НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

НАВЧАЛЬНИЙ ПОСІБНИК

Київ – 2018

УДК 351.746.1
0-64

Рецензенти:
І.В. Слюсарчук, доктор юридичних наук, професор;
А.І. Марущак, доктор юридичних наук, професор

Авторський колектив
Внесок авторів: Гуз А.М. – розділ – 1; Касперський І.П. – розділ 3; Князєв С.О. – вступ, розділ 4; Савченко Д.С. - розділ 6; Семчишина С.В. – розділ 5; Ткачук Т.Ю. – розділ 2; Тугарова О.К. – розділ – 7; Шепата О.В. – розділ 5.

Рекомендовано до друку редакційно-видавничою радою Національної академії СБ України (протокол № 3 від 31 жовтня 2017 р.)

Організація захисту інформації з обмеженим доступом: навч. посіб. /А.М.Гуз, І.П.Касперський, С.О.Князєв та ін. – К.: Нац. акад., СБУ, 2018. – 252 с.

У навчальному посібнику розглядаються питання пов'язані з організацією захисту інформації з обмеженим доступом.

Для студентів ННІІБ НА СБ України, працівників режимно-секретних органів, які навчаються на курсах підвищення кваліфікації ННІІБ НА СБ України, курсантів і слухачів НА СБ України, які вивчають навчальні дисципліні, що повязани з вивченням питань організації захисту інформації з обмеженим доступом, а також науково-педагогічних працівників НА СБ України.

УДК 351.746.1

ЗМІСТ

УМОВНІ СКОРОЧЕННЯ

АС – автоматизована система;
ДСТУ – Державний стандарт України;
ЗМІ – засоби масової інформації;
ЗУ – закон України;
ІЗОД – інформація з обмеженим доступом;
ЕОМ – електронно-обчислювальна машина;
КЗпП України - Кодекс законів про працю України;
КК України – Кримінальний кодекс України;
КПК Укаїни – Кримінальний процесуальний кодекс України;
КУпАП - Кодексу України про адміністративні правопорушення;
НА СБ України – Національна академія Служби безпеки України;
НДІ – науково-дослідний інститут;
ННІБ НА СБ України – Навчально-науковий інститут інформаційної безпеки Національної академії Служби безпеки України;
НКВС – Народний комісаріат внутрішніх справ;
НСД – несанкціонований доступ;
ПЕМВН – паразитне електромагнітне випромінення та наведення;
ОУН – Організації українських націоналістів;
СБ – Служба безпеки;
СБ України – Служба безпеки України;
УВО – Українська військова організація;
УПА – Українська повстанська армія;
ЦК України – Цивільний кодекс України

ВСТУП

Питання забезпечення інформаційної безпеки завжди є важливими і актуальними для будь-якої держави, про що наголошується й у статті 17 Конституції України. Створений в нашій державі значний масив нормативно-правових актів, щодо врегулювання суспільних відносин в інформаційній сфері, який постіно оновлюється та вдосконалюється, наочно свідчить про пріоритетність даного питання для країни.

Проте, постійний, динамічний розвиток суспільства супроводжується різноманітними загрозами існуванню інформації, що вимагає безперервного вдосконалення системи інформаційної безпеки. Зрозуміло, що найбільш уразливим сегментом загальнодержавної інформаційної сфери стає інформація з обмеженим доступом (далі – ІЗОД).

Зважаючи на вітчизняне законодавче розмежування ІЗОД та використання значної кількості різних її видів, у пропонованому посібнику акцентовано увагу як на загальних питаннях пов'язаних із правовим врегулюванням й організацією захисту ІЗОД, так і на особливостях використання окремих видів в умовах підприємств, установ і організацій.

Зокрема, загальнотеоретичні засади правового регулювання ІЗОД, представлені в окремомому розділі, логічно доповнюються виділенням та систематизацією сучасних загроз щодо ІЗОД, особливостями використання такої інформації в установах під час здійснення підприємницької діяльності, технічним забезпеченням захисту інформації в сучасних інформаційних системах тощо.

Крім того, створенню цілісного уявлення про організацію захисту ІЗОД безперечно буде сприяти розгляд питань стосовно еволюції системи ІЗОД в Україні та юридичної відповідальності у сфері обігу такої інформації.

Структурно видання складається з шести розділів після кожного визначені питання для самоконтролю, використана та рекомендована література.

Посібник розраховано на студентів ННІІБ НА СБ України, які вивчать навчальні дисципліни: «Організаційно-правові основи захисту інформації з обмеженим доступом», «Охорона державної таємниці», «Охорона комерційної таємниці», «Інформаційне право». Крім того, його зможуть використовувати для підготовки до проведення занять за відповідною тематикою працівникі режимно-секретних органів, які навчаються на курсах підвищення кваліфікації в ННІІБ НА СБ України, а також курсанти і слухачі НА СБ України, які вивчають навчальну дисципліну «Забезпечення державної безпеки у сфері охорони державної таємниці» та науково-педагогічні працівники НА СБ України.

РОЗДІЛ 1

ЕВОЛЮЦІЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В УКРАЇНІ

1.1. Особливості організації захисту інформації з обмеженим доступом на території України в різні історичні періоди

Проблемам захисту інформації з обмеженим доступом на теренах України в різні періоди її історії приділялося чимало уваги. Українські вчені довели, що органи державної адміністрації завжди намагалися захистити таємниці. Зокрема, ще відчасів скіфсько-сарматського панування й до утвердження князівської влади в Київській Русі інформації про військо племінного князя, його особу, дислокаціювійська під час походу, території через які воно пересуватиметься, зміст укладених договорів з сусідніми державами, розташування, укріплення, забезпечення продовольством та спорядженням «княжого граду» приділялося багато уваги, і саме ці відомості охоронялися.

Військо на той час відігравало стратегічне значення у розвитку племінного княжіння. Від знання інформації про його чисельність, розташування залежала багато в чому перемога на полі битви. Можемо констатувати, що першим видом інформації, якиа підлягала охороні, була саме військова. Охорону такої інформації спочатку забезпечував племінний князь, потім – особа, якувін призначав особисто. Інформація про зміст невигідно укладених договорів того часу теж підлягала захисту і нерозголошеннюя, оскільки сусіди могли використати її у своїх корисливих цілях.

Уже за доби розвитку державності аж до середини XI ст. тривали походи Русі на Візантію. Насамперед тому, що війна була на тоді головним і загальновизнаним засобом ведення зовнішньої політики будь-якої держави. А тому і захист військової інформації превалював у політиці Олега, Ігоря, Ольги, Святослава, Ярослава. Князі, йдучи в похід, намагалися приховати

чисельність війська і напрям головного удару. Ворог, який достаменно не знав кількості противника не міг приймати адекватні рішення, а заздалегідь поширені страхітливі чутки, перебільшена дезінформація доводили його до паніки.

Як зазначалося вище, ще одним видом інформації, яка захищалася, були івідомості про розташування, укріплення і забезпечення продовольством та спорядженням міст. Знання таких даних дозволяло розробити успішний план облоги. Коли ж нападник не зміг роздобути такої інформації, облога часто-густо не мала успіху.

Перші князі приховували своє віросповідання, зокрема Ольга. Та й сам Володимир тривалий час не наважувався приймати християнське віровчення, попри неодноразові пропозиції Візантії. Хоча на це існувало чимало причин, можливо, інформація про християнські вподобання князя могла неоднозначно сприйнятися русичами, тому й охоронялася, не доводячи до широких мас населення.

За Володимира та Ярослава особливого розмаху набуває зовнішньополітична, дипломатична діяльність держави, тому інформація про міжнародні зносини підлягє охороні.

Маємо підстави припустити, що вже за доби Київської Русі з'являються державні службовці, на яких покладається захист згаданих відомостей.

Отже названі вище різні види інформації охоронялися державою. Про це свідчать тогочасні джерела, і зокрема правові. Так, влада та особа князя охоронялася понад усе, за посягання на панування та життя князя призначалася найвища міра покарання – потік та пограбування. Передання військової інформації ворогу (тобто зрада) або втеча з поля бою з метою видачі таких відомостейвважалася державним злочином і теж жорстоко каралися за законами Київської Русі.

Традиції Київської Русі із захисту інформації розвинулися в Галицько-Волинській державі та Руcько-Литовській державах.

Від середини XIV ст. українські землі поступово були інкорпоровані до складу Литовсько-Польської держави, яка теж чимало уваги приділяла захисту виокремлених вище відомостей. Військова інформація залишається одним із найважливішим об'єктів утаємничення. Можна сказати, що за польського панування захист інформації набуває особливого значення. Особа князя, короля захищається державою. З'являється новий вид інформації, який активно охороняється – державна таємниця. Починає формуватися нормативна база, яка регулювала віловідні питання. Зокрема, в першому розділі арт.3 Литовського статуту Великого князівства Литовського 1588 р., що діяв на більшій території Україні, йшлося про злочини проти престолу.Відповідно до цього документа передбачалася страта за листування з ворогом і повідомлення йому даних, які могли б зашкодити державі. «Хто б с неприятельми нашими поразуменьемел, листы до них або послы радечи против нас, государя и Речи Посполитой, або остерегаючи слал, … такова чести отсудить и горлом карать».

Зрозуміло, що на той час в епоху середньовіччя, коли зв'язки між державами за відсутності швидкої комунікації були слабкі, важливу роль починає відігравати інформація про внутрішньополітичне становище Речі Посполитої, її зовнішню політику. Тому сусідні держави переманювали на свій бік королівських службовців, і всіх тих, хто був обізнаний з інформацією з обмеженим доступом, або навіть засилали шпигунів (розвідників), які здобували потрібні відомості. Це були високоосвічені люди, переважно представники дипломатичних місій, які брали участь у налагодженні міждержавних відносин. Звісно, шпигунство завдавало шкоди державі й жорстоко каралося, в Речі Посполитій людина, яка це чинила, оголошувалася зрадником. Саме з метою захисту таких даних у Статут була введена норма, яка законодавчо визначала захист важливої державної інформації. Причому кримінальна відповідальність за розголошення зазначеної інформації була одним із елементів її захисту інформації. Вочевидь, у XVI столітті в Речі Посполитій пошуком та знешкодженням шпигунів займалися відповідальні

перед королем і ним призначені державні службовці, його найближче оточення. До їх компетенції, напевно, було віднесено і захист найбільш важливої інформації. Яким чином вони здійснювали її захист? На нашу думку, до роботи з важливими документами, які приймав польський Сейм, допускалося обмежене коло відданих королю осіб, переважно магнатів (канцлер, гетьман, підскарбій). Теж саме стосується складання та підписання міждержавних угод. Інформація про місце перебування та пересування короля країною теж підлягала охороні, оскільки цим могли скористатися незадоволені його діяльністю верстви населення або магнати, шляхта. Тому охороною його особи та королівських угідь опікувалися слуги – замкові, путні, сторожеві та інші. Можна стверджувати, що саме в цей період у польській державі створюються окремі підрозділи, на які покладаються безпека особи короля, держави та захист важливої інформації. Очевидно, що керівництво захистом інформації в Польщі зосереджувалося в руках коронного або польного гетьманів.

