УДК 343.2.7

Брягін О.В.,. Розорінов Г.М.

ЗАХИСТ ІНФОРМАЦІЇ В УМОВАХ ДІЇ КРИМІНАЛЬНОГО ПРОЦЕСУАЛЬНОГО КОДЕКСУ УКРАЇНИ

Розглядаються питання захисту інформації спеціально змодельованого суб'єкта інформаційної діяльності в умовах дії Кримінального процесуального кодексу України та оновлених положень Закону України "Про оперативно-розшукову діяльність". Визначено основні якісні та кількісні зміни у моделі загроз. Головна увага приділяється побудові системи захисту інформації суб'єкта інформаційної діяльності у запропонованих обмеженнях. Запропоновано алгоритм дій щодо забезпечення захисту інформації в умовах дії загроз, що можуть виникати в результаті проведення негласних слідчих (розшукових) дій, або інших дій, що містять ознаки втручання у приватне спілкування.

Ключові слова: суб'єкт інформаційної діяльності, захист інформації, оперативно-розшукова діяльність.

Вступ. Загальновідомою диспозицією двох типів суб'єктів інформаційних відносин, які здійснюють свою діяльність у галузях організації та здійснення несанкціонованого власником доступу до інформаційних повідомлень (суб'єкти 1-го типу), та забезпеченням захисту від такого доступу (суб'єкти 2-го типу), є лідируюча, активна позиція перших по відношенню до других. Іншими словами, спочатку суб'єктом 1-го типу генерується новий вид загрози, через деякий час суть загрози має стати відомою суб'єктам 2-го типу, потім ця загроза включається у модель загроз, потім відбувається розробка систем та технічних заходів протидії, коригування технічного завдання та плану технічного захисту інформації. Після цього знову створюється новий тип загрози та реалізується черговий цикл захисту. На сьогодні є не спростованим факт, що саме на таких засадах відбувається розвиток ринку технологій і засобів негласного доступу та протидії такому. Своєрідним підтвердженням цього є певна схожість переліків господарюючих суб'єктів, які мають ліцензії на розроблення, виготовлення спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації та торгівлю цими засобами [1], що є інструментарієм суб'єктів 1-го типу, з переліком суб'єктів господарювання, які мають ліцензії на провадження господарської діяльності з надання послуг в галузі технічного захисту інформації [2], які є, за суттю, переліком легальних суб'єктів 2-го типу. Важливою особливістю для подальшого викладення є те, що питання організації негласного доступу у встановленому законом порядку є питанням державного рівня [3].

Дана стаття присвячена аналізу можливих змін у стратегії захисту інформації, пов'язаних з введенням у дію Кримінального процесуального кодексу України.

Основна частина. Розглянемо правовий аспект проблеми. Конституцією України встановлені основні передумови виникнення та практичної реалізації права окремих суб'єктів на тимчасове обмеження приватності, у тому числі - таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції. До введення у дію Кримінального процесуального кодексу (КПК) України та внесення відповідних змін до Закону України "Про оперативно-розшукову діяльність" зазначеними суб'єктами виступали виключно суб'єкти оперативно-розшукової діяльності (ОРД), які були визначені статтею 5 згаданого Закону. Слід зазначити, що буквальне визначення відповідного права суб'єктів ОРД не зовсім відповідало термінології Конституції України, – суб'єктам ОРД надавалося право "зняття інформації з каналів зв'язку, застосування інших технічних засобів отримання інформації", безпосереднього права прослуховувати телефонні розмови громадянина шляхом тимчасового обмеження його конституційного права за дозволом суду законодавцем передбачено не було. Хоча, слід зазначити, що в аналогічному федеральному законі Російської Федерації визначене саме таке право [4].

З введенням у дію КПК перелік легальних суб'єктів 1-го типу, які мають право втручатися у приватне спілкування шляхом проведення негласних слідчих (розшукових) дій (НСРД) розширено, - крім суб'єктів ОРД право проводити НСРД надано слідчим, які

здійснюють досудове розслідування, а за рішенням слідчого чи прокурора до проведення негласних слідчих (розшукових) дій можуть залучатися також інші особи (п. 6 ст. 246 КПК).

