directions of activity of subjects providing public safety in Ukraine in modern terms are distinguished.
It is resumed that the indicated activity is sent to realization of such priority tasks: creation of the effective state control after activity of subjects providing public safety system; legislative decision of control-supervisory plenary powers of organs of the state control system; expansion of supervisory plenary powers of public prosecutor office in the field of public safety; increase of role of public inspection after activity of subjects providing public safety.

Keywords: *public safety, aim, task, direction, providing.*

УДК 342.9

О. В. ОЛІЙНИК,
доктор юридичних наук, старший науковий співробітник,
головний консультант Інституту законодавства Верховної Ради України

МЕТОДОЛОГІЧНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЇЇ СКЛАДОВОЇ – ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Проаналізовано методологічні засади забезпечення системи інформаційної безпеки та її складової – захисту інформаційних ресурсів. Розглянуто методи – важливі складові загальної теорії і методології побудови системи захисту інформації. Визначено чинники якими зумовлено практичне застосування методів захисту інформації.

Ключові слова: *інформаційна безпека, методи, захист, інформації, державна таємниця, інформація з обмеженим доступом, національна безпека, інформація.*

Поряд із традиційними загрозами, які діють у сфері формування, зберігання і поширення інформації, інформаційних ресурсів, що підлягають охороні з боку держави, зростає небезпека несанкціонованого втручання в роботу інформаційних систем не тільки з метою отримання охоронюваної інформації, а й порушення її цілісності та знищення, дезорганізації інформаційної системи держави тощо. Все це вимагає не тільки застосування традиційних заходів охорони інформації, інформаційних ресурсів, що містять відомості, віднесені до державної таємниці, іншої інформації з обмеженим доступом та суспільно важливої відкритої інформації, а й розроблення і впровадження заходів і засобів правового, організаційного, інженерно-технічного та криптографічного захисту вказаної інформації, адекватного загрозам інформаційним ресурсам, що підлягають охороні з боку держави у всіх сферах її життєдіяльності.

У сучасних умовах жорсткої конкуренції особливу увагу має бути зосереджено на забезпеченні ефективного захисту інформаційно-інтелектуального ресурсу, високоефективних наукових і конструкторсько-технологічних розробках, які будуть визначальними у соціально-економічному розвитку майбутнього нашого суспільства. При цьому слід зауважити, так як це недопустиме надмірне засекречування в інформаційній сфері, що може призвести до великих економічних та політичних втрат.

Тому аналіз методів захисту інформації є актуальним в умовах розвитку глобалізаційних інформаційних процесів.

Мета статті – відповідно до сучасних реалій і тенденцій визначити й розглянути методологічні підходи формування та вдосконалення захисту інформації.

Методи – важливі складові загальної теорії і методології побудови системи захисту інформації. Ґрунтовні висновки щодо змісту методів захисту інформації, їх систематизації, а також способів забезпечення інформаційної безпеки, серед яких заходи і практичні дії щодо попередження загроз, їх виявлення, локалізації, ліквідації як загроз, так і наслідків їхньої можливої дії, викладено у працях А. А. Шиверського [1, с. 90–96], та І. К. Корнєєва [2, с. 239–242]. Водночас слід нагадати про те, що система захисту інформації має сталу тенденцію до ускладнення. Як відзначено колективом авторів Національного інституту стратегічних досліджень (НІСД), «головним носієм інформації завжди була і є людина, свобода пересування якої є природним правом у демократичних державах. Тому методи захисту інформації повинні виходити з цієї парадигми, а не копіюватися механічно з тоталітарного минулого» [3, с. 129].

Світова і вітчизняна наука свідчать про те, що в сучасних умовах необхідне всебічне знання змістовної сутності різноманітних методів забезпечення безпеки інформації та сфери її обігу, а також активне і цілеспрямоване їх застосування.

Під методами захисту інформації будемо розуміти способи (процедури, операції, заходи) формування і забезпечення чіткого функціонування загальної комплексної системи захисту інформації та складових її частин, що створюють умови для попередження, усунення (нейтралізації) або послаблення загрози інформації та сфері її обігу.