У період існування Запорізької Січі та України-Гетьманщини захисту інформації з обмеженим доступом теж приділялася значна увага. Передусім це стосувалося інформації, повязаної з військовою сферою. Особливість цього періоду в тому, що захист військово-політичної інформації Б. Хмельницьким здійснювався у процесі формування держави та війни з Польщею, а його наступниками – у процесі протидії зазіханням московитів.

Захищаючи військову інформацію, Б. Хмельницький, знаючи про традиційну недооцінку польською стороною необхідності важливості втаємничення своїх планів, прагнув насамперед шляхом дезінформації посіяти в польському війську невпевненість у власних силах, панічні настрої, тобто застосовував елементи, за сучсною термінологією, «психологічної війни». Тому не випадково у своїх універсалах він наполягав на необхідності створення в лавах ворога атмосфери приреченості, напруги, непевності, що й було досягнуто у ході боїв приміром, під Корсунем, Пилявцями, Берестечком.

Історичні джерелане підтверджують існування окремої інституції, яка б спеціально займалася цією важливою ділянкою захисту державних інтересів козацької України. Проте потреба у протидії іноземним агентам, які прагнули здобути інформацію про військові плани Хмельницького, існувала. У зв'язку з чим можна припустити, що виконання функції захисту інформації покладалося на центральні й місцеві органи влади.Як уже зазначалося, особливу увагу гетьман звертав на збереження у таємниці військово-політичної інформації. І те, що це в цій царині відносят неабиякий успіхів, промовисто свідчать польські спогади польських урядовців, воєначальників, офіцерів.

Під час проведення воєнних операцій Б. Хмельницький вживав рішучих заходів для запобігання одержанню ворогом відомостей про чисельність війська та оперативно-тактичні плани. З цією метою, він, по-перше, знаючи про наявність польських розвідників у своєму таборі, часто вдавався до поширення серед козаків дезінформації щодо подальшого способу дій. По-друге, – запроваджував сувору дисципліну, щоб позбавити польські роз'їзди можливості захоплення цінних «язиків». І, по-третє, максимально обмежував коло осіб, обізнаних із суттю задуманих операцій. Доводилося також гетьманові протистояти «інформаційним атакам» провокаційного ідеологічного ґатунку, спрямованим на його дискредитацію в очах козацтва та інших прошарків українського населення, на розкол Війська Запорозького, а також захищати інфомацію, яка могла посприяти таким атакам.

Таким чином, у ході розбудови національної держави в середині XVII ст. (час гетьманства Б. Хмельницького) захисту інформації відводилася важлива роль у боротьбі українців за незалежність, щосприяло реалізації політичних і військово-стратегічних задумів українського уряду.

Аналізуючи особливості захисту інформації в державі Б. Хмельницького, слід зазначити, що, на нашу думку, ці функції частково були покладені на контррозвідку. У період Національної революції гетьман,

Генеральна канцелярія та інші органи влади приділяли велику увагу втаємниченою військово-політичних планів, успішно протидіяли заходам польської розвідки, зокрема її спробам організувати державний переворот шляхом усунення від влади Б. Хмельницького чи його вбивства, тощо. Спромігся Б. Хмельницький приховати від ворога плани передислокації військау різних битвах. Наприкінці 1650 – у першій половині 1651 рр. було вжито рішучих заходів проти розвідувальної діяльності московських засланців на теренах України.

Велику увагу збереженню в таємниці інформації про військові плани приділяв Б. Хмельницький під час Берестечкової кампанії. Задля цього ві вимагав суворої дисципліни не лише від українців, а й своїх від союзників – татар. За даними джерел, останнім заборонялося від'їздити від обозу далі, ніж на 3,5-4 км, що звело до мінімуму шанси польського командування одержувати відомості шляхом захоплення «язиків».

Не втрачав Б. Хмельницький пильності й надалі, про що, хоч і вельми скупо свідчать джерела. Так, київський воєвода у листі до польського короля (січень 1655 р.) неприховував невдоволення тим, що навіть «добрі язики» неможуть про українського гетьмана «дати певної відомості».

Уряд Б. Хмельницького вчасно вживав необхідних заходів у сфері захисту військово-політичної інформації Української держави від ворожих дій Польщі. Завдяки цьому вдавалося зберігати у таємниці військові плани найголовніших кампаній, розкривати змови, організовані ворожою агентурою, протидіяти спробам правлячих кіл Речі Посполитої спровокувати міжусобицю серед українців, внести розкол у лави національно-патріотичних сил. Основним видом інформації з обмеженим доступом цього періоду, яка захищалася, були івідомості про військово-політичне становище країни.

На Запорозькій Січі теж чимало уваги приділялося захисту військової інформації, оскільки вона була військовим об’єднанням і, очевидно, осавул і писар, які відали прикордонними роз'їздами і управляли розкиданими по степових слободах і хуторах козаками (т. зв. «сиднями»), займалися її

захистом. На роз'їзди покладалася розвідка становища за межами кордону. Про її результати повідомлялося в Січ. Залишається ще додати, що військовий товмач, будучи знавцем інших мов, іноді посилався з таємним завданням на кордон або в розташування супротивника.

Можна зазначити, що в умовах будівництва держави фактично формувалася й організація захисту інформації з обмеженим доступом. Наступні гетьмани України І. Виговський, Ю. Хмельницький, П. Тетеря, І. Брюховецький, П. Дорошенко, Д. Многогрішний, І. Мазепа, І. Скоропадський, П. Полуботок, К. Розумовський теж приділяли чимало уваги захисту військово-політичних планів держави.

Активні дипломатичні зносини з Кримом вів І. Виговський, перебуваючи на посту писаря за часів Б.Хмельницького, і пізніше, – ставши гетьманом І. Виговському дослідники відводять одну із провідних ролей у створенні системи захисту інформації, а саме: створення спеціальних органів – розвідки та контррозвідки України, які займалися захистом військово-політичної інформації.

Найпевніше, на писаря було покладено захист військово-політичної інформації в державі та здобуття найбільш важливих відомостей корисних для держави через драгоманів (товмачів).

Неабияких зусиль до захисту військово-політичної інформації докладав І. Мазепа. Наприклад, гетьман кілька років вів перемови з королем Швеції Карлом XII і спромігся інформацію про мету цих зносин практично повністю захистити. Навіть цар не знав про зміст перемовин, хоча про сам факт йому неодноразово доносили наближені до гетьмана особи. Ці переговори, як відомо, закінчилися підписанням таємної угоди між королем «шведів, готів і вандалів і гетьманом України угодою» щодо боротьби проти Москвії. Очевидно, що Мазепа розумівся на захисті інформації. Передовсім, доступ до важливих відомостей надавав вузькому колу наближених осіб, полковникам не довіряв, позаяк знав, що більшість із них та їхнього оточення московські

шептуни. Підтвердженням цього є таємні переговори, які вів Мазепа з Карлом XII.

У XVII-XVIII столітті спроба створити власну незалежну Українську державу не увінчалась успіхом. На початку XX століття історія дала українцям ще один шанс. Перша світова війна та її результати кардинально перекроїли всю систему міжнародних відносин. На політичній карті Європи, особливо на сході континенту, з'явилися нові держави, які закладали підвалини повоєнних відносин. Серед них у 1917 році постала й незалежна Українська Держава, яка пройшла різні етапи й форми розбудови – Українська Народна Республіка періоду Центральної Ради, Українська Держава гетьмана П. Скоропадського, Українська Народна Республіка доби Директорії, Західноукраїнська Народна Республіка.

Війна показала, що захист усіх видів інформації вимагав значних змін і серйозної централізованої організації. Усі уряди незалежної української національної держави багато уваги приділяли побудові дієвої системи захисту не лише військових та державних секретів, а ц усієї важливої військово-політичної інформації та створенню спеціальних органів, які б опікувалися цими проблемами.

Починаючи зперіоду Центральної Ради, можна виділити кілька видів інформації, які підлягали захисту державою: військова, державна, інформація з обмеженим доступом, службова, слідча, персональна тощо. У роки різних форм незалежної української державності (1917 – 1921) на передній план ставився захист різних видів інформації. Характер відповідної нормативної бази в цей період багато в чому визначався його особливостями та іншими чинниками, що впливали на дії вищих органів влади тогочасної України.

Специфіка та особливості створення перших вітчизняних органів, які опікувалися захистом інформації та державної безпеки, свідчить, що на початковому етапі свого функціонування вони намагалися зробити посильний внесок в державотворення України та забезпечення її існування. Однак їх діяльність була ще малоефективною.

Дослідники виділяють три головні причини цього. По-перше, хоча створення координаційного органу з питань безпеки та оборони стало нагальною потребою тогочасного суспільно-політичного життя в Україні, в керманичів держави не було чіткого уявлення про статус, функції, компетенцію і стратегію діяльності цієї інституції. Це викликало взаємні нерозуміння і гальмувало ініціативу з обох боків. По-друге, до створення цих інституцій практично не залучалися висококваліфіковані військовики та досвідчені керівники та співробітники спеціальних служб, які були в розпорядженні, зокрема, Генерального Секретаріату за часів Гетьманату. По-третє, за діяльністю створених комітетів і комісій не здійснювався необхідний і результативний контроль, механізм виконання їхніх рішень та постанов не був відпрацьований.

Уряд П. Скоропадського працював у складних умовах: внутрішня та зовнішня скрута в державі посилювалася партійними чварами та класовими суперечностями. Проте система захисту інформації, хоч і не вельми досконала, вже функціонувала. Професіоналізм гетьманської розвідки дозволив певною мірою протидіяти іноземному шпигунству та диверсійно-терористичним акціям антидержавних елементів (комуністичному підпіллю, яке дислокувалося переважно у промислових центрах, російським шовіністичним організаціям під прапором «білого» руху, спеціальним службам країн австро-німецького блоку та ін.).

Про шкоду від потрапляння важливої військово-політичної інформації розуміли усі урядовці, однак серйозних заходів та установ, які б могли здійснювати її держава не виробила. Освідомчі (контррозвідувальні) підрозділи Державної варти (зустрічається назва «інформаційні») виконували роботу з попередження, виявлення і припинення злочинів проти державного ладу й безпеки держави, збір інформації про політичні партії тощо.Керівництвом Департаменту Державної варти вперше в Україні була створена мережа конспіративних та явочних квартир для роботи з агентурою. Крім того, добування інформації про суспільно-політичне становище в

Україні здійснювалося шляхом опрацювання й узагальнення відкритих періодичних (особливо партійних) видань. Відповідно цей крок був направлений на створення дієвої цензури засобів масової інформації, яка б могла захистити витік інформації про військово-політичне становище у державі через друковані органи.