Пропонуємо порівняти змінені обсяги повноважень з негласного доступу до інформації у зв'язку з введенням у дію КПК. Дані наведенні у Таблиці 1.

Обсяги повноважень з негласного доступу до інформації Таблиця 1

Захід та його суть (на основі чинних на той час нормативно-правових актів)	**Визначений законодавством суб'єкт заходу**
1	**2**
До 19.11.2012	
Негласне виявляння та фіксування слідів тяжкого або особливо тяжкого злочину, документів та інших предметів, що можуть бути доказами підготовки або вчинення такого злочину, чи одержувати розвідувальну інформацію, у тому числі шляхом проникнення оперативного працівника в приміщення, транспортні засоби, на земельні ділянки.	тільки суб'єкти ОРД
Зняття інформації з каналів зв'язку, застосовування інших технічних засобів отримання інформації.	тільки суб'єкти ОРД
Контроль шляхом відбору за окремими ознаками телеграфно-поштових відправлень	тільки суб'єкти ОРД
Здійснення візуального спостереження в громадських місцях із застосуванням фото-, кіно- і відеозйомки, оптичних та радіоприладів, інших технічних засобів	тільки суб'єкти ОРД
Після 19.11.2012	
Тимчасовий доступ до речей і документів, які містять охоронювану законом таємницю (інформація, якою володіють ЗМІ, лікарська, нотаріальна, комерційна, банківська таємниці, особисте листування, інформація, яка знаходиться в операторів та провайдерів телекомунікацій, персональні данні, державна таємниця), глава 15 КПК	Сторони кримінального провадження за ухвалою слідчого судді, глава 15 КПК
Обстеження публічно недоступних місць, житла чи іншого володіння особи з метою: 1) виявлення і фіксації слідів вчинення тяжкого або особливо тяжкого злочину, речей і документів, що мають значення для їх досудового розслідування; 2) виготовлення копій чи зразків зазначених речей і документів; 3) виявлення та вилучення зразків для дослідження під час досудового розслідування тяжкого або особливо тяжкого злочину; 4) виявлення осіб, які розшукуються; 5) встановлення технічних засобів аудіо-, відеоконтролю особи, ст. 267 КПК	Слідчий, або за його дорученням – суб'єкти ОРД. За рішенням слідчого чи прокурора до проведення НСРД дій можуть залучатися також інші особи, ст. 246 КПК; суб'єкти ОРД самостійно.
Аудіо-, відеоконтроль особи, ст. 260 КПК.	зазначені вище суб'єкти
Накладення арешту на кореспонденцію особи без її відома, ст. 261 КПК.	зазначені вище суб'єкти
Огляд і виїмка кореспонденції, ст. 262 КПК.	зазначені вище суб'єкти

Продовження Таблиці 1

1	2
Зняття інформації з транспортних телекомунікаційних мереж (мереж, що забезпечують передавання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого виду між підключеними до неї телекомунікаційними мережами доступу, ст. 263 КПК.	зазначені вище суб'єкти
Зняття інформації з електронних інформаційних систем, - пошук, виявлення і фіксація відомостей, що містяться в електронній інформаційній системі або їх частин, доступ до електронної інформаційної системи або її частини, а також отримання таких відомостей без відома її власника, володільця або утримувача, ст. 264 КПК.	зазначені вище суб'єкти
Установлення місцезнаходження радіоелектронного засобу є негласною слідчою (розшуковою) дією, яка полягає в застосуванні технічних засобів для локалізації місцезнаходження радіоелектронного засобу, у тому числі мобільного терміналу систем зв'язку, та інших радіовипромінювальних пристроїв, активованих у мережах операторів рухомого (мобільного) зв'язку, ст. 268 КПК.	зазначені вище суб'єкти
Спостереження за особою, річчю або місцем для пошуку, фіксації і перевірки під час досудового розслідування тяжкого або особливо тяжкого злочину відомостей про особу та її поведінку або тих, з ким ця особа контактує, або певної речі чи місця у публічно доступних місцях, ст. 269 КПК.	зазначені вище суб'єкти
Аудіо-, відеоконтроль місця може здійснюватися під час досудового розслідування тяжкого або особливо тяжкого злочину і полягає у здійсненні прихованої фіксації відомостей за допомогою аудіо-, відеозапису всередині публічно доступних місць, без відома їх власника, володільця або присутніх у цьому місці осіб, ст. 270.	зазначені вище суб'єкти
Контроль за вчиненням злочину, ст. 271 КПК.	зазначені вище суб'єкти
Отримання відомостей, речей і документів, які мають значення для досудового розслідування, особою, яка відповідно до закону виконує спеціальне завдання, беручи участь в організованій групі чи злочинній організації, або є учасником зазначеної групи чи організації, який на конфіденційній основі співпрацює з органами досудового розслідування, ст. 272 КПК.	зазначені вище суб'єкти
Негласне отримання зразків для порівняльного дослідження, ст. 274 КПК.	зазначені вище суб'єкти