Розглянемо загальнобазові (універсальні) методи захисту інформації.

Метод регламентації процесів захисту інформації полягає у визначенні правовими нормами умов, за яких може здійснюватися діяльність, пов'язана з інформацією з обмеженим доступом, що є власністю держави.

В умовах роздержавлення власності і формування багатоукладненої економіки цей метод дозволяє сформувати належні умови для захисту інформації. Законом України «Про державну таємницю» з цією метою введено дозвільний порядок провадження діяльності, пов'язаної з державною таємницею. Визначено, що дозвіл на провадження такого виду діяльності надається органам державної влади, органам місцевого самоврядування, підприємствам, установам, організаціям за результатами спеціальної експертизи, вимоги щодо змісту якої встановлені Законом [4, ст. 20].

На рівні Закону регламентуються також умови, за яких в автоматизованих системах має оброблятися інформація, що є власністю держави, або інформація, захист якої гарантується державою. Такими обов'язковими умовами є наявність атестата захищеності системи, її відповідності роботі з певною категорією інформації з обмеженим доступом [5].

Стосовно інформації, яка є приватною власністю фізичних та юридичних осіб, у процесі їх взаємовідносин з іншими суб'єктами інформаційної діяльності регламентація процесів захисту інформації здійснюється її власниками.

Метод регламентації процесів захисту інформації сприятиме як формуванню загальної комплексної системи захисту інформації, так і її складових та окремих елементів на підставі норм, правил, регламентів діяльності спеціальних підрозділів і служб, що реалізують функції захисту інформації, повноваження користувачів на доступ до відповідної інформації та її захист тощо. Отже, реалізація цього методу забезпечується законодавчими актами, загальнодержавними, відомчими і внутрішніми нормативно-правовими документами. В процесі міжнародного співробітництва реалізація методу регламентації процесів захисту інформації здійснюється відповідно до національних законодавств та згідно із зобов'язаннями сторін щодо захисту інформації та її носіїв, якими обмінюються партнери, що визначається відповідними угодами та спільно узгодженими критеріями і процедурами.

Метод приховування інформації та процесу обігу відомостей, що підлягають захисту, як свідчить практика та висновки дослідників [1, с. 63], є найбільш поширеним, він застосовується в усіх елементах системи захисту. Практична реалізація цього методу забезпечується:

– встановленням обмежень доступу, тобто ступенів секретності та конфіденційності інформації;

– обігом інформації тільки в умовах, обмежених режимними, конфіденційними заходами;

– зберіганням традиційних носіїв інформації з обмеженим доступом у спеціальних сховищах, можливість доступу сторонніх осіб до яких виключена;

– застосуванням інженерно-технічних засобів захисту, засобів кодування і шифрування інформації у процесі її обробки, передавання інформаційно-телекомунікаційними каналами, каналами зв'язку та в період зберігання в електронних базах і банках даних;

– застосуванням організаційних, організаційно-технічних та інженерно-технічних заходів для усунення світлових, звукових, хімічних, електромагнітних тощо демаскуючих ознак носіїв інформації з обмеженим доступом, а також захисту технічних каналів від можливого витоку такої інформації.

У цивілізованих міжнародних відносинах, пов'язаних із використанням інформації з обмеженим доступом, відкритість і секретність не суперечать одна одній. Приховування інформації та процесу її обігу – це метод, застосування якого у процесі міжнародного інформаційного співробітництва вважається легітимним, якщо обмеження доступу до певних видів інформації встановлено національними законами. Важливою при цьому є необхідність виконання зобов'язань, визначених міжнародними домовленостями (двосторонніми чи багатосторонніми угодами) з питань захисту інформації, а також досягнення взаємної упевненості про надійність методів, що

застосовуються сторонами для захисту інформації та її носіїв, якими вони обмінюються у процесі співробітництва.

