуального використання оперативної інформації, попередження тиску впливових посадових осіб на слідчі та судові органи, відповідно до яких розроблені тактичні операції.

Досить проблематичним залишається правове забезпечення нерозголошення даних досудового слідства стосовно діяльності ЗМІ. Недостатнім є законодавче врегулювання порядку висвітлення засобами масової інформації процесу розслідування у кримінальній справі та його результатів до вступу вироку в законну силу. У зв'язку з цим пропонується внести

зміни до Закону України “Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації”, і закріпити обов’язок журналістів погоджувати зі слідчим текст майбутньої публікації в ЗМІ, що ґрунтується на матеріалах кримінальної справи, й отримання від нього письмового дозволу на висвітлення певної інформації по обставинам розслідування злочину.

Необхідно впровадження наступних найважливіших технологій захисту інформації: нових стандартів електронного цифрового підпису; масштабованої системи електронних цифрових сертифікатів з використанням центрів довіри; криптографічно захищених корпоративних (віртуальних) комп’ютерних мереж і засобів міжмережевого екранування;засобів антивірусного захисту й засобів захисту від несанкціонованого доступу до інформації для неоднорідних розподілених інформаційних систем; моніторингу й аудиту безпеки мережних інформаційних ресурсів; захищених програмно-апаратних засобів для IP-телефонії; засобів захисту мереж мобільного зв’язку й персональних комунікацій; засобів біометричної ідентифікації й аутентифікації на базі інтелектуальних карт і інших малогабаритних технічних засобів обробки інформації та ін.

Аналіз літературних джерел та практики розкриття та розслідування злочинів, учинених ОЗУ, дозволив автору визначити тактичні основи використання інформаційних технологій і засобів масової інформації в діяльності з розкриття та розслідування злочинів.

Дієвими заходами розкриття та розслідування злочинів, учинених ОЗУ є типові тактичні операції з використанням ЗМІ під умовною назвою «свідок», «підозрюваний». На матеріалах публікацій ЗМІ, вивчання досвіду протидії організованій злочинності пропонується тактика проведення різновидів тактичних операцій: «полювання за жертвою», «імітація», «міраж», «витік інформації», «протидія».

При розслідуванні злочинів слідчі дії здійснюються не ізольовано, а у взаємодії з оперативно-розшуковими заходами іншими діями і заходами і в необхідній послідовності.

Аналізуючи дискусійні питання щодо понять тактична комбінація та операція, автор вважає, що вони є самостійними категоріями криміналістики і пропонує авторське бачення цих понять: тактична комбінація – це визнана обставинами справи ефективна сукупність тактичних прийомів або слідчих дій, яка проводиться з метою зміни слідчої ситуації, поведінки чи позиції підозрюваних, обвинувачених та інших осіб і створюють сприятливі умови для вирішення конкретного завдання розслідування; тактична операція – це система процесуальних і непроцесуальних дій і заходів (слідчих і оперативно-

вів даних або працювати в режимі електронної пошти - для пересилання текстової інформації. Створення автоматизованих робочих місць співробітників чергової частин ОВС дає можливість відслідковувати стан оперативної обстановки на території, що обслуговується, у режимі реального часу й координувати діяльність нижчих чергових підрозділів у розкритті злочинів по "гарячих слідах" [392].

Автоматизоване робоче місце — це програмно-технічний комплекс, призначений для автоматизації діяльності певного виду. Основною характеристикою АРМ є орієнтація на людину, яка не має професійної підготовки з використання обчислювальної техніки, але професійно обізнана у конкретній предметній галузі [393, с.5]. Впровадження АРМ дозволяє оперативному складу ОВС створювати власні (локальні) бази даних, направляти інформацію й одержувати відповіді на запити з ІБД вищих рівнів засобами обчислювальної техніки.