Організація захисту військової інформації в період Директорії (1919-1920 рр.) здійснювалася в Генеральному штабі УНР. За захист інформації відповідав контррозвідувальний відділ та його окремий загін – польової артилерії.

1.2 Специфіка захисту інформації з обмеженим доступом у націоналістичному русі в 20-40-х роках 20 ст.

Про будівництво системи захисту інформації з обмеженим доступом на території України за радянської доби написано чимало праць, які здебільшого об'єктивно висвітлюють це питання. Водночас ця тематика стосовно українського націоналістичного руху в 20-40-х роках 20 ст. досліджена мало й недостатньо представлена в навчальних виданнях. Спробуємо у цьому розділіу цьому розділі певною мірою заповнити цю прогалину.

Боротьба українців за свою незалежну державу в 1917-1921 рр. завершилась поразкою. Проте значна їхня частина не змирилася з цим і продовжила боротьбу. Організований рух українських націоналістів виникає як реакція на поразку національно-визвольних змагань 1917-1921 рр., ліквідацію національної державності, територіальне розчленування західноукраїнських земель між Польщею, Румунією та Чехословаччиною. Водночас його поява стала і проявом глобальної тенденції до радикалізації національно-визвольних рухів в Європі після Першої світової війни. За цих умов активні учасники боротьби за незалежність і соборність України вживають заходів до створення опозиційної окупантам воєнізованої структури для відновлення збройної боротьби за державний суверенітет та

територіальну цілісність України.

На засіданні Стрілецької ради у липні 1920 р. та на з'їзді представників військово-патріотичних організацій 31 серпня цього ж року у Празі ухвалюється рішення про заснування Військової організації (після 1924 р. утверджується назва Українська військова організація (УВО), щоб «зберегти в організованій формі існуючі поза територією України військові частини й об'єднати їх ідейно між собою».

Потреба всебічного вивчення свого головного противника, інформаційного забезпечення підпільно-підривної діяльності та майбутнього масштабного збройного виступу проти поневолювачів, захисту від силових структур ворога зумовила неодмінність оперативного супроводження діяльності УВО, налагодження розвідувальної та контррозвідувальної активності. Першим спеціальним підрозділом в організаційних структурах українських націоналістів стала «розвідочна» (розвідувальна) референтура УВО.

За умов кваліфікованих оперативно-розшукових заходів польських спецслужб в УВО велике значення надавалося дотриманню конспірації, яка в перші два-три роки була незадовільною, навіть запроваджені псевдоніми застосовувались рідко. Однак завдяки вжитим заходам і розумінню небезпечності противника у 1923-1928 рр. конспірація в УВО була «найліпшепоставлена й найсильніше збережена, як ніколи перед тим або потім». Посилена увага приділялася вихованню у націоналістів відповідних особистих якостей та озброєнню їх знаннями щодо методів оперативної роботи противника, повчальним досвідом аналогічних антиурядових рухів та організацій. У свідомості членів підпілля міцно закарбовувалися такі постулати, як «конспірація», «мовчазність», «безоглядний послух і дисципліна», «негайне виконання всіх наказів», неминучість «кари за зраду тайни».

У друкарнях Німеччини та Литви видавалися «вишкільні» (навчально-інструктивні) брошури «Методи конспірації», «Значення розвідки», «Хто

працює в розвідці», «Що загал знає про розвідку», методичні матеріали з диверсійної справи та партизанської війни. На шпальтах друкованого органу УВО «Сурма» регулярно вміщувалися матеріали з досвіду діяльності революційних або екстремістських рухів («Як російські революціонери втікали з тюрем», «Нігілісти», «Орсіні»), щодо методів протидії польській поліції («З практик ляцької поліції», «Зізнання», «Техніка слідства») тощо.

З 28 січня по 3 лютого 1929 р. у Відні відбувся Установчий конгрес Організації українських націоналістів (ОУН), який об'єднав УВО з молодіжними організаціями націоналістів – Групою української національної молоді, Лігою українських націоналістів, Союзом української націоналістичної молоді та інших – в єдину ОУН. На цьому конгресі було обрано Провід ОУН на чолі з Є. Коновальцем, ухвалено статут та основні підвалини політичної лінії ОУН.

На початку 30-х років 20 ст. значно активізувалася терористична, саботажна та пропагандистська діяльність ОУН щодо Польщі. У липні 1932 р. на Празькій конференції ОУН створюється «контрольно-розвідочна» референтура на чолі зі студентом-медиком Я. Макарушою (заступник – О. Пашкевич). На підрозділ покладалося завдання «зовнішньої розвідки» (збору інформації про збройні сили, правоохоронні органи та структури влади Польщі, створення в них агентурних позицій) і «внутрішньої розвідки»(контррозвідувального захисту підпілля, перевірки його членів на лояльність). Одним із пріоритетів у діяльності цього органу стає також сувора конспірація та контррозвідувальний захист власного середовища, поширення навчально-методичної літератури з питань підпільної боротьби.

У націоналістичному русі в 1920-1940-х рр. сформувалисяспецифічні морально-психологічні риси його учасників, відображені у моральному кодексі націоналістів – «Декалозі».

Що стосується організації захисту інформації з обмеженим доступом, то в пункті 6«Декалогу» зазначалося, що підпільнику «говорити про справи організації можна лише з тим, із ким потрібно в інтересах справи». У

навчальній літературі підкреслювалося також, що підпільник повинен бути мовчазним, холоднокровним, вміти виробляти бездоганне алібі.

Для конспірації кожен підпільник мав псевдонім, який повинен бути не співзвучним зі справжнім іменем людини, не нагадувати рис зовнішності й характеру та змінювався залежно від місцеперебування або при загрозі викриття. Провідник (керівник) будь-якого рівня не мав знати псевдоніми підлеглих нижче, ніж на два ступені. Чимало давалося рекомендацій щодо ретельного підбору конспіративних та явочних квартир, підготовки зустрічей.

Важливим напрямом організації захисту інформації з обмеженим доступом стало розповсюдження навчальних матеріалів з правил і способів конспірації.Зокрема, широкого застосування отримала книга з основ конспірації «Пашні буряки», написана в 1937 році функціонером ОУН на Тернопільщині В. Куком. Це – підручник з широкого кола питань нелегального буття, зокрема, дотримання конспірації у повсякденному житті та проведенні терористичної діяльності, організації конспіративних зустрічей та квартир, формування і зберігання справ у архівах, уникнення переслідування поліції, уміння нелегально перетинати кордон, виготовляти фальшиві документи, знання методів тайнопису.

Крім того, вживалися заходи для підтримки внутрішньої безпеки та порядку в організації, поповнення лав підпілля супроводжувалося ретельною перевіркою.Кандидат до вступу в ОУН «проходив підготовку і перевірку: чи є правдомовний, чи не має поганих звичок і лихих намірів, які негативні риси йому притаманні». Ті, хто здійснював перевірку, могли видавати себе польськими поліцейськими, інсценувати події в лісі, полі, на спеціальній квартирі чи в хаті.

Наприкінці 30-х років 20 ст. з’явилася нова форма спеціального підрозділу в ОУН – у лютому 1939 р. вперше заснували референтуру Служби безпеки (СБ).Досвід творення СБ ОУН у довоєнний період відображено в інструктивному документі «Організація служби безпеки» (укладений між

березнем та червнем 1941 р.). Центральним елементом СБ був інститут референтів – керівників підрозділів СБ у структурі територіальних проводів. На референта покладалася турбота про «належну охорону організаційної роботи та її членів, збирання інформації про ворожі сили, що діють на шкоду ОУН, проведення їх ліквідації, ведення внутрішньої розвідної праці». Референтура безпеки крайового проводу виконувала функції виявлення та припинення діяльності агентури противника, виконання диверсійно-терористичних акцій, охорони конспіративних нарад проводу, виготовлення фальшивих документів прикриття.

Також на Службу безпеки покладалася насамперед протидія агентурній діяльності НКВС-НКДБ у середовищі підпілля, облаштування конспіративних та явочних квартир. Про високий рівень конспіративності та рішучості у захисті власних лав від оперативних заходів противника є свідчення у радянських документах. Зокрема, в орієнтуванні 3-го Управління НКДБ СРСР від 31 травня 1941 р. зазначалося:«оунівці-нелегали є добре навчені стосовно нелегальної техніки, загартовані й вельми агресивні кадри. Як правило, при арештах... вчиняють збройний спротив, намагаються покінчити самогубством. Оунівці, запідозрені у співробітництві з радянською владою, фізично знищуються».

Варто зазначити, що Директиви ОУН вимагали активно просувати розвідників на роботу, у тому числі на керівну, до офіційних закладів для збору інформації, здобуття бланків документів та іншого сприяння підпіллю. Особлива роль у розвідувально-інформаційній роботі відводилася «Юнацтву». Осередки молодіжного резерву існували у всіх школах Львова, в одній зі шкіл Коломиї половина учнів перебувала в «юнаках», їх навчали методів збору інформації, конспірації, вони становили більшість персоналу конспіративних ліній зв’язку.

Першим серйозним випробуванням спецпідрозділів ОУН(Б) став двобій зі спецслужбами Радянського Союзу на землях Західної України у 1939-1941 рр.Після вступу радянських військ 17 вересня 1939 р. у цей регіон

та включення західноукраїнських земель до складу УРСР та СРСР швидко відбувається творення потужної системи радянських органів та військ внутрішніх справ і державної безпеки. Як зазначалося в орієнтуванні глави НКВС УРСР І. Сєрова начальникам УНКВС Західної України №26/СН-1940 р., ретельна перевірка оунівцями своїх лав, знання ними прийомів конспірації вимагає вдосконалення методів оперативно-розшукової діяльності. Першочерговим завданням стало просування радянської агентури до керівних ланок і закордонних центрів ОУН.

Підпілля в Західній Україні існувало у постійному протиборстві з радянськими силовими структурами. Лише у 1940-1941 рр. радянськими органами і військами НКВС-НКДБ викрито декілька десятків великих націоналістичних організацій, на кордоні затримано понад 400 емісарів, ліквідовано понад 200 розвідувально-диверсійних груп ОУН, що намагалися прорватися через кордон. Контррозвідувального забезпечення потребували й закордонні центри ОУН, до яких радянські органи держбезпеки у довоєнний період спромагалися запровадити свої оперативні джерела.