Метод обмеження доступу до інформації та процесу її обігу полягає у розподілі відомостей за ознаками ступеня секретності та конфіденційності («особливої важливості», «цілком таємна», «таємна», «для службового користування» тощо), у наданні права доступу до інформації відповідного ступеня секретності згідно з певною формою допуску [4, ст. 22].

Реалізація методу обмеження доступу до інформації, що має гриф «для службового користування», та процесу обігу такої інформації здійснюється керівниками державних органів, підприємств, установ і організацій відповідно до встановлених регламентів [6, п. 6]. Порядок обмеження доступу до конфіденційної інформації, що є власністю окремих фізичних та юридичних осіб, встановлюють власники цієї інформації [7, ст. 30].

Застосування цього методу захисту інформації у процесі міжнародного інформаційного співробітництва здійснюється на підставі взаємно узгоджених сторонами угод, що укладаються з питань захисту інформації, ступеня секретності (конфіденційності) інформації.

Метод роздроблення (розчленування) інформації та процесів її обігу полягає в наданні доступу до інформації з обмеженим доступом (доведення, ознайомлення) користувачам лише в тій частині інформації, яка безпосередньо необхідна для виконання покладених на них завдань. Застосування цього методу дозволяє забезпечити комплексний захист усіх елементів певної сфери діяльності, об'єкта, що містять відомості обмеженого доступу. Головними вимогами методу роздроблення (розчленування) інформації та процесів її обігу є те, щоб знання користувачем частини відомостей, яка необхідна йому для виконання завдання, не давало повного уявлення про сферу діяльності або про об'єкт у цілому.

Особливе значення має застосування методу роздроблення (розчленування) інформації для захисту інтересів і прав суб'єктів України у процесі міжнародного співробітництва з використанням відомостей обмеженого доступу. Необхідність цього зумовлена реаліями сучасності: «Спостерігається нав'язування іноземними контрагентами несправедливих умов договорів, наприклад, вимог про передачу прав не тільки на інтелектуальну власність, що створюється під час реалізації контракту, й на попередні розробки, а також вимог в однобічному порядку безкоштовно передавати покупцеві удосконалення предмета ліцензії. З такими проблемами раніше зустрілися країни, які розвиваються, що викликало необхідність розробки в рамках ООН проекту Міжнародного кодексу поведінки у галузі передачі технологій, а також введення в законодавство багатьох країн (Корея, Індія, Бразилія, Франція, Польща, Греція та ін.) спеціальних норм, що перешкоджають укладанню несправедливих договорів» [8, с. 19].

Отже, роздроблення (розчленування) інформації можна вважати одним із найважливіших методів захисту прав суб'єктів України на інформацію з обмеженим доступом та забезпечення рівноправного співробітництва з іноземними партнерами в цій сфері. Надання іноземним партнерам права доступу лише до інформації, яка є предметом угоди або контракту, створюватиме умови для припинення виконання деякими суб'єктами України «донорської ролі» щодо безкоштовної передачі як виконаних, так і майбутніх результатів наукових досліджень і розробок, що містять відомості обмеженого доступу.

Метод дезінформування у процесі захисту інформації та її носіїв полягає у свідомому поширенні фальшивої (викривленої) інформації стосовно деяких сфер діяльності, об'єктів, виробів, а також стану справ на окремих ділянках роботи.

Відповідно до висновків колективу авторів НІСД «головним методом захисту важливої інформації має бути ... конкретна інформаційна контргра щодо намірів, а не результатів їхнього втілення. Ця контргра має вестися на зразок різних суперечливих повідомлень (тобто дезінформація), оскільки важливу для національної безпеки інформацію неможливо захистити загальними засобами» [3, с. 129].

Метод дезінформування широко застосовується для захисту відповідної інформації у світовій практиці. Цей метод активно використовувався в радянські часи для легендування підприємств, установ, організацій, напрямів досліджень, розробок, промислового виробництва, пов'язаних з державною таємницею, яким надавалися умовні назви, шифри, коди тощо. Дезінформування (легендування) здійснювалося на підставі відповідних нормативно визначених правил і вимог. Підхід до цих питань, що було характерним для радянських часів, передбачав тоталітарну засекреченість. Безумовно, в сучасних умовах таке ставлення до

дезінформування з метою захисту інформації не може бути прийнятним.