З огляду на розвиток нових інформаційних технологій, представляється можливим визначити криміналістичну реєстрацію як елемент системи інформаційного забезпечення процесу розкриття, розслідування й попередження злочинів, що заснований на нормах права, а при їх відсутності на ініціативі компетентних правоохоронних органів, криміналістичну реєстраційно-інформаційну систему (КРІС) одержання, зосередження, обробки й видачі криміналістично значимої інформації.

Так в умовах постійного зростання криміналістичних дактиломасивів для того, щоб їх обробка не гальмувалася через ручний метод перевірок, єдиним шляхом вирішення цієї проблеми є автоматизація накопичування дактилоскопічної інформації та процес перевірок з використанням ЕОМ.

У світі розроблено та впроваджено в практику багато автоматизованих дактилоскопічних ідентифікаційних систем (далі – АДІС). До найбільш відомих АДІС можна віднести французьку систему “Morfo”, яка впроваджена в практику поліції Франції, ФРН, Ізраїлю, Словаччини, РФ та інших країн світу, американські системи “Printrak” та “Kogent”, японську систему “NEC”, російські системи “Сонда”, “Папілон”, “DEX”, білоруську систему “Дакто” та інші [394, с. 75-76].

Усі зазначені системи відрізняються одна від одної як операційною системою та системою керування базою даних, так і алгоритмами побудови цифрових образів зображення для зберігання в базі даних та пошуку. Для створення таких систем використовуються різні програмні засоби розробки інтерфейсу.

Такий стан справ не дозволяє створити однотипну розподілену систему дактилоскопічної реєстрації, робить неможливим взаємодію між регіонами,

дно з КПК; зберігання та використання різноманітної довідкової інформації з кримінальних справ; контроль з боку керівників підрозділів за розслідуванням кримінальних справ на всіх етапах; організація та проведення бухгалтерських ревізій та експертиз, різноманітні розрахунки з кримінальних справ по економічних злочинах; використання у ході розслідування програм з методиками розслідування злочинів різних видів.

У сучасний період істотно розширилися технічні можливості використання слідчим засобів комп'ютерної техніки по таким напрямкам: застосування комп'ютерних технологій слідчим при збиранні доказів; використання слідчим як докази інформації, яка отримана з різних комп'ютерних баз даних; одержання слідчим з комп'ютерних баз даних інформації й використання її при плануванні роботи з розслідування злочинів; використання електронної пошти для переписки в процесі провадження по кримінальних справах; прилучення до кримінальної справи як докази, інформації, що зберігається на магнітних носіях; використання при розслідуванні злочинів як докази документів, які виготовлені іншими учасниками кримінального процесу із застосуванням комп'ютерних технологій; прилучення до кримінальної справи документів, виготовлених слідчим із використанням комп'ютерних технологій; застосування слідчим комп'ютерних технологій при плануванні розслідування по кримінальних справах і здійсненні контролю за виконанням запланованих слідчих дій, оперативно-розшукових, організаційних і інших заходів; використання слідчим комп'ютерних баз даних для контролю за дотриманням процесуальних термінів затримання підозрюваних, утримання під вартою обвинувачуваних (підозрюваних), досудового слідства й інших, передбачених кримінально-процесуальним законодавством, термінів; застосування комп'ютерних технологій слідчим при оцінці наявних у справі доказів, у тому числі й отриманих або виготовлених іншими учасниками кримінально-процесуальної діяльності з використанням комп'ютерних технологій; використання засобів комп'ютерної техніки в навчанні слідчих та ін.

Найпоширенішим у слідчій практиці є застосування комп'ютерних технології слідчим при збиранні доказів, що дозволяє автоматизувати виконання багатьох видів трудових операцій. Найбільше частіше ЕОМ застосовують для підготовки, редагування й друкування текстів документів, рідше для розрахунків при підготовці процесуальних, організаційних і інших документів.