Слід зазначити про наявність певних розбіжностей у формулюваннях суті деяких НСРД та відповідних оперативно-технічних заходів та про додаткову можливість ініціювати проведення НСРД стороною захисту та потерпілим. Формальне розширення повноважень, не виключено, спричинене деталізацією наведеного раніш вислову "застосування інших технічних засобів отримання інформації".

Проте принциповими питаннями для подальшого розгляду у даній роботі є розширення переліку легальних суб'єктів 1-го типу і об'єктивно існуюча державна підтримка їх зусиль

щодо негласного отримання різновидів інформації, що може містити докази скоєння злочину.

Розглянемо тепер необхідні умови для набуття прав законного втручання у приватне спілкування. Права зазначених суб'єктів 1-го типу вступають в силу за наступних умов.

Слідчі, суб'єкти ОРД (за дорученням слідчого), інші особи (за рішенням слідчого, прокурора) набувають відповідних прав за таких необхідних умов (перелік не є повним):

1) наявність розпочатого кримінального провадження, що у свою чергу (ст. 214 КПК) передбачає наявність заяви, повідомлення про вчинене кримінальне правопорушення або самостійне виявлення слідчим, прокурором з будь-якого джерела обставин, що можуть свідчити про вчинення кримінального правопорушення;

2) обґрунтування того, що необхідну інформацію неможливо отримати в інший спосіб;

3) обґрунтування того, що під час проведення НСРД можливо отримати докази, які самостійно або в сукупності з іншими доказами можуть мати суттєве значення для з'ясування обставин злочину або встановлення осіб, які його вчинили.

Суб'єкти ОРД набувають прав за наступних обставин (перелік не є повним):

наявність достатньої інформації, одержаної в установленому законом порядку, що потребує перевірки за допомогою оперативно-розшукових заходів і засобів, про:

1) злочини, що готуються;

2) осіб, які готують вчинення злочину;

3) осіб, які переховуються від органів досудового розслідування, слідчого судді, суду або ухиляються від відбування кримінального покарання;

4) осіб безвісно відсутніх;

5) розвідувально-підривну діяльність спецслужб іноземних держав, організацій та окремих осіб проти України;

6) реальну загрозу життю, здоров'ю, житлу, майну працівників суду і правоохоронних органів у зв'язку з їх службовою діяльністю, а також осіб, які беруть участь у кримінальному судочинстві, членів їх сімей та близьких родичів, з метою створення необхідних умов для належного відправлення правосуддя; співробітників розвідувальних органів України у зв'язку із службовою діяльністю цих осіб, їх близьких родичів, а також осіб, які конфіденційно співробітничають або співробітничали з розвідувальними органами України, та членів їх сімей з метою належного здійснення розвідувальної діяльності.

Зазначені підстави можуть міститися в заявах, повідомленнях громадян, посадових осіб, громадських організацій, засобів масової інформації, у письмових дорученнях і постановах слідчого, вказівках прокурора, ухвалах слідчого судді, суду, матеріалах правоохоронних органів, у запитах і повідомленнях правоохоронних органів інших держав тощо (ст. 6 Закону України «Про оперативно-розшукову діяльність»).