Водночас слід підкреслити, що для забезпечення захисту важливої для національної безпеки інформації дезінформування є не тільки виправданим, а й необхідним методом приховування реальних напрямів діяльності. Особливо воно важливе у питаннях зовнішньополітичних і зовнішньоекономічних відносин, розголошення яких розкриває стратегію і тактику зовнішньої політики України. Метод дезінформування також може бути використаний спільно з іноземними партнерами стосовно договорів або їх окремих статей, які відповідно до взаємних домовленостей прийнято рішення зберігати в таємниці на весь час дії цих договорів чи на певний проміжок часу.

Метод системного обліку інформації з обмеженим доступом і процесу її автоматизованої обробки як метод захисту інформації з обмеженим доступом найбільш поширений у практичній діяльності і застосовується на всіх етапах роботи з такою інформацією, починаючи від етапу її виготовлення (розроблення) до її знищення або зняття обмежень доступу.

Основними вимогами методу системного обліку інформації з обмеженим доступом і процесу її автоматизованої обробки є такі:

– обов'язкова реєстрація усіх носіїв інформації з обмеженим доступом: паперових, магнітних, а також самих виробів;

– одноразовість реєстрації, тобто кожний носій такої інформації використовується лише за номером, наданим відповідно до основної форми обліку згідно з датою його реєстрації;

– відображення в облікових даних користувача (адресата), у якого у цей час перебуває документ (інший носій інформації), а також усіх попередніх користувачів цього носія закритої інформації із зазначенням дати його отримання і повернення;

– здійснення розробки (виготовлення) інформації, що підлягає захисту, тільки на зареєстрованих паперових або магнітних носіях;

– здійснення реєстрації всіх дій щодо автоматизованої обробки інформації з обмеженим доступом в облікових документах автоматизованого робочого місця (АРМ) та в автоматизованій системі (комп'ютері) із зазначенням посадової особи (користувача), часу обробки інформації, реквізиту розробленого, отриманого, переданого, розміщеного в базі (банку) даних або в інший спосіб використаного документа (інформації на магнітному носії), а також реквізитів джерела (паперового, магнітного носія), на основі якого розроблявся новий документ (інформація) з грифом обмеження доступу.

Наведений метод дозволяє: забезпечувати персональну відповідальність розробника і користувача носіїв інформації з обмеженим доступом за їх зберігання; в будь-який час встановити місцезнаходження носія вказаної інформації; створювати умови, за яких виключається можливість знеособлення носіїв секретної та конфіденційної інформації.

Метод підвищення ефективності людського фактора у сфері захисту інформації набуває особливої актуальності в сучасних умовах. Лібералізація економічних відносин, широкий розвиток міжнародного співробітництва значно загострили суперечності між потребами суб'єктів України у вільному обміні інформацією та необхідністю додержання певних обмежень на її поширення. Як свідчать сучасні реалії, в окремих випадках зазначені суперечності загострюються штучно через недостатню обізнаність учасників інформаційних відносин щодо порядку і правил, прав і обов'язків у сфері обміну інформацією та її захисту.

Реалізація наведеного методу потребує проведення єдиної державної політики і скоординованої діяльності державних органів та освітніх установ, що здійснюють підготовку та підвищення кваліфікації кадрів, і чіткого визначення функцій державних органів, які здійснюють управління освітою в галузі захисту інформації та координацію цієї діяльності; впровадження освітніх стандартів, що встановлюють єдині вимоги до підготовки спеціалістів з питань інформаційної безпеки та захисту інформації. Важливим елементом системи освітньої підготовки і підвищення кваліфікації має стати виховання інформаційно-правової культури – правової свідомості у сфері інформаційних відносин та інформаційної безпеки. Інформаційно-правову культуру та правову свідомість доцільно розглядати як один з головних факторів підвищення ефективності людського фактора в сфері захисту інформації. Потребують вдосконалення: система профілактично-запобіжної роботи з посадовими особами і громадянами, діяльність яких пов'язана з інформацією з обмеженим доступом; рівень галузевого і відомчого контролю; практика морального і матеріального стимулювання позитивних результатів у сфері захисту інформації.