Використання спеціального програмного забезпечення надає доступ до бази даних управлінь інформаційних технологій і одночасно всіх чергових частин ОВС, дозволяє одержувати інформацію з усіх існуючих маси-

розшукових, організаційних), тактичних комбінацій з використанням інформаційних технологій, яка зумовлена ситуаційною необхідністю взаємодії посадових осіб різних служб правоохоронних органів і спрямована на вирішення проміжного завдання розслідування.

Автор наголошує на тому, що необхідно використовувати нові тактико-криміналістичні засобів протидії злочинності зокрема можливості комп'ютерних технологій та засобів масової комунікації. Розкриваються особливості використання можливостей ЗМІ у процесі розслідування злочинів, як канал психологічного впливу на учасників кримінального процесу, який здійснюється шляхом передачі значимої для адресата інформації і направлений на формування бажаної психологічної установки для успішного розслідування злочинів, учинених ОЗУ.

Автор враховуючи міжнародний досвід протидії злочинності пропонує проведення тактичних операцій з використанням Інтернет-пасток при проведенні тактичних операцій по виявленню та затриманню осіб, які підозрюються у вчиненні злочинів, які вчиняються ОЗУ.

РОЗДІЛ 3
ОСОБЛИВОСТІ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРИ РОЗКРИТТІ І РОЗСЛІДУВАННІ ЗЛОЧИНІВ, УЧИНЕНИХ ОРГАНІЗОВАНИМИ ЗЛОЧИННИМИ УГРУПОВАННЯМИ

3.1. Інформаційне забезпечення діяльності щодо розкриття і розслідування злочинів

Інформаційне забезпечення розкриття злочинів є невід'ємною частиною комплексу проблем, що пов'язані з вивченням та використанням закономірностей збирання джерел інформації для формування судових доказів. Їх актуальність і важливість пояснюється тим значенням, яке значення має інформація в процесі доказування. В останній час з'явилися нові науково-технічні засоби пошуку, дослідження, фіксації і вилучення криміналістичної інформації, що спонукає до перегляду низки процесуальних положень, технічних і тактичних рекомендацій відносно інформаційного забезпечення діяльності ОВС.

За останнє десятиріччя в діяльність підрозділів було впроваджено системи електронного та комп'ютерного зв'язку, геоінформаційні системи, на основі вже існуючих банків і баз даних, впроваджено автоматизовані інформаційно-пошукові системи та підсистеми, створено автоматизовані робочі місця чергових частин ОВС, оперативних та слідчих працівників.

Специфіка боротьби з інформаційною злочинністю полягає в тому, що вона потребує активного використання інформації, яка знаходиться в цільових автоматизованих системах різних міністерств та відомств.

У ході аналізу сучасного стану забезпеченості діяльності оперативних підрозділів інформаційними ресурсами, визначені наступні масиви інформації, які використовуються в оперативно-розшуковій діяльності ОВС найчастіше:

бази даних Державної податкової адміністрації України, що дозволяють установити відомості про реєстрацію суб'єкта підприємницької діяльності, коди ОКПО, податкові номери, фактичну і юридичну адресу, анкетні дані керівників, засновників, їхні телефонні номери, рахунки, що маються в банківських установах, одержати іншу інформацію, а так само дозволяють аналітичним шляхом виявити зв'язаних, афілійованих осіб, неформальні об'єднуючі групу підприємств умови, провести вибірку групи підприємств за визначеними умовами та інше;

інформаційно-пошуковій системі (ІПС), і автоматизовані банки даних (АБД) [390, с. 269].

Як показує практика, для виконання професійних функцій співробітниками оперативних підрозділів потрібна різнопланова інформація, збір якої може забезпечуватись кількома типами інформаційних банків даних: звичайні інтегровані банки даних (ІБД), які містять структуровану форматну інформацію з механізмом виведення та аналізом змісту; інтегрована система моніторингу (ІСМ) телекомунікацій і система моніторингу Інтернету.