На даному етапі викладення позицію та сферу діяльності легальних суб'єктів 1-го типу можливо вважати окресленими:

1) за наявності інформації (як мінімуму – заяви громадянина N) про скоєння об'єктом "X" злочину або про підготовку до скоєння злочину, легальні суб'єкти 1-го типу при підтримці держави можуть втручатися у приватне спілкування осіб, більш-менш детальна суть яких зазначена у главі 21 КПК та частині першій ст. 8 Закону України "Про оперативно-розшукову діяльність";

2) ініціатором втручання у приватне спілкування виступає конкретна людина, – слідчий, керівник оперативного підрозділу, сторона захисту;

3) такий результат втручання у приватне спілкування, як отримання доказів злочину, не є єдино можливим, іншим результатом може бути неможливість отримання таких доказів, наприклад, у випадках:

- недостовірності первинної інформації про кримінальне правопорушення або про підготовку до злочину;
- прорахунків у діяльності легальних суб'єктів 1-го типу та інших "ланцюгів" сторони обвинувачення;

- наявності на об’єкті "Х" системи захисту інформації, яка унеможливлює застосування арсеналу НСРД;

наявності обставин непереборної сили, що унеможливили отримання доказів.

Змін у позиції нелегальних суб’єктів 1-го типу, пов’язаних з введенням в дію КПК, вірогідно слід очікувати лише тих, що пов’язані з перерозподілом сил і засобів серед легальних суб’єктів 1-го типу (вихід на пенсію фахівців – носіїв спеціальних знань та технологій у галузі втручання у приватне спілкування, формальний перехід фахівців нелегальних суб’єктів 1-го типу на службу до легальних тощо), появою на нелегальному ринку технологій, технічних, програмних та програмно-апаратних засобів, що створюватимуться для проведення НСРД та можливою реалізацією загроз системного характеру, наведених, наприклад, в [5].

Змоделюємо у зазначених вище умовах існування суб’єкта інформаційних відносин, діяльність якого відбувається за абсолютно легальних, законних підстав, з дотриманням всіх передбачених законодавством вимог, – ідеального суб’єкта інформаційних відносин (ІСІВ).

Системно вирішуючи питання захисту власної інформації від несанкціонованого доступу, ІСІВ може прийняти одне з двох рішень:

1. Захист інформації не потрібний.

2. Захист інформації є необхідним.

Оскільки рішення першого типу можуть приймати лише особи, які не мають інстинкту самозбереження, або особи, не обізнані з основами і суттю охорони власної інформації, причини і наслідки прийняття такого рішення розглядатися не будуть.

У разі прийняття рішення про необхідність захисту власної інформації виключимо з моделі такі опції, як захист інформації від дії обставин непереборної сили та інші, не пов’язані із застосуванням спеціальних технічних засобів негласного отримання інформації, а також наслідки можливих дій власника інформації щодо внутрішнього об’єктового контролю, у тому числі - негласного. Ще одним необхідним припущенням є припущення про відсутність будь-якого зв’язку між легальними і нелегальними суб’єктами 1-го типу у відношенні до ІСІВ.

Зрозуміло, що ідеальність інформаційного об’єкту не гарантує його безпеку від можливих активних дій легальних суб’єктів 1-го типу, адже, як вже було показано, ініціаторові НСРД іноді достатньо заяви громадянина N про можливе кримінальне правопорушення за участю ІСІВ для "запуску" механізму втручання у його приватне спілкування. Не слід забувати і про те, що на посадах ініціаторів НСРД знаходяться звичайні люди, які мають як власні позитивні для цих посад характеристики, так і суб’єктивні вади, перелік яких розглянутий, наприклад, в [6].

Ще більш зрозумілим є те, що гарантії безпеки ІСІВ від активних дій нелегальних суб’єктів 1-го типу взагалі відсутні.

Об’єктами можливих посягань нелегальних суб’єктів 1-го типу не обов’язково може бути інформація ІСІВ, - несанкціонований доступ до інформації ІСІВ може бути лише одним з елементів певної комбінації для досягнення контролю, можливості маніпулювання об’єктом в цілому, отримання доступу до зв’язків ІСІВ тощо.

Усвідомлюючи зазначене, логічним є висновок по те, що стратегія захисту інформації в ІСІВ повинна будуватися на техніко-економічних засадах компромісу між достатніми та необхідними технологіями захисту, придатними для вирішення конкретної задачі.