Метод створення фізичних і технічних перешкод на шляху зловмисника до інформації,

що захищається, полягає у здійсненні нижченаведених заходів.

1. Організація фізичної охорони як складової внутрішньооб'єктового режиму секретності (конфіденційності). Головна мета цих заходів – виключити можливість таємного проникнення на територію й у приміщення сторонніх осіб; забезпечити контроль проходу у переміщення працівників і відвідувачів та їх перебування на території, що охороняється. За необхідності можуть створюватися окремі режимні (конфіденційні) виробничі зони або приміщення з відповідною системою перепускного режиму і контролю працівників і відвідувачів [9, с. 49–50].

2. Застосування різноманітних механічних, електромеханічних, електронних, електронно-оптичних, радіо і радіотехнічних та інших систем і обладнання для створення кількох рубежів охорони режимних об'єктів. Відповідно до тактичного призначення охоронні системи і обладнання застосовуються для охорони периметрів об'єктів, службових і складських приміщень, сейфів тощо, тобто створюються декілька рубежів охорони з урахуванням ступенів важливості різних частин об'єкта з точки зору нанесення можливих збитків від різного виду загроз. Оптимальне розташування на відповідних рубежах охорони ефективних технічних засобів виявлення, запобігання, перешкоджання та усунення наслідків можливих протиправних дій становить основу інженерно-технічного захисту об'єкта, на якому виконуються роботи, що містять інформацію обмеженого доступу.

3. Специфічною сферою є застосування методу фізичних і технічних перешкод на шляху зловмисника до інформації, що обробляється, зберігається і циркулює в комп'ютерах, інформаційно-телекомунікаційних системах і мережах. Цей метод передбачає впровадження комплексу заходів захисту інформації, які неможливо вирішити апаратними, програмними і криптографічними засобами. Комплекс включає організаційні, організаційно-правові та організаційно-технічні запобіжні заходи, які дозволяють відвернути несанкціонований доступ зловмисників до технічних засобів обробки інформації та уникнути недбалості персоналу і користувачів.

Метод колегіальності контролю за додержанням режиму секретності (конфіденційності) – один із важливих методів забезпечення збереження документів, інших носіїв секретної і конфіденційної інформації та встановленого порядку обробки інформації, в тому числі і з використанням технічних засобів та автоматизованих систем.

Застосування названого методу передбачає проведення колегіальних (комісійних) перевірок додержання режиму секретності (конфіденційності): внутрішньооб'єктових, тобто в центральних апаратах державних органів, на підприємствах, установах і організаціях – у строки, визначені нормативними документами; галузевих, відомчих, загальнодержавних (здійснюються спеціально уповноваженим органом державної влади у сфері охорони державної таємниці) – у строки, визначені відповідними керівниками. Обов'язок контролювати стан охорони державної таємниці чинним законодавством покладено на органи державної влади, органи місцевого самоврядування, підприємства, установи й організації, що розміщують у підрядників замовлення, пов'язані з державною таємницею [4, ст. 37]. Контроль за нерозголошенням відомостей, що містяться у документах з грифом «Для службового користування», здійснюється режимно-секретними підрозділами установ і організацій відповідно до рішень їх керівників [6, п. 7].

Окремим напрямом колегіального внутрішньооб'єктового контролю можуть бути перевірки дотримання організаційних, організаційно-правових, організаційно-технічних та інженерно-технічних заходів захисту інформації в технічних засобах обробки інформації та автоматизованих системах.

Галузевий, відомчий, загальнодержавний контроль може здійснюватися у вигляді комплексних, цільових та тематичних перевірок додержання режиму секретності та конфіденційності.