Застосування сучасних інформаційних технологій породжує впровадження нових напрямків у діяльності ОВС у боротьбі зі злочинністю. Як уже зазначалась, одним із основних напрямків інформаційного-аналітичного забезпечення ОВС є аналітична розвідка, а інформаційно-технічного забезпечення – комп'ютерна розвідка, яка являє собою розвідку в інформаційному просторі [391, с. 26].

Однією з обов'язкових умов підвищення ефективності розкриття й розслідування злочинів є впровадження в практику діяльності правоохоронних органів сучасних інформаційних технологій, програмно-технічних засобів, комунікаційних засобів прийому - передачі інформації, створення єдиної інформаційно-обчислювальної мережі й інтегрованих банків даних на основі типізації й уніфікації.

Засоби обчислювальної техніки активно застосовуються в діяльності ОВС з початку 60-х років XX ст. по таких основних напрямках: забезпечення інформаційно-аналітичної роботи в процесі управління органами й службами; інформаційне забезпечення діяльності по розкриттю й розслідуванню злочинів; методичне забезпечення діяльності різних категорій співробітників і їх навчання. Але сьогодні цього не достатньо необхідна інтенсифікувати ці процеси автоматизувати більшість процесів.

У сфері розслідування злочинів автоматизації підлягають: процес слідчого виробництва з використанням баз процесуальних та інших документів, що оформляються на стадії попереднього розслідування; планування заходів по конкретних кримінальних злочинах; створення календарних планів і мережних графів розслідування; нагромадження та аналіз інформації з кримінальних справ, зокрема великого обсягу та багатоепізодних; складання слідчих та інших документів (у першу чергу, постанов щодо притягнення як обвинуваченого та висновків з обвинувачення) на основі даних, занесених у базу; передача до суду протоколів допитів, постанов та інших процесуальних документів на магнітних носіях та по каналах зв'язку; вибір та передача необхідної інформації для проведення відповідних заходів у ході оперативно-розшукової діяльності, її оформлення згі-

бігання злочинів оперативними підрозділами кримінальної міліції в процесі ОРД є одним із його компонентів, сутність якого пов'язана з отриманням, обробкою, аналізом, використанням та зберіганням інформації, що відображає реальні явища і процеси, факти і події, які відбуваються в оперативно-розшуковій сфері діяльності [385, с. 207].

Інформаційне забезпечення — процес складний, і його здійснення повинно мати не тільки цілеспрямований, а й централізований характер [386].

Поділяючи думку Журавльова В.Ю. під інформаційним забезпеченням ОРД спеціальних підрозділів по боротьбі з організованою злочинністю необхідно розуміти комплекс заходів, який виконується різноманітними структурними підрозділами і спрямований на одержання з гласних і негласних джерел оперативно-розшукової інформації, її фіксацію, збереження, опрацювання, багатофакторний аналіз і використання первинних і збагачених даних з метою виконання підрозділами по боротьби з організованою злочинністю покладених на них функцій [387, с.8; 388].

Дослідження стану інформаційного забезпечення оперативного підрозділів кримінальної міліції, у тому числі механізму обміну оперативно значущої інформацією між різними оперативними службами, свідчить про низку небажаних моментів: розвинена конкуренція різних оперативних служб міліції та певна їх відособленість, а також закономірні вимоги контррозвідувального характеру щодо захисту таємної оперативної інформації на носіях, що призводить до створення замкнутих баз даних, які набули значного поширення. Це зумовлено такими факторами, відсутністю взаємодії між функціональними підрозділами у вигляді обміну документів, обмеженістю доступу до «кишенькових» баз даних, відсутністю ефективного механізму обміну; ізольованістю роботи підрозділів за профілями спеціалізації; відсутністю спеціального координуючого аналітичного підрозділу з правом опрацювання даних функціональних відділів, тобто відсутність ланцюга аналітичної розвідки, який існує в підрозділах по боротьбі з організованою злочинністю [389, с. 207].