На нашу думку подальші дії ІСІВ можливо розмежувати за такими напрямками:

1. Що саме підлягатиме захисту?

2. Від кого маємо захищатися?

3. Як маємо захищатися?

4 Що робитимемо, коли система захисту зафіксує порушника?

З урахуванням змодельованих характеристик захисту підлягатимуть:

- інформація, як складова частина властивостей, що визначають змодельований суб'єкт саме як ІСІВ, з метою недопущення її модифікації або знищення для перетворення ідеального суб'єкта в неідеальний (інформація "І-1");

- інформація внутрішнього характеру, що дозволяє додатково вивчати особливості структури та функцій ІСІВ, знаходити його «слабкі ланцюги» (інформація "І-2");

- зв'язки ІСІВ з іншими суб'єктами, які сприймають його саме у вигляді ідеального суб'єкта та партнера (інформація "І-3").

Формування такого переліку відомостей викликано необхідністю збереження "ідеальності" суб'єкта, адже для неідеального суб'єкту, стратегія захисту та ресурси на її реалізацію є зовсім іншими.

Потенційними супротивниками, знов ж таки, у змодельованих умовах, можуть бути, скоріш за все, нелегальні суб'єкти 1-го типу. Враховуючи юридичну значимість (процесуальну цінність) саме оригіналів документів, основними загрозами для інформації "І-1" є її знищення або її тимчасова недоступність.

Для інформації "І-2" основними загрозами є негласне отримання інформації про розмови та дії осіб, а також всі інші різновиди втручання у приватне спілкування. Слід усвідомлювати, що реалізація зазначених дій з боку нелегального суб'єкту 1-го типу є кримінальним злочином (ст. 359, 361-363 Кримінального кодексу України).

Загрозами інформації "І-3", очевидно, є поєднання арсеналу загроз, актуальних для інформацій "І-1" та "І-2".

Після окреслення об'єктів захисту, потенційних загроз та можливих супротивників, можливо шукати відповідь на питання: як захищатися?.

В наших умовах є два варіанти:

1. Скористатися послугами легальних або нелегальних суб'єктів 2-го типу.

2. Організувати у складі ІСІВ власну службу захисту інформації.

З певною відповідальністю можливо констатувати, що в разі відсутності у керівника ІСІВ системних знань у галузі захисту інформації і перший, і другий варіант можуть бути неефективними. Часто основною метою суб'єктів 2-го типу не є захист інформації клієнта як такий, а розвиток власного бізнесу і отримання постійного джерела прибутку, разом з цим, організація власної служби не завжди є виправданою і майже ніколи – рентабельною.

Побудова оптимальної системи захисту можлива тільки за наявності системних знань у керівника ІСІВ.

Відомо, що основні види технічних засобів захисту поділяють на:

- засоби пошуку та знешкодження можливих каналів несанкціонованого доступу до інформації;

- засоби втаємничення інформаційної складової можливих каналів несанкціонованого витоку інформації.

Відомо, що вибір для захисту технічних засобів першого типу передбачатиме певну періодичність їх застосування, тому саме засоби другого типу можуть бути вибрані, як основні для нашого випадку. Виходячи з опису основної диспозиції суб'єктів 1-го і 2-го типу, наведеного на початку цієї роботи, перевагу під час вибору засобів захисту слід надавати оригінальним технологіям захисту, які «випадають» із загального ланцюга розвитку систем негласного доступу та захисту від нього. До таких систем можливо, наприклад, віднести захист інформації з використанням методів стеганографії [7], застосування ідеальних криптографічних систем [8], алгоритмів захисту інформації на основі тригонометричних функцій [9], систем передавання інформації на основі стохастичного модему [10], тощо.

Зрозуміло, що за мінімумом змодельованих характеристик ІСІВ, що розглядаються, а від так – певною його відірваністю від реальних умов функціонування, пропонування будь-яких конкретних способів захисту інформації неможливе.