Інтереси оперативного забезпечення підпільної мережі ОУН(Б) на окупованій гітлерівцями території, потреба протидії спецслужбам держав-агресорів, зафронтовій розвідувальній діяльності радянських спецслужб потужному польському націоналістичному підпіллю в Західній Україні зумовили те, що до кінця 1941 р. майже всі територіальні проводи ОУН (Б) мали у складі референтури СБ. Крах сподівань на толерантне ставлення Німеччини до відродження національної державності, а також фізичні переслідування учасників націоналістичного руху (як складової масового терору нацистів проти українського народу) прискорили перехід бандерівців на нелегальний стан, каталізували творення територіальних органів Служби безпеки та підвищену увагу до захисту організаційної таємниці й удосконалення конспіративних засад діяльності.

Розроблялися навчально-методичні матеріали з організації розвідувальної та контррозвідувальної роботи. Інструкція проводу

бандерівців у Галичині «Суспільна безпека» (серпень 1942 р.), наприклад, містила характеристику завдань і складових роботи агентурного апарату (резиденти, агенти, зв'язкові тощо), методів отримання доступу до конфіденційної інформації. Ішлося про тактику роботи контррозвідувальних органів, захист внутрішньої безпеки.

Протинімецькі заходи СБ мали здебільшого пасивний характер, що випливало із загальної тактичної лінії ОУН того часу стосовно окупантів, спрямовувалися на захист лав організації від ударів нацистських спецслужб.

За свідченням В. Кука, «до завдань референтур в період німецької окупації входило вивчення методів роботи німецької розвідки і контррозвідки, і з цією метою ...засилали членів ОУН для роботи в органах німецької розвідки та контррозвідки». Робота СБ проти німців активізувалася з 1942 р. Зокрема, восени у Києві на конспіративному засіданні функціонерів підпілля ухвалюється рішення про створення спеціальних агентурних груп для збору інформації про німців. Контррозвідка підпілля виявляла та заводила справи розробки на агентів гестапо серед оунівців. Крім того, вивчалися співробітники гітлерівських силових структур, їх зв'язки серед місцевого населення.

Кожний референт СБ повинен був двічі на місяць подавати керівництву звіт про роботу німецьких карально-репресивних органів, проведені ними арешти або розшукові заходи, про осіб, підозрюваних в агентурних стосунках або таких, що офіційно співробітничали з окупантами. Збір попереджувальної інформації допомагав виводити підпільників з-під ударів німецьких спецслужб. З осені 1943 р. здійснюються спроби запровадити уніфіковану структуру референтури СБ.

Питання організації роботи СБ із захисту лав організації розкривалися у численних інструктивних документах у зв'язку з переходом до боротьби з радянською владою: «СБ – робота», «Інструкція організаційної роботи під кутом совітської окупації України» (січень 1944 р.), «Боротьба з сексотством і провокацією» (жовтень 1944 р.), «Коротка інструкція з розвідки при

допомозі агентури і донощиків контррозвідки».

За умов підпілля та активної роботи проти ОУН спецслужб держав-противників особливе значення надавалося забезпеченню таємності й конспірації у передачі інформації(ця ділянка роботи також покладалася на референтуру СБ).

Для забезпечення надійного і своєчасного надходження інформації від низових ланок підпілля по вертикалі до вищих провідників ОУН створювалися лінії конспіративного зв'язку. Розрізнялися «живий» та «мертвий» засоби зв'язку. Перший здійснювався кур'єрами-жінками на відстань до 10-15 км, кур'єрами- чоловіками – до 50-300 км, спецкур'єрами– до 500 км (як правило, для інформаційного обміну із закордонними центрами ОУН). Для потреб кур'єрських груп на маршрутах влаштовувалися пункти зв'язку (у помешканнях надійних помічників з населення, спеціально обладнаних бункерах, котрим надавалися криптоніми для зашифровки, наприклад, «Яр», «Безодня», «Вулик»). Розроблялися графіки зустрічей, ретельно підбиралися явочні квартири для прийому кур'єрів. «Мертві» пункти зв'язку визначалися для більш конспіративної, безконтактної передачі інформації. У тайники у старих будинках, господарських будівлях, дуплах дерев, під камінням закладалися письмові повідомлення («гріпси», «штафетки»). В обумовлений час повідомлення (часто – зашифровані) вилучалися іншим підпільником та передавалися за належністю.

Оперативність та повнота надходження розвідувальної інформації вирішальним чином залежали від якісного підбору учасників агентурно-інформаторської мережі ОУН. Кандидат на вербування та його близьке оточення попередньо вивчалися. З’ясовувалося ставлення особи до ідей ОУН, хоч в окремих випадках допускалося залучення до співробітництва втемну і тих, хто не поділяв ідей підпілля. «Коротка інструкція з розвідки за допомогою агентів» від 6 вересня 1943 р. наголошувала на необхідності ретельної перевірки роботи інформатора, зокрема, чи справді він має доступ до певної інформації, чи не веде подвійної гри, чи не підсовує

дезінформацію. Оцінювалися також його рівень інтелекту, пам'яті, морально-психологічний стан.

Вербування інформатора СБ закріплювалася підпискою («заявою»). У ній наводилися установчі дані особи, яка «добровільно згоджувалася приступити до служби таємного інформатора СБ». Агент зобов'язувався «доносити сумлінно і чесно як вірний член української нації» про діяльність органів НКВС-НКДБ та осіб, що з ними співробітничають. За невиконання встановлених обов'язків агента карали найвищоюмірою покарання. Агенту також встановлювався псевдонім, і він особисто підписував зобов'язання.

У ході розвідувально-інформаційної діяльності СБ ОУНвиробила власну систему оперативного обліку, спрямовану на збереження й систематизацію одержаних даних. Основною його формою стали картотеки («скоровид-зошити»). Зазвичай, інформація заносилася на картонні картки форматом у півaркуша, що зберігалися у теках або валізах. В інтересах конспірації та запобігання надмірному канцеляризму право вести картотеки надавалося референтам СБ. За оформлення картотеки та інших видів службової документації відповідали технічні референти осередків СБ та спеціальні співробітники – архіваріуси. Для маркування документів СБ вживався індекс «Р-31» угорі зліва на першому аркуші. Встановлювалися ступені таємності–«довірочно», «суворо довірочно» та інші.

До картотеки належало заносити «всі дані про ворогів визвольної революційної боротьби українського народу, про ворожі органи поліції й адміністрації, про агентуру органів поліції, ...всі злочини зроблені супроти українського народу і його визвольно-революційної боротьби органами поліції, совєтської адміністрації та тих, хто вислужувався перед ворогом».Перед постановкою на облік співробітник мусив ретельно перевіряти правдивість відомостей про людину, які заносилися до картотеки, шляхом зіставлення даних різних інформаторів або свідчень підслідних. Приклад рубрик (розділів) картотеки за однією з інструкцій СБ:

І. Виявлена агентура противника («Здемаскована агентура»). Дані про

агентуру радянських правоохоронних органів, здобуті з протоколів допиту або повідомлень працівників та інформаторів самої СБ.

II. Підозрювані в агентурних стосунках з НКВС-НКДБ. Поділялися на декілька категорій : а) особи, які зізналися на слідстві або викриті матеріалами інформаційної служби СБ; б) ті, хто втік з місць попереднього ув'язнення або відбуття покарань; в) особи, що перебували під слідством та звільнені; г) ті, хто повернувся з Німеччини в рамках репатріації; д) особи, що добровільно з'явилися з повинною до правоохоронних органів; Е) особи, які підозрюються у проживання за фіктивними документами; є) громадяни, які до 1941 р. працювали в органах влади та міліції; ж) спеціалісти, що прибули зі східних областей України; з) різні категорії громадян – міліціонери, бійці винищувальних батальйонів, активісти, ремісники-заробітчани, спекулянти та ін. До цього ж розділу вносилися особи, що перебувають у розшуку СБ.

III. Особовий склад органів і військ НКВС-НКДБ, адреси, плани-схеми місцевих осередків цих відомств.

IV.Органи радянської влади, компартії, комсомолу, народної освіти, кооперації.

V. Підпільники, розшифровані перед радянськими правоохоронними органами.

Референт СБ персонально відповідав за збереження документів. Інші підпільники не мали права з ними знайомитися. Про випадки їх втрати слід було негайно доповідати керівникам(зверхникам). Захоплення документів у полонених або ліквідованих есбістів, у бункерах, де переховувалися архіви, часто призводили до відчутних оперативно-бойових ударів радянської сторони. У разі потреби службовий архів вкладали у металеві контейнери (наприклад, молочарські бідони), ховали в тайниках. Про схованки мали знати не більше 5-6 осіб, включаючи референтайархіваріуса.

Інструкція «СБ – робота» наголошувала на ретельній конспірації у веденні службового діловодства. Рекомендувалося окремо зберігати

протоколи допитів, звітну документацію, картотеки, у житлових бункерах (таємних сховищах підпільників) тримати лише поточні справи. СБ контролювала й особисте життя підпільників, що було цілком зрозумілим за умов суворої конспірації, необхідності підтримувати боєздатність руху опору та його репутацію у населення. За розкладання організації, обман зверхників та невиконання наказів члена організації могли стратити, а за аморальні вчинки – виключити з ОУН. Дозвіл на одруження підпільник діставав від окружного провідника після перевірки нареченої есбістами. В «Організаційних вказівках» СБ зазначалося: «Чоловік - підпільник не повинен ходити до жінок у особистих справах. Якщо він іде до жінок у службових справах, то повинен брати з собою свідка... Чоловік, якого здеморалізує жінка, буде покараний пониженням у посаді».

Питанням збереження секретності й конспіративності значна увага приділялася у процесі професійної та виховної роботи з особовим складом СБ, для чого було підготовлено значний обсяг навчально-методичної літератури та програм, на цю тему проводили численні семінари та лекційні курси для есбістів.

Неодноразово перероблялися та перевидавалися такі матеріали, як «Студійно-інформативний матеріал про більшовицькі органи поліції», «Агентура НКГБ в дії», «Більше революційної пильності», «Агентура більшовицьких органів поліції», «Студія психіки об’єкта», «Які прийоми щодо молоді застосовує більшовицька агентура і як перед нею оборонитися» тощо.

Ефективна контррозвідувальна та режимна діяльність стала одним із головних чинників збереження розгалуженої мережі націоналістичного підпілля після відновлення в регіоні радянської влади. Проведена у згаданий період робота зробила Службу безпеки важливим компонентом антирадянського руху опору, здатним до гнучкої перебудови діяльності підпілля відповідно до нових умов його функціонування в Західній Україні в післявоєнний період.

Навесні-влітку 1943 р. була створена Українська повстанська армія, політичне керівництво якою здійснювала ОУН (Б).В УПА також потрібно було організувати захист військової таємниці та забезпечувати режимність своєї діяльності.