Аналіз слідчої практики, дозволяє визначити доцільність передбачення можливості доступу і використання більшості оперативних обліків слідчим, який має допуск до державної таємниці при розкритті і розслідування злочинів.

У теорії ОРД визначені три основні методи інформаційного забезпечення оперативної роботи, зокрема: інформаційно-аналітичний метод оцінки оперативної обстановки; інформаційно-аналітичний метод отримання, обробки відомостей про осіб, події і факти, які становлять оперативний інтерес; метод розшуку та використання відомостей що містяться і в

оперативні бази даних податкової міліції, що дозволяють установити відомості про виявлені підприємства, які мають ознаки фіктивності, про їхніх номінальних засновників і керівників, реєстраційні дані підприємств, використані банківські рахунки, підрозділ податкової міліції, яким виявлена дана фірма;

бази даних місцевих телефонних станцій, що дозволяють установити відомості про анкетні дані абонента телефонного номера чи адресу об'єкта, місцезнаходження номера, безпосередньо телефонний номер;

бази даних Державного комітету статистики України, що дозволяють установити відомості про реєстрацію і місцезнаходження підприємств, анкетні дані керівників і номери їхніх контактних телефонів;

бази даних місцевих бюро технічної інвентаризації, що дозволяють установити відомості про належність нерухомості, зміну прав власності на неї, іншу інформацію про нерухомість і т.д.

Як правильно зазначає В.В. Лисенко, існуючий рівень інформаційного забезпечення при належному його використанні є головною умовою ефективної діяльності слідчих та оперативних підрозділів міліції. Така робота повинна проводитися на постійній основі і мати цілеспрямований та наступальний характер. Необхідно проводити дослідження та створювати відповідні методичні розробки про зміст аналітичної роботи міліції та використання інформації у ході виявлення та розслідування злочинів [371].

Проблематика інформаційного забезпечення слідчої діяльності перебуває у зв'язку з більш широким питанням - інформаційною діяльністю. Під нею розуміють сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави. Закон визначає чотири основні види інформаційної діяльності: одержання, використання, поширення та зберігання інформації [372, с.263-264]

Впровадження сучасних інформаційних технологій у зазначену діяльність потребує створення такого предметного інформаційного середовища, яке забезпечить необхідними даними, мінімізує затрати на виконання технічної роботи, що сприятиме якості й оперативності прийняття рішень [373, с.83]

Проблема інформаційного забезпечення, певного поширення набула дослідженням у зв'язку з питань криміналістичного забезпечення боротьби зі злочинністю.

Криміналістичне забезпечення практики протидії злочинності є іманентно суттєвою ознакою криміналістики та полягає у виявленні потреб оперативно-розшукової, слідчої й експертної практики та всебічному озброєнні працівників правоохоронних органів дієвими криміналістични-

ми рекомендаціями, які забезпечують оптимізацію розкриття, розслідування й попередження злочинів. [36,с.116] Як зазначає, В.В. Лисенко, криміналістичне забезпечення діяльності правоохоронних органів щодо виявлення та розслідування злочинів являє собою певну систему. Відповідно, вона складається із окремих елементів, що у сукупності створюють структуру. Такими елементами, зокрема, можуть бути: 1) блок криміналістичних рекомендацій (як організаційного, тактичного, так і методичного характеру); 2) блок підготовки відповідних кадрів (спеціальної криміналістичної освіти); 3) блок технічного та інформаційного забезпечення процесу виявлення, розслідування та запобігання злочинам [374].

В Україні забезпечення слідчої та експертної практики розглядається переважно з інформаційної, наукової та науково-методичної точок зору, хоча на дисертаційному рівні проблеми криміналістичного забезпечення слідчої практики розглядалися ще в 1983 р. [375].