Нижче будуть викладені деякі положення, які враховують те, що втаємничити інформаційну складову іноді є неможливим, а пошук каналів несанкціонованого доступу до

інформації залишається загальновживаним і традиційним методом. Основною принциповою вимогою, з точки зору авторів, під час організації процедур виявлення спроб несанкціонованого доступу до інформаційних ресурсів ІСІВ, є залишення в таємниці для суб'єкта 1-го типу як факту проведення такої процедури, так і результатів її проведення.

Для пояснення цього припустимо, що потенційний суб'єкт 1-го типу – легальний.

Вище було показано, що у переважній більшості випадків інтерес такого суб'єкта до ІСІВ носить суто "перевірочний" характер. Іншими словами, розгляд заяви громадянина N (не виключено – особи, звільненої з ІСІВ, та яка має власні претензії до колишнього керівництва), або аналіз певних версій кримінального або оперативно-розшукового проваджень надав підстави для перевірки скоєння можливого злочину шляхом втручання у приватне спілкування ІСІВ. У більшості випадків імідж ІСІВ в очах легального суб'єкта 1-го типу є приблизно наступним: ІСІВ є звичайним, з тисяч інших суб'єктів, який не розуміється на різних оперативних хитрощах, нічого особливого в ІСІВ нема, власної служби безпеки, де працюють колишні співробітники (працівники) правоохоронних органів, також нема, і в результаті 2-х місячного проведення заходів ми отримаємо цьому підтвердження. Уявимо, що під час проведення таких заходів суб'єкту 1-го типу стає відомим, що ІСІВ організував перевірку наявності фактів втручання у своє приватне спілкування, а потім, що ще гірше, виявив та вилучив якісь спеціальні технічні засоби, що були впроваджені до ІСІВ. В результаті таких дій легальний суб'єкт 1-го типу докорінно змінює своє уявлення про ІСІВ (якщо захищаються, то є за для чого), а факт вилучення спеціальних технічних засобів, враховуючи можливу перевірку законності їх встановлення, може призвести до штучної комбінації "доказів" кримінальної діяльності ІСІВ з метою додаткового обґрунтування свого інтересу до цього об'єкту. В результаті, дії ІСІВ, направлені на захист своєї інформації, матимуть наслідки набагато гірші за ті, що мали місце до здійснення заходів захисту.

Якщо суб'єкт 1-го типу є нелегальним, здійснення процедур захисту також викличе певну реакцію, але за суттю вона буде, на нашу думку, дещо іншою. Так, враховуючи притаманну будь-яким нелегальним суб'єктам економність витрат (адже вони витрачають власні гроші), не виключено, що для організації незаконного негласного доступу до інформації ІСІВ на першому етапі буде прийнята до реалізації якась мінімізована за витратами технологія. Виявлення та вилучення спеціальних технічних засобів аж ніяк не призведе до втрати інтересу до ІСІВ з боку нелегального суб'єкта 2-го типу. Наслідком такого можливе лише застосування більш витонченої та витратної технології негласного доступу, в залежності від того, якими методами ІСІВ реалізував пошук та вилучення спеціальних технічних засобів. Знов ж таки, в результаті намагань захистити свою інформацію, ІСІВ отримує замість невеликої проблеми (мінімізована технологія доступу) велику проблему разом з коригуванням уявлення про ІСІВ з боку нелегального суб'єкту 2-го типу.

Тепер є очевидним, що факт організації та проведення засобів захисту:

- повинен бути втаємниченим;
- в жодному разі не повинен передбачати вилучення спеціальних технічних засобів;
- повинен мати на меті єдине: збереження цілісності каналу несанкціонованого доступу;
- знаходження одного каналу не зупиняє перевірку для виявлення інших каналів.

Дотримання цих правил дозволить ІСІВ реалізувати технологію самозбереження за мінімальних витрат власних ресурсів. Враховуючи, що під час організації заходів захисту свої інформації ІСІВ заздалегідь не відомо, легальний або нелегальний суб'єкт 1-го типу реалізував свої наміри, основним завданням під час розробки плану дій за фактом виявлення каналу НСД є встановлення, яким саме суб'єктом, - легальним або нелегальним, він організований. Завдання не з простих, однак тут може стати у нагоді «мінімізація» витрат на організацію НСД з боку нелегальних суб'єктів. Наступним завданням є розробка плану використання знайденого каналу НСД у власних, ІСІВ, цілях. Це може бути дезінформаційна активність з проведенням певних комбінацій, що також може надати допомогу у виявленні

замовників організації НСД, імітація інформаційних повідомлень псевдо значущого характеру тощо.