Уже в перших наказах, пов'язаних із заснуванням УПА як організованої військової сили, зверталася увага на дотримання режиму таємності. У наказі командувача УПА Д. Клячківського («Клима Савура») від 30 серпня 1943 р. № 8 щодо організації самооборонних підрозділів у запіллі УПА підкреслювалося, що цей процес має відбуватися «з найбільшою тайною, притримуючись загальних засад конспірації». Заходи із забезпечення секретності та недопущення вільного обігу інформації поширювалися й на населення зайнятої УПА території. Наказ Д. Клячківського від 1 вересня 1943 р. №9 зобов'язував брати на облік й контроль усі наявні в населення засоби радіозв'язку, приймачі та спеціалістів з радіозв'язку.

Вже 10 вересня 1943 р. з'явився наказ командувача УПА № 10 «Про зберігання військових таємниць». У ньому констатувався вкрай незадовільний стан із забезпеченням секретності у бойовій діяльності та побуті повстанців. Зазначалося, що у штабах частин УПА панує безлад, не запроваджено умови для зберігання секретних документів, до них мають доступ випадкові люди (навіть таємні матеріали викидаються на смітник), вояків УПА не виховують у дусі дотримання військової таємниці. Наказ вимагав: завести «скритки» (сейфи, шафи тощо) для зберігання таємних документів у штабах та помешканнях керівного складу; обмежити коло осіб, з якими й у присутності яких обговорюються таємні справи; усі помешкання штабів та командні пункти «суворо законспірувати»; вжити заходів до належного зберігання секретної документації карт, не потрібну документацію спалювати; запровадити шифри і коди для забезпечення секретності у паперових повідомленнях, радіопереговорах тощо;засекретити місця дислокації частин і загонів УПА;щоденно виділяти 10-20 хвилин для проведення виховної роботи з особовим складом, роз'яснення значення та

способів зберігання військової таємниці;бойові накази віддавати безпосередньо перед початком операції;зберігати у таємниці від населення плани з передислокації військ; ввічливо ставитися до населення, не допускати утисків мирних мешканців, підтримувати авторитет повстанців;відповідальність за дотримання таємниці покласти особисто на командирів та функціональних начальників.

Наказ командирам Груп та військово-територіальних формувань УПА від 30 жовтня 1943 р. № 19 також наголошував на підвищенні військової дисципліни (аж до скасування відпусток повстанцям з метою профілактики розголошення таємниці перед населенням), посиленні уваги до збереження таємниці та навчання вояків методам конспірації.

Вимоги командування УПА у сфері забезпечення таємності дублювалися й конкретизувалися у розпорядчих документах територіальних з'єднань УПА. Наприклад, наказ із дисциплінарних справ командира групи УПА «Заграва» від 15 серпня 1943 р. №8 приписував домогтися точності й конспіративності у виконанні завдань, забезпечення належного зв'язку, реєстрації усіх зашифрованих повідомлень («грипсів»).

Вживалися заходи із виховання у повстанців (здебільшого – сільських хлопців, які не служили у війську) свідомого ставлення до дотримання режимності, навчання їх навичок зберігання таємниці, пильності. Зокрема, наказ про політичну роботу в УПА від 26 листопада 1943 р. № 22 вимагав при проведенні вишколу й виховної роботи звертати особливу увагу на ознайомлення із методами конспірації (особливо це стосувалося зв'язківців, кур'єрів та ін.). Про відповідальне ставлення до військової таємниці йшлося і в інструкції для пропагандистів-виховниківсуспільно-політичної референтури УПА (10 червня 1943 р.).

Після повернення радянських військ на Правобережну Україну (кінець 1943 - початок 1944 рр.) командування УПА докладає додаткових зусиль із забезпечення таємності й конспіративності у бойовій діяльності та нелегальній роботі. Наказ командувача УПА від 6 січня 1944 р. № 29,

присвячений новим принципам роботи у «совєтських умовах», вимагав посилити конспірацію місць дислокації повстанських сил, особистості підпільників, запровадити секретні лінії зв'язку, широко вживати у листуванні та зв'язку умовності, шифри, підбирати надійних людей для роботи на лініях зв'язку, а також розгорнути «безпощадну боротьбу з сексотами і ворожим агентами». Перехід до масового будівництва підземних та інших прихованих сховищ для підрозділів УПА, шпиталів, складів тощо викликав появу окремого наказу від 25 листопада 1943 р. про дотримання таємниці підземних помешкань.

Активізація оперативної діяльності радянських спецслужб змушувала вдаватися до додаткових режимних заходів. Оперативна інструкція УПА від 7 вересня 1944 р. вимагала від повстанців звернення один до одного лише за військовими званнями, забороняла обговорювати деталі бойових дій перед місцевим населенням та спілкування з вояками інших загонів, звертала увагу на необхідність забезпечення таємності на марші та під час постою.

У липні 1944 р. з'явилася окрема Інструкція з конспірації. Вона рекомендувала повстанцям та підпільникам:постійно навчатися навичок конспірації та обережно підходити до визначення кола спілкування;обирати псевдонім, застосовувати різні псевдо під час перебування на різних теренах;контролювати зберігання таємниці підлеглими, суворо перевіряти на предмет дотримання таємності;не розкривати організаційних таємниць навіть перед вищими командирами і провідниками;не вести зайвих записів, систематично знищувати не потрібну документацію, ретельно переховувати архіви.

Потреби надійного контррозвідувального забезпечення бойових дій зумовлювали проведення заходів з відповідної підготовки особового складу (наприклад, інструкції для УПА «Вояцький стан та його обов'язки» та «Організація армії» 1944 року). Крім того, під час вишколу кандидатів на старшинські (офіцерські) посади на опанування мистецтвом спеціальних заходів відводилося 14 годин, з них 4 – на закордонну розвідку, 4 – на

контррозвідку, стільки ж – на опанування методамипильності й конспірації, по годині – на військово-польову жандармерію й судову справу. За програмою підстаршинськоговишколу Групи УПА «Захід» (травень 1946 р.) на розвідувальну справу відводилося 14 годин, із них 4 – на польову розвідку, 2 – на історію радянських органів держбезпеки, по годині – на основи агентурно-оперативної роботи, контррозвідку, шифрувальну справу тощо.

Варіант навчальної програми для «кандидатів на старшин УПА» у розділі «Розвідка» передбачав студіювання таких проблем, як «революційна пильність і конспірація», «протидія шпигунству та диверсії», устрій розвідувальних служб іноземних держав, організація військово-польової жандармерії та польового судочинства.

«Інструкція розвідної і контррозвідчої служби» (груднь 1944 р.) чимало уваги приділяла організації зв'язку, вважаючи його «одним з найважливіших чинників в розвідній роботі». У ній зазначалося, що передача розвідінформації повинна бути своєчасною, достовірною, конспіративною, вестися винятково за надійними лініями зв'язку із застосуванням шифрів і кодів. Також інструкцією визначалися єдині форми діловодства спецслужб, встановлювалася схема агентурного повідомлення із зазначенням оперативного працівника, що його прийняв, та оперативного джерела, висновків за інформацією, плану наступнихагентурно-оперативних заходів, розяснювався спосіб ведення агентурної справи, яка містила певну тематичну інформацію.

Документи повстанського руху свідчать про велику увагу командування до підтримки внутрішньої безпеки, захисту військової таємниці, підтримки внутрішнього порядку, розглядаючи їх серед основних чинників забезпечення високої боєздатності.

Навіть присяга вояка УПА (затверджена наказом ГВШ ч. 7 від 19 липня 1944 р.) закликала повстанця бути «революційно-пильним», суворо зберігати військову і державну таємницю. Розроблялася низка нормативних

документів, спрямованих на безпосередній захист місць дислокації та засобів зв'язку. Інструкція «Протишпигунське забезпечення постою» визначала заходи із забезпечення безпеки розквартирування повстанських підрозділів (заборона розголошувати справжнє найменування підрозділів, розмовляти з місцевим населенням зі службових питань тощо). Положення «Конспіративно-розвідчого вишколу», зокрема, наголошували на повсякденному застосуванні шифрів і кодів у службовому діловодстві, переговорах на лініях зв'язку, організації контрспостереження навколо місць розташування повстанців. Документ «Оборона проти ворожого підслуху» визначав вимоги щодо забезпечення конспіративності у користуванні телеграфно-телефонними лініями.

В УПА та озброєному підпіллі ОУН знайшли широке застосування різноманітні системи шифрування інформації. Серед найбільш уживаних були такі:простий шифрувальний квадрат;складний шифрувальний квадрат;шифрування за допомогою підпільної або іншої (нейтральної) літератури;шифрування цифровим ключем;шифрування за допомогою заміни літер;застосування «шифрувальної решітки»;тайнопис.

Були також розроблені відповідні навчально-методичні документи стосовно роботи СБ в УПА, зокрема: «Як підбирати працівників СБ», «Праця розвідника всередині», «Коротка інструкція відносно розвідки при помочі агентів і донощиків контррозвідки», «Способи вербування інформаторів».

Ці документи, крім питань діяльності контррозвідувальної служби розкривали специфіку боротьби зі шпигунами й диверсантами противника, порушниками норм збереження військової таємниці, дисципліни й моралі, саботажниками й непевними елементами у власних лавах.

До основних завдань контррозвідувальної служби, належали: оперативне спостереження («обсервація») за рядовим і командним складом УПА, який перебуває у бойових підрозділах «чи по спеціальних справах», новобранцями, цивільним населенням у місцевостях маршів або дислокації; контррозвідувальні операції;допит підозрілих у здійсненні ворожої

діяльності або «викритих на шпигунській роботі»;проведення відкритих або негласних перевірок підозрілих на плановій основі.

При контррозвідувальному нагляді за вояками УПА рекомендувалося звертати увагу на такі обставини або окремі категорії осіб: родинні та приватні зв'язки з населенням;характер стосунків у військовому середовищі та під час відпусток, особисте листування;минуле людини, мотиви вступу до УПА; при цьому особливу увагу необхідно було звертати на тих, що влилися до повстанців у 1944 р., дезертирів з Червоної армії «без різниці на їх попередні заслуги», втікачів від органів НКВС, таборів і примусових робіт;осіб, які перебували під арештом, мали контакти з радянськими правоохоронними органами, або таких вояків, рідні яких імовірно пов'язані з органами держбезпеки; вояків, поведінка яких виявляється підозрілою, таких, що мають стосунки з дезертирами або «ухильниками» від служби в УПА; вояків підрозділів спеціального призначення та забезпечення (зв'язкові, господарчі працівники та інші), котрі мають змогу за умовами служби певний час перебувати поза контролем командирів.