Стосовно інформаційного забезпечення назвемо дисертаційні дослідження українських криміналістів К.І. Бєлякова [376], В.І. Ґалаґана [377], Н.С. Карпова [378]; та науковці, які дещо змінили напрямки своїх наукових пошуків, — В.Я. Лукашенка [379], Ю.В. Попова [380], П.В. Цимбала [381], Відзначимо також докторську дисертацію азербайджанського вченого Д.І. Сулейманова [382].

К.І. Бєляков, зокрема, висвітлив теорію й практику інформаційного забезпечення розслідування злочинів, зупинившись при ньому на інформаційному аспекті процесу розслідування, методах і засобах його інформаційного забезпечення, можливостях застосування АІС у слідчій практиці. Однак вивчення цих проблем фактично слугувало основою розробки питання про можливість побудови автоматизованих інформаційно-логічних систем інформаційного забезпечення розслідування.

Робота В.І. Галагана присвячена проблемам використання слідчим інформації на початковому етапі розслідування, для нього схарактеризовані наявні на цьому етапі інформаційні процеси, окреслені методи аналізу та оцінки отриманої інформації, визначені на цій основі напрями й форми використання інформації.

У дисертації В.Я. Лукашенка увага зосереджена на теоретичних основах відображення й подання інформації, криміналістичних та правових аспектах її представлення на досудовому слідстві.

Н.С. Карпов дослідив поняття, значення і критерії передового досвіду розкриття і розслідування злочинів, джерела інформації про такий досвід та можливості його вивчення, а також напрями використання досвіду для вдосконалення розкриття й розслідування злочинів.

Ю.В. Попов присвятив свою роботу теоретичним аспектам використання методів інформатики в боротьбі зі злочинністю, питанням удосконалення інформаційних систем і банків даних органів внутрішніх справ, комп'ютеризації робочого місця слідчого для ефективної реалізації концепції автоматизованого інформаційного забезпечення.

П.В. Цимбал розкрив проблему інформаційного забезпечення розслідування, яка розглядалася крізь призму використання науково-технічних досягнень як умови підвищення ефективності слідчої діяльності та визначення на цьому ґрунті шляхів активізації використання науково-технічних засобів.

Д.І. Сулейманов, розглянув криміналістичну характеристику інформації, інформаційні основи розслідування, пошук та дослідження джерел криміналістично значимої інформації.

Разом з тим здебільшого при розгляді проблем інформаційного забезпечення протидії злочинності автори виходять з того, що інформаційне забезпечення розслідування — це оптимальний пошук та використання інформації, яка утворена злочинними діями, розслідування злочинів неможливе без надійних засобів вилучення й дослідження саме цієї інформації. Разом з тим, проблема не вичерпала себе. Новітні інформаційні технології використовуються ОЗУ повсякденно і потребують відповідного оновлення процесу інформаційно-технічного забезпечення діяльності щодо розкриття та розслідування злочинів.

Інформаційне забезпечення є передумовою здійснення оперативно-розшукових заходів. Водночас застосування оперативно-розшукових заходів спрямовано на збирання інформації, тобто інформаційне забезпечення подальшої пізнавальної діяльності слідчого та перетворення інформації в докази. Стратегічними напрямками удосконалення оперативно-розшукової політики на думку Ортинського В.Л. є: розроблення і застосування інноваційних методів, алгоритмів та технологій ОРД; підвищення ефективності роботи конфідентів; покращення інформаційного забезпечення діяльності спеціальних підрозділів у протидії нелегальній економіці; оптимізація взаємодії елементів правоохоронної системи [383, с.7].

Правильно зазначається, що одним з основних напрямів інформаційно-аналітичного забезпечення діяльності ОВС є аналітична розвідка, а відповідно, інформаційно-технічного забезпечення – комп'ютерна розвідка [384].

Перспективним напрямом становлення аналітичної розвідки в підрозділах кримінальної міліції могло б бути використання експертних або інтелектуальних систем з метою аналізу даних і планування операцій. Інформаційно-аналітичне забезпечення оперативно-розшукової функції запо-