Саме такі дії зможуть унеможливити втрати іміджу та ресурсів ІСІВ під час організації різними суб'єктами каналів НСД.

Висновки. З введенням у дію Кримінального процесуального кодексу України значно зросла кількість суб'єктів, що можуть ініціювати та проводити, легально або нелегально, заходи з втручанням у приватне спілкування суб'єктів інформаційної діяльності. Цей факт зобов'язує зазначені суб'єкти переглянути існуючі моделі загроз, внести корективи у тактику та стратегію захисту власної інформації, надавши перевагу при цьому застосуванню нетрадиційних, оригінальних форм і методів захисту інформації, у тому числі тих, в основі яких є пошук та локалізація каналів несанкціонованого доступу до інформації.

Необхідною умовою розробки ефективних та дієвих планів захисту інформаційних ресурсів є наявність у відповідальної особи системних знань у галузі як організації негласного отримання інформації, так і у галузі захисту від реалізації таких негласних заходів.

ЛІТЕРАТУРА

1. Перелік суб'єктів господарювання, які мають ліцензії на провадження господарської діяльності з надання послуг в галузі технічного захисту інформації – [режим доступу до переліку:http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article;jsessionid=C6C23682E4B9C0362CF2D06D1B898A65?art_id=94056&cat id=94055].

2. Відомості з ліцензійного реєстру у сфері СТЗ – [режим доступу до відомостей: http://ssu.gov.ua/sbu/control/uk/publish/article?art_id=106134&cat_id=106105].

3. Указ Президента України N 256/2001 "Про впорядкування виготовлення, придбання та застосування технічних засобів для зняття інформації з каналів зв'язку".

4. Федеральный Закон РФ "Об оперативно-розыскной деятельности" –[режим доступу до закону: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=138366].

5. Брягин О.В. Безопасность Вашего бизнеса. Советы постороннего: систем. подход, аналит. материалы, практ. рекомендации / О.В. Брягин. - К.: КНТ, 2006. - 228 с.

6. Борисова С.Е. Профессиональная деформация сотрудников милиции и ее личностные детерминанты: автореф. дис. на соиск. учен. степ. канд. психол. наук: спец. 19.00.06 "Юридическая психология" [режим доступу до автореф.:http://www.dissercat.com/content/professionalnaya-deformatsiya-sotrudnikov-militsii-i-ee-lichnostnye-determinanty#ixzz2HPH21sJG].

7. Савченко Ю. Г. Организация скрытого информационного обмена в режиме реального времени / Ю.Г. Савченко, І.А. Сажина // Наукові записки УНДІЗ. - 2010. - №1(13). - С. 57-62.

8. Фионов А.Н. Эффективные методы построения идеальных криптографических систем защиты информации: автореф. дис. на соиск. учен. степ. докт. техн. наук: спец. 05.12.13 "Системы, сети и устройства телекоммуникаций" [режим доступу до автореф.: http://www.dissercat.com/content/effektivnye-metody-postroeniya-idealnykh-kriptograficheskikh-sistem-zashchity-informatsii#ixzz2HZPbKPiJ].

9. Сизов В.П. Алгоритм защиты информации на основе тригонометрических функций информации: автореф. дис. на соиск. учен. степ. канд. техн. наук: спец. 05.13.19 "Методы и системы защиты информации, информационная безопасность" [режим доступу до автореф.: http://www.dissers.ru/1tehnicheskie/algoritm-zaschiti-informacii-na-osnovetrigonometricheskih-funkciy-05-13-19-metodi-sistemi-zaschiti-informacii-informacionnaya-bezopasnost.php].

10. Патент РФ №2309547, С2 RU. МПК H04K 1/00. Способ передачи информации / Брягин О.В., Розоринов Г.Н., Егоров А.К.; опубл. 27.10.2007. - Бюл. №30.

Надійшла: 12.03.2013 р.

Рецензент: д.т.н., проф. Козловський В.В.