Документами визначалися також ознаки, що свідчили про належність вояків УПА до «непевних елементів», серед них: критичні висловлювання щодо доцільності боротьби, її перспективи, зневіра у перемогу УПА, поширення панічних настроїв; невиконання наказів командирів; підозріла поведінка у критичних ситуаціях;розголошення військової таємниці (додавався перелік з 18 пунктів для її конкретизації); моральний стан, ставлення до військового майна;спроби дезертирства. Разом з цим, суворо заборонялося контактувати з причетними до НКВС особами, залишати на полі бою поранених, відвідувати цивільним особам місця дислокації повстанців, фотографувати підрозділи й осіб, пов'язаних з повстанцями, розголошувати маршрути пересування та інші відомості, що мали характер військової таємниці.

Крім цього, апарат СБ здійснював контррозвідувальне забезпечення конспіративних ліній зв'язку. Пропонувалося на пунктах зв'язку

розташовувати співробітників СБ з правами перлюстрації підпільної кореспонденції та перевірки надійності кур'єрівзв'язку.

Отже, основні завдання СБ в УПА принципово не відрізнялися від завдань СБ ОУН, хоча були більше наближені до потреб бойової практики. СБ УПА вимагала від вояків співпрацювати й безумовно виконувати всі доручення есбістів. Командири і провідники, що приймали нових учасників ОУН та УПА без попередньої перевірки їх СБ, прирівнювалися до «явних ворогів». СБ УПА запроваджувала посилене режимне забезпечення місць перебування командного складу УПА. СБ мала виконувати і функції навчально-методичного осередку навчання повстанців секретності й конспіративності. Зокрема, 24 жовтня 1944 р. вийшов наказ про необхідність збору силами референтур СБ літератури з проблем розвідки, контррозвідки, криміналістики, психології і навіть детективних романів.

Вояки УПА могли каратися смертю кара за дезертирство, розголошення військової таємниці, крадіжки, невиконання наказів, надмірне вживання алкоголю. «Правила польової жандармерії при УПА» від 16 січня 1944 р. передбачали «кару смерті» за «зраду військової тайни».

Дбаючи про перетворення УПА у повноцінну, згуртовану бойову силу, яка б користувалася повагою та підтримкою населення, її тодішній командувач Д. Клячківський 15 травня 1943 р. підписав наказ, який містив перелік «тяжких злочинів» проти українського народу, його влади, окремих громадян та їхнього майна. За їх скоєння до осіб, котрі досягли 17-річного віку, могла застосовуватися «найвища кара військового часу – смерть». Серед таких злочинів називалося і шпигунство, яке трактувалося як вивідування військових, економічних таємниць, збір відомостей щодо настроїв населення.

Таким чином, у 20-40-х роках 20 століття у націоналістичному русівідбулосяорганізаційне оформлення підрозділівконтррозвідувального спрямування, які також забезпечували захист інформації з обмеженим доступом, зокрема, про учасників підпільного руху, внутрішню безпеку та

конспірацію. Специфікою діяльності цих органів було й те, що діяли вони в умовах ворожого оточення та відсутностівласної держави.

Питання для самоконтролю до розділу1

1. Дайте характеристику організації захисту інформації з обмеженим доступом в Київській Русі.
2. Охарактеризуйте стан захисту інформації на території України в період литовсько-польського панування.
3. Порівняйте особливості захисту інформації в Запорозькій Січі та державі Богдана Хмельницького.
4. Розкрийте питання організації захисту інформації на території України в XVII-XIX ст.
5. Охарактеризуйте досягнення українських урядів з питань організації захисту інформації в період національно-визвольних змагань 1917-1921 рр.
6. Розкрийте еволюцію утворення та форгенезис української радянської системи захисту інформації (1920-1930 рр.).
7. Розкрийте принципи діяльності розвідувальноїреферентури УВО.
8. Охарактеризуйте діяльність спеціального розвідувального та контррозвідувального підрозділу ОУН. Яким чином здійснювався контррозвідувальний захист підпілля.
9. Розкрийте специфіку діяльності Спеціального підрозділу ОУН референтуриСлужби безпеки. Розкрийте протинімецькі заходи СБ ОУН.
10. Розкрийте питання забезпечення таємності й конспірації у передачі інформації в ОУН. Охарактеризуйте систему оперативного обліку в ОУН.
11. Опишіть організацію захисту військової таємниці та режимність у діяльності УПА.
12. Розкрийте контрозвідувальне забезпечення бойових дій в УПА. Розкрийте принципи діяльності СБ УПА.
13. Охарактеризуйте боротьбу УПА зі шпигунами і диверсантами, порушниками норм збереження військової таємниці.

Література

1. Антонюк Я.М. СБ ОУН (б) на Волині та Західному Поліссі (1946-1951 рр.). – Луцьк: Ключі, 2013. – 256 с.
2. Васюта І.К. Національно-визвольний рух у Західній Україні (1918-1939 рр.) // Український історичний журнал. – 2001. – № 6. – С. 36-37.
3. Вєдєнєєв Д.В. «Бункерна війна» в Західній Україні у 1940-1950-х роках // Сторінки воєнної історії України. – 2003. – Вип. 7. – Ч.ІІ. – С. 77-88.
4. Вєдєнєєв Д.В. Військово-польова жандармерія - спеціальний орган Української повстанської армії // Воєнна історія. – 2002. – № 5-6. – С.32-40.

5. Вєдєнєєв Д.В. Захист секретних відомостей у військових формуваннях руху українських самостійників-державників (1920-1950-ті рр.). Науковий огляд. К., НА СБ України, 2014. Інв.418/426 (р/н29/20-2605 від21.03.2014). – 35 с.

6. Вєдєнєєв Д.В. Погляди ОУН (Б) на місце органів безпеки у структурі Української самостійної держави (1940-1941 рр.) // Наукові записки Інституту політичних і етнонаціональних досліджень НАНУ. – 2002. – Вип. 18. – С. 230-236.

7. Галузевий державний архів СБ України. – Ф. 2, 13,16.

8. Гуз А.М.Історія захисту інформації в Україні та провідних країнах світу. Курс лекцій. – К., 2006. – 208 с.

9. Гуз А.М.Історія захисту інформації в Україні та провідних країнах світу. Навчальний посібник. – К., 2007. – 260 с.

10. Кентій А. В. Українська повстанська армія в 1942 - 1943 рр. – К.: Інститут історії України НАН України, 1999. – 350 с.

11. Кентій А.В. Українська військова організація (УВО) в 1920-1928 рр. Короткий нарис. – К.: Ін-т історії України НАН України, 1998. – 250 с.

12. Літопис УПА. Нова серія. – Київ-Торонто, 1999. – Т.3. – С.12-239.

13. Літопис УПА. Нова серія. – Київ-Торонто, 2006. – Т.18. – С.413-841.

14. Мечник С. У боротьбі проти московської агентури. – Мюнхен: Українське видавництво, 1980. – С.13.

15. Мірчук П. Нарис історії ОУН. – Мюнхен, Б.в., 1968. – Т.1. – 350 с.

16. Мудрик-Мечник С. ОУН в Україні і за кордоном під проводом С. Бандери. – Львів: Галицька Видавнича Спілка, 1997. – 270 с.

17. ОгородникВ.Ю. Підготовка кадрів Служби безпеки Організації українських націоналістів (бандерівців) (1941-1951 рр.). Автореферат дис. канд. істор. наук. 07.00.01. – К.: КНУ імені Тараса Шевченка, 2009. – 16 с.

18. Організаційно-правові основи захисту інформації з обмеженим доступом/ Навч. посібник. За редакцією Сідака В.С. – К., 2006. – 232с.

19. Організація захисту інформації з обмеженим доступом» / Є.Д.Скулиш, А.М.Гуз, О.Д.Довгань, А.І.Марущак, І.П. Касперський, О.М. Солодка та ін. .– К., Вид-во. НА СБ України. 2011. – 378 с.

20. Ремесло повстанця. Збірник праць підполковника УПА Степана Фрасуляка - Хмеля». – Львів: ЦЦВР, 2007. – С.269.

21. Сідак В.С. Спецслужби України часів національної революції 1917 - 1920 р.р. Навчальний посібник. – К., 1994. – 184с.

22. Сідак В.С., Степанков В.С. З історії української розвідки та контррозвідки. – К., 1994. – 201 с.

23. Сідак В.С., Степанков В.С. Історія української розвідки та контррозвідки (нариси). – К., 1994. – 402 с.

24. Ткаченко Н.С. Повстанческая армия (тактика борьбы). – Минск: Харвест; М.: АСТ, 2000 – С. 376.

25. Центральний державний архів вищих органів влади та управління

України. – Ф.3833, 3836, 3837,3838. – Оп.1, 2.
26. Центральний державний архів громадських об’єднань України. – Ф.1. – Оп.23; – Ф.57. – Оп.4; – Ф.62 – Оп.1.

РОЗДІЛ 2

ЗАГАЛЬНОТЕОРЕТИЧНІ ЗАСАДИ ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

2.1 Поняття інформації та її ознаки

Визначаючи право на інформацію в якості самостійного об'єкту захисту, було б безнадійно намагатися захищати усю інформацію. Для ефективнішого вирішення завдань нормотворчості і правового захисту інформації вже досить давно було запропоновано в якості об'єкту захисту брати лише інформацію з обмеженим доступом права на неї. Ще в Радянському Союзі склалася певна система захисту інформації з обмеженим доступом, в якій виділяли три види такої інформації:державна таємниця (інформація з грифами «особливої важливості», «цілком таємно»), службова таємниця (інформація з грифом «таємно») та інформація «для службового користування».

Механізм захисту ґрунтувався на вільному принципі права, тоді як уся інформація мала обмежений доступ. У кожному конкретному випадку посадовець (чиновник) приймав рішення про доступ до інформації, входило в пряме протиріччя з нормами міжнародного права і не дозволяло успішно реалізувати право кожного на отримання інформації.

З метою більш ґрунтовного дослідження змісту поняття «службова інформація в сфері діяльності органів публічної влади України» звернемося до етимологічного, доктринального та нормативного поняття «інформації», яке є родовим по відношенню до досліджуваного та інших суміжних понять з досліджуваним нами, зокрема поняття «таємниця».

Енциклопедичні видання визначають інформацію досить загально, виходячи із базових установок даного поняття. Так, в узагальненому значенні, за філософським словником «інформація» являє собою «певні відомості, сукупність будь-яких даних, знань».

В словнику іншомовних слів, за редакцією члена-кореспондента АН України О.С.Мельничука, термін «інформація» (від лат. informatio) перекладається як роз'яснення, повідомлення про щось.

Налічується значна кількість доктринальних підходів до поняття «інформація».