Комплексні перевірки передбачають здійснення у повному обсязі контролю за додержанням на об'єкті, що перевіряється, чинного законодавства, загальнодержавних, відомчих і внутрішніх нормативно-правових документів щодо встановленого порядку і правил охорони державної таємниці та іншої інформації з обмеженим доступом.

Цільові перевірки передбачають здійснення контролю на окремих напрямах діяльності, пов'язаної з державною таємницею та іншою інформацією з обмеженим доступом.

Тематичні перевірки передбачають здійснення контролю за додержанням режиму секретності (конфіденційності) щодо конкретних тем робіт, пов'язаних з державною таємницею та іншою інформацією з обмеженим доступом.

Відповідно до світової практики може здійснюватися взаємний контроль у процесі міжнародного співробітництва з використанням інформації з обмеженим доступом та її носіїв, згідно з узгодженими строками, для досягнення впевненості у створенні партнерами умов, що забезпечують зберігання і використання отриманої (переданої) інформації та її носіїв, як встановлено зобов'язаннями сторін.

Зазначимо, що практичне застосування методів захисту інформації завжди зумовлене: важливістю інформації та її носіїв (ступенями секретності, конфіденційності); реальними та потенційними загрозами для конкретного виду інформації з обмеженим доступом; умовами розташування режимних об'єктів, службових приміщень, технічних засобів обробки інформації та робочих місць працівників, діяльність яких пов'язана з державною таємницею та іншою інформацією з обмеженим доступом. Отже, наведені методи використовуються для створення і забезпечення функціонування системи захисту інформації безпосередньо в державних органах, на підприємствах, установах і організаціях, де створюється (розробляється), використовується, пересилається та в інший спосіб відбувається циркуляція інформації, віднесеної до державної таємниці та до іншої інформації з обмеженим доступом.

Необхідність визначення політичних, правових, методологічних і в цілому концептуальних засад удосконалення захисту інформаційних ресурсів на сьогодні стає надзвичайно актуальною науковою проблемою.

Список використаних джерел

1. Шиверский А. А. Защита информации: проблемы теории и практики / А. А. Шиверский. – М. : Юристъ, 1996. – 112 с.

2. Степанов Е. А. Информационная безопасность и защита информации : учеб. пособие / Е. А. Степанов, И. К. Корнеев. – М. : Инфра-М, 2001. – 304 с. – (Сер. «Высш. образование»).

3. Національна безпека України 1994–1996 рр. : наук. доп. НІСД / редкол. : О. Ф. Бєлов (голова) та ін. – Київ : НІСД, 1997. – 200 с. – (Сер. «Загальноін-тські доп.»)

4. Про державну таємницю : закон України від 31 трав. 2005 р. № 2594-IV // Голос України. – 1999. – 26 жовт.

5. Про захист інформації в автоматизованих системах : закон України // Інформаційні технології. Нормативна база. – Київ : КНТ, 2005. – С. 71–77.

6. Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави : затв. постановою Кабінету Міністрів України від 27 листоп. 1998 р. № 1893 : із змінами та допов. // Інформаційні технології. Нормативна база. – Київ : КНТ, 2005. – 500 с.

7. Про інформацію : закон України від 2 жовт. 1992 р. № 2657-XII // Голос України. – 2011. – 19 лют.

8. Шпак А. П. Передача технологій в Україні: ситуація і проблеми / А. П. Шпак // Наука та наукознавство. – 2000. – № 1–2. – С. 14–20.

9. Ярочкин В. И. Информационная безопасность: учеб. пособие / В. И. Ярочкин. – М. : Междунар. отношения, 2000. – 400 с.

Надійшла до редколегії 01.04.2014

ОЛЕЙНИК О. В. МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЕЁ СОСТАВЛЯЮЩЕЙ – ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Проанализированы методологические основы обеспечения системы информационной безопасности и её составляющей – защиты информационных ресурсов. Рассмотрены методы – важные составляющие общей теории и методологии построения системы защиты информации. Определены факторы, которыми обусловлено практические применения методов защиты информации.