Стосовно цього розрізняються два аспекти існування інформації як окремої категорії. По-перше, це структурна інформація. Вона являє собою міру впорядкованості чи організації певної системи або процесу. По-друге, інформація пов'язанаб езпосередньо з процессом відображення як у матеріальному світі, так і в нематеріальному. Уразі якщо предмет змінюється, що є результатом (відображенням чи віддзеркаленням) дії предмета іншого, то перший є носієм інформації про другий. На відміну від неживої природи, де таке віддзеркалення є пасивним, оскільки являє собою простий механізм констатації даних, для об'єктів живої природи, і передусім для людини, такий процесс має активний характер і пов'язаний як зі сприйняттям інформації, так і з її аналізом, переробкою та переданням.

Зауважимо, що введення терміна «інформація» в ряд наукової категорії відбулося не одразу. Перші інформаційні теорії в науці виникають у 50-ті роки як вірогідно статистичні напрямки.

Початківцем наукового обґрунтування інформації як категорії був К. Шеннон. Він вважав, що інформацію слід характеризувати через її «кількість». У результаті цього під інформацією почали розуміти не будь-які відомості, а лише ті, які зменшують або знижують складену невизначеність щодо їх отримання, тобто інформація – це ступінь заперечення невизначеності в результаті передачі повідомлень.

Проте пізніше виявилося, що такий підхід визначає інформацію не всебічно, а надає виключно її кількісну характеристику.

Подальше вивчення інформації як багатогранного явища підштовхнуло вчених до спроби охарактеризувати її з погляду виконання нею статистичної функції. Найбільш повноце вдалося зробити вченим-кібернетикам. Вони

пояснювали свою позицію щодо інформації тим, що в усіх системах, які є самоорганізованими, зовнішні сигнали, перш ніж бути сприйнятими, перетворюються і стають здатними для сприйняття. Протягом останніх кількох десятиліть ми спостерігаємо, що інформаційна революція почала змінювати сааме джерело добробуту. Тому все вагомішим стає не матеріальний бік існування, а знання, застосовуване для створення цінностей, бізнесу і добробуту.

Середовище, в якому створюється інформація, дужевідрізняється від індустріального, яке будується на основі матеріальних ресурсів. Інформація функціонує в різних формах – від потоків даних, що мають короткострокове значення, до даних довгострокових, накопичених за роки досліджень, які зберігаються в бібліотеках, архівах, у пам'яті комп'ютерів або фахівців.

Сьогодні удосконалюються основи створення інформаційної бази, оскільки з'явилася нова техніка, маємо досконалі програмні платформи, є можливість в електронномувигляді швидко користуватися й обмінюватися інформацією, з'явилися провайдери, комунікаційні мережі, Інтернет тощо. Ось чому сьогодні багатоуваги приділяється як на теоретико-методичному, так і на практичному рівнях функціонування інформаційній сфері діяльності. Слід зазначити, що практиків в інформаційній сферіді яльності набагато більше, тому теоретичні наробки, методичні рекомендації відстають від потреб практики.

Є різні рівні споживання інформаційної складової – державні, галузеві, регіональні, рівень підприємств, фірм та організацій, а також рівень фізичної особи. Створення інформаційної бази для кожного рівня має свої особливості як на стадіях розробки інформаційно-пошукових систем у разі створення БД і електронних масивів інформації, їх наповнення, так і на стадіях створення зручного, реального доступу.

Дослідження інформації з позицій вірогідно-статистичної теорії також не дало змоги здійснити повний аналіз поняття «інформація», оскільки ця теорія не дає якісної характеристики цього поняття. Вірогідне розуміння

інформації та її кількості, притаманне статистичній теорії, не відтворює суті багатьох процесів, у тому числі й процесів інформаційної діяльності суб'єктів господарювання.

Надалі почали розвиватися теорії розгляду інформації як базису для передбачення, як міри неоднорідності розподілу матерії та енергії в просторі й у часі тощо.

Іноді інформацію визначали як зміст категорії, що відтворює дійсність, або як категорію, що поєднує в собі відтворення розмаїтості дійсності. Оскільки здатністю відтворювати існуючу дійсність володіє людська свідомість, то в цьому випадку термін «інформація» найбільш близький за своєю сутністю до терміна «знання». Але знання – нелише певні відомості, їх сукупність і факт володіння ними. Цим характеризується тільки статичний бік інформації. Інформація ж відтворює процесс динаміки та циркуляції раніше набутих, отриманих і переданих далі знань, що і виділяєїї з усієї різноманітності понять, які стоять поряді з нею.

На нашу думку, у своїй єдності всі ці характеристики оцінювали лише окремі функції інформації, не обґрунтувавши при цьому єдиного і всеохоплюючого її поняття.

Один із засновників кібернетики Н. Вінер розглядав інформацію як специфічну субстанцію, відмінну як відматеріального, так і відідеального, стверджуючи, що «інформація – це ані матерія, ані енергія».

Отже, кожне з цих визначень істинне, але лише в контексті завдання, яке виконує інформація в певній галузі діяльності.

Наприкінці XX ст. соціальне значення інформації значно зросло, а сааме поняття інформації почало сприйматися поіншому. На це вплинули процеси формування та становлення «інформаційного суспільства», тобто суспільства, що передусім характеризується швидко зростаючою та все пронизуючою інформацією про різні сферижиттєдіяльності цього суспільства. Найважливішими рисами, що характеризують соціальний і політичний стан, а також рівень розвитку інформаційногосуспільства, є:

«інформованість населення, безперешкодна робота всіх служб масової інформації та їх здатність збирати і передавати об'єктивні відомості та їх оцінки; а також, що не менш важливо, інтерес до їх роботи у всіх верствах народу, доступність інформації та наявність технічних засобів, що дозволяють їїо тримати».

Є й інші підходи до визначення поняття "інформація". Наприклад, у роботі авторів А.С. Гальчинського, В.М. Геєць, А.К. Кінаха, В.П. Семиноженка визначено, що "інформація є характеристика, що здійснюється, аналізується через системні взаємодії і відносини свідомості, властивої творчій особистості людини". Дехто з дослідників вважає за норму відсутність єдиного підходу до визначення терміна "інформація", тому наврядчи є потреба шукати загальне його визначення, яке б охоплювало багато векторність його застосування. Мабуть, на сьогоднішньому етапі розуміння терміна "інформація" слід використовувати юридичні норми, які маємо в законах України і державних стандартах.

Узагальнюючи існуючі наукові позиції, беззаперечним у комплексному розумінні дефініції «інформація», на нашу думку, є те, що інформація – це певні відомості, які можуть накопичуватися, передаватися, оброблятися та використовуватися. Разом із тим це і сукупність відомостей, повідомлень, матеріалів та даних, виражених у відповідних формах, що визначають міру потенційних знань про процеси або явища в їх взаємозв'язку. А критерієм визначення інформації як наукової категорії є сукупність її функцій, цілей і завдань, виконання яких передбачене тією або іншою наукою.

На сьогодні категорія «інформація» є однією з найпоширеніших не тільки в науці, а й на практиці. І все це незважаючи на невизначеність та дискусійний характер самого визначення поняття інформації. Багато в чому ця дискусійність пов'язана зі специфічним характером принципів та методів вивчення й використання інформації в різних галузях науки і практики. Ці розбіжності проявляються у сприйнятті самої інформації, у визначенні форм її прояву в матеріальному світі, її місця у певних системах світогляду, її ролі

у функціонуванні індивідів, суб'єктів господарювання, держави та суспільства в цілому.

Основним законодавчим актом при нормативному підході до визначення поняття інформація є, безумовно, Закон України «Про інформацію», стаття 1 якого визначає інформацію як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Через розмаїтість підходів щодо визначення поняття «інформація» і поглядів учених на розв'язання чисельних наукових інформаційних проблем, надати визначення поняття «інформація», щоб відповідало всім критичним зауваженням є занадто складним завданням.

Ми підтримуємо думку Р.С. Бєлкіна, що загальне визначення інформації може мати лише гносеологічний чи науковий характер. Будь-яке визначення має відображати функціональне призначення інформації. Саме тому для більш повного розкриття поняття «інформація», слід окреслити ознаки, властивості інформації як феномену.

Уперше на науковому рівні про ознаки інформації висловився А.Б. Венгеров, зокрема вчений навів такі ознаки інформації:

- самостійність інформації по відношенню до свого носія;
- можливість багаторазового використання однієї і тієї самої інформації;
- вона не зникає при споживанні;
- збереження інформації, що передається, у суб'єкта, що її передає;
- здатність до збереження, агрегування, інтегрування, накопичення, «стискання»;
- кількісна визначеність інформації;
- системність.

Мацюк В.Я. також акцентує увагу, що інформація, як товар, має особливості, що вирізняються від матеріальної речі: інформація виступає як об'єкт нових правовідносин, після її передачі, вона зберігається: у особи, що

її передає та одночасно з'являється в того, хто її прийняв, тобто вона належить одночасно двом суб'єктам, при цьому зберігаючи свій правовий статус характеристикою не відчуженості від виробника, від володіння споживача.

Інтенсивний розвиток наукових досліджень інформаційної проблематики сприяв виокремленню нових ознак інформації.

Так, Кормич Б.А. виділяє ряд властивих суспільно-правових характеристик інформації: по-перше, інформацією з правої точки зору можуть вважатися лише ті дані, які є систематизованими у формі, що робить їх придатною до передачі, тобто, інформацією є дані, документовані на фізичних носіях або публічно оголошені в усній формі чи за допомогою відповідних технічних засобів; по-друге, дані стають інформацією лише в певному контексті і лише в тому випадку, коли вони зрозумілі людям. Крім того, автор зазначає, що кожна конкретна інформація також має певні індивідуальні характеристики, до яких відносяться її кількість, зміст та цінність.

Н.О. Дементій, не пояснюючи сутність визначених властивостей інформації, зазначає, що крім кількості, цінності та змісту, інформація має й інші властивості – правдивість, достовірність, повноту, глибину, точність, доказовість, ефективність, новизну, оперативність, отриманість, надійність.

В.А.Копилов виокремлює такі ознаки інформації як фізична невідчужуваність, здатність до тиражування, екземплярність, відособленість, властивість інформаційної речі.

В.Н.Лопатін та І.Л.Бачило виділяють системний характер, трансформованість, невичерпність, субстанційну несамостійність, селективність, здатність до обмеження, універсальність.

О.В.Кохановська зазначає про нематеріальний характер інформації та про таку ознаку інформації як те, що вона є благом неспоживчим, яке піддається лише моральному, але не фізичному старінню, а також

самостійність по відношенню до носія, можливість багаторазового використання.