Ключевые слова: *информационная безопасность, методы, защита, информации, государственная тайна, информация с ограниченным доступом, национальная безопасность, информация.*

OLIINYK O. V. METHODOLOGICAL ESSENTIAL PRINCIPLES OF PROMOTION SYSTEM OF INFORMATIONAL SECURITY AND ITS COMPONENT – SECURITY OF INFORMATIONAL RESOURCES

The author analyses methodological aspects of promotion system of informational security and its component – security of informational resources, the methods of information protection – the most important elements of general theory and methodology of development of information protection systems – are analyzed.

The author examines methods of information protection and systematizes them, as well as means of maintenance of informational security, in particular measures aimed at prevention of threats to the informational security, their identification, localization and elimination. The author emphasizes that the system of information security tends to be more complex. It is highlighted that foreign and domestic scientific thought provides that today the comprehensive knowledge of the essence of various methods of maintaining the security of information and the sphere of its circulation is required.

The author considers that the methods of informational security may be defined as procedures of formation and maintenance of clearly functioning general comprehensive system of informational security and its components, which are aimed at prevention, elimination (neutralization) and weakening of threats to information.

The general (universal) methods of information protection are analyzed, in particular: the method of regulation of information protection processes, the method of hiding the information and the processes of circulation of data, which require protection, the method of disintegration of information and the processes of its circulation, the method of disinformation, the method of systematic record of information with restricted access and its automatic processing, the method of increasing the efficiency of human factor in information protection, the method of creation of physical and technical barriers to prevent the perpetrator to access the information under protection, the method of collegiality aimed at control of maintaining the secrecy, etc.

The author concludes that application of methods of information protection is always caused by such reasons: the importance of information and its carriers (the level of secrecy and confidentiality), real and potential threats to specific information with restricted access, the location of secrecy objects, office premises, technical means of information processing and workplaces of employees whose activity is related to state secrets and other information with restricted access. Thus abovementioned methods are applied to create and maintain the proper functioning of information protection system directly at the governmental bodies, enterprises and organizations, where the state secret or other information with restricted access is being created (developed), used, transmitted and in any other way circulated.

Keywords: *information security, methods, information protection, state secret, information with restricted access, national security, information.*

УДК [343.37:665.71](477)

І. А. ПЕТРОВА,
доктор юридичних наук, доцент,
начальник кафедри інформаційної та економічної безпеки навчально-наукового інституту підготовки фахівців для підрозділів кримінальної міліції
Харківського національного університету внутрішніх справ

ОСОБЛИВОСТІ ВИЯВЛЕННЯ ПРАВООХОРОНЦЯМИ ЗЛОВЖИВАНЬ ПРИ ОБІГУ НАФТОПРОДУКТІВ

Розглянуто питання викриття працівниками правоохоронних органів основних джерел створення надлишків нафтопродуктів та шляхи їх фальсифікації з метою обману споживачів і отримання незаконних прибутків. Розроблено рекомендації щодо встановлення жорсткого контролю за кількісним та якісним складом нафтопродуктів на нафтобазах, складах, автозаправних станціях під час їх прийому, зберігання та реалізації.

Ключові слова: *нафтопродукти, фальсифікація, пересортиця, невраховані надлишки, нафтобази, автозаправні станції.*

В умовах сьогодення ефективна боротьба з економічними злочинами стає запорукою економічної безпеки держави. Не останнє місце у такій боротьбі займає виявлення фальсифікованої продукції, яка створюється для отримання незаконних прибутків і у великій кількості постачається на український ринок. Одним із різновидів продукції підвищеного попиту є нафтопродукти, які також часто фальсифікують, щоб отримати незаконні доходи у процесі їхнього обігу. Така ситуація притаманна не тільки представникам великого бізнесу, є бажання отримувати доходи без сплати податків у середнього і малого бізнесу, який сам може і