Цікаву та важливу ознаку інформації виділяє Антопольский А.А., зокрема суб'єктивний характер – інформація виникає в результаті діяльності суб'єкта, що володіє свідомістю. Але, на нашу думку, доречно доповнити, що інформація виникає не просто в результаті діяльності суб'єкта, що володіє свідомістю, а є результатом інтелектуальної діяльності суб'єкта. Саме тому слід зазначати про таку ознаку інформації як її інтелектуальність.

Письменський А. А. вказує ще на одну особливість інформації, що полягає в тому, що на відміну від споживання матеріалів чи енергії, яке призводить до збільшення ентропії у Всесвіті, використання інформації призводить до протилежного ефекту – воно збільшує знання людини, підвищує організованість в оточуючому середовищі та зменшує ентропію.

Неординарністю відзначається думка Марценюка О.Г., який зазначив, що в той час як угоди з приводу матеріальних речей призводять до конкуренції, інформаційний обмін призводить до співробітництва.

Таким чином, перелік ознак інформації як феномену є доволі значним та їх виокремлення залежить від багатьох факторів.

2.2. Інформація з обмеженим доступом у доктрині та праві

Вся інформація за режимом доступу, відповідно до Закону України «Про інформацію» поділяється на відкриту та з обмеженим доступом (див рис. 1).

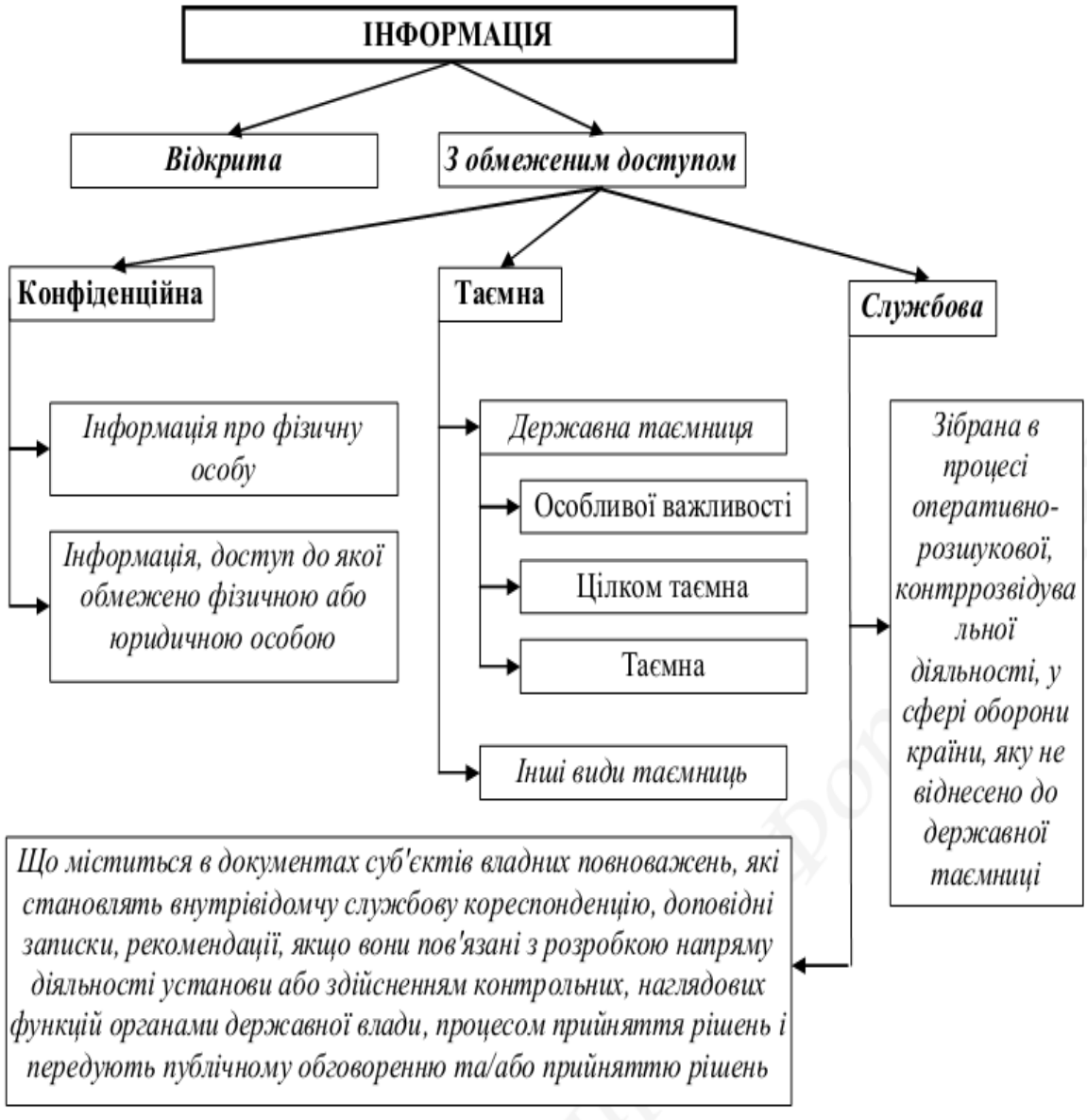


Рис. 1. Види інформації за режимом доступу

Джерело: розроблено відповідно до Закону України «Про інформацію».

Відповідно до ст. 38 Закону України «Про інформацію» інформація поділяється навідкриту інформацію та інформацію з обмеженим доступом. На сьогодні термін «інформація з обмеженим доступом» законодавчо невизначений. Лише у міжнародній Угодіміж урядом України та Урядом Республіки Білорусь про співробітництво в галузі технічного захисту інформації закріплене подібне визначення «Інформація обмеженого доступу–

інформація, право доступу до якої обмежено відповідно до національних законодавствдержав Сторін».

Також в Угоді між Кабінетом Міністрів України та Урядом Словацької Республіки про взаємну охорону інформації з обмеженим доступом закріплено інше визначення: «інформація з обмеженим доступом» – інформація у будь-якій формі та будь-які документи, матеріали, вироби, речовини або фізичні поля, на/в яких представлена інформація, яка в інтересах національної безпеки держав Сторін та відповідно до їх національного законодавства підлягає охороні від несанкціонованого доступу, включаючи інформацію, яку спільно створено юридичними особами держав Сторін в рамках співробітництва та доступ до якої обмежено на основі вимог національного законодавства держав Сторін та відповідно до критеріїв цієї Угоди.

Угода між Україною та Угорською Республікою про взаємну охорону інформації з обмеженим доступом також містить визначення поняття «інформація з обмеженим доступом», згідно з яким це будь-які дані незалежно від їхньої форми представлення, виду та умов відтворення, що потребують охорони від несанкціонованого доступу та доступ до яких обмежено будь-якою з Договірних сторін відповідно до свого національного законодавства.

Більш стисле визначення інформації з обмеженим доступом містить Угода між Україною та Республікою Словенія про обмін та взаємну охорону інформації з обмеженим доступом: інформація, яка за законодавством кожної Договірної сторони потребує охорони від розголошення, незаконного заволодіння чи втрати, та визначена такою незалежно від її форми.

Інший підхід до визначення цього поняття використаний в Угоді між Кабінетом Міністрів України та Урядом Алжирської Народної Демократичної Республіки про охорону інформації з обмеженим доступом, де закріплено, що інформація з обмеженим доступом означає будь-який документ, рисунок, план, карту, фотографію, звукову чи відеоплівку або

інший документ чи інший носій інформації, що містять інформацію, якою обмінюються Сторони в рамках їхньої діяльності, і розголошення якої може завдати шкоди відповідним інтересам та/або безпеці однієї з двох держав.

У одній із останніх угод – Угоді між Кабінетом Міністрів України та Урядом Республіки Македонія про взаємну охорону інформації з обмеженим доступом, закріплено, що інформація з обмеженим доступом – інформація, відображена в будь-якій формі, що охороняється відповідно до національного законодавства Договірних сторін та передана в порядку, встановленому кожною з Договірних сторін і цією Угодою, розголошення якої може завдати шкоди безпеці та інтересам держав Договірних сторін.

На основі аналізу вищезазначених визначень поняття інформації з обмеженим доступом, можна прийти до висновку, що здебільшого в міжнародних документах акцентується увага на певних матеріальних носіях, де може міститися інформація, а не на визначенні сутності що є такою інформацією.

Що стосується інших категорій, змістовно пов’язаних з інформацією з обмеженим доступом, наведемо окремі їх визначення. *Конфіденційна інформація* - інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов.

Таємна інформація - інформація, доступ до якої обмежується відповідно, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю.

До *службової* може належати така інформація:

1) що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи

або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Кожна особа має право:

1) знати у період збирання інформації, але до початку її використання, які відомості про неї та з якою метою збираються, як, ким і з якою метою вони використовуються, передаються чи поширюються, крім випадків, встановлених законом;

2) доступу до інформації про неї, яка збирається та зберігається;

3) вимагати виправлення неточної, неповної, застарілої інформації про себе, знищення інформації про себе, збирання, використання чи зберігання якої здійснюється з порушенням вимог закону;

4) на ознайомлення за рішенням суду з інформацією про інших осіб, якщо це необхідно для реалізації та захисту прав та законних інтересів;

5) на відшкодування шкоди у разі розкриття інформації про цю особу з порушенням вимог, визначених законом.

Обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог:

1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

2) розголошення інформації може завдати істотної шкоди цим інтересам;

3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

3. Інформація з обмеженим доступом має надаватися розпорядником інформації, якщо він правомірно оприлюднив її раніше.

Суб'єктами права власності на інформацію є громадяни, юридичні особи, держава.

Власник інформації щодо об'єктів своєї власності має право здійснюватибудь-якізаконнідії.

Інформація може бути об'єктом права власності як у повному обсязі, так і володіння, користування чи розпорядження нею окремо.

Підстави для виникнення права власності на інформацію:

- створення інформації власними силами і за свій рахунок;

- договір на створення інформації, договір, що містить умови переходу П. в. на і. до іншої особи (наприклад, купівля, продаж, поставки та ін.).

Інформація, створена кількома громадянами або юридичними особами, є їхньою колективною власністю. Порядок і правила користування такою власністю визначаються договором, укладеним між співвласниками.

Інформація, створена організаціями (юридичними особами) або придбана ними іншим законним способом, є власністю цих організацій.

Інформація, створена на кошти державного бюджету, є державною власністю.

Інформація, створена на правах індивідуальної власності, може бути віднесена до державної власності у разі передачі її на зберігання у відповідні банки даних, фонди або архіви на договірній основі.

Власник інформації має право визначати правила доступу до неї, правила обробки її, призначати особу, яка здійснює володіння, використання і розпорядження інформацією та інші дії щодо неї.

Закон України «Про доступ до публічної інформації», від 13 січня 2011 р., № 2939-VI, встановлює, що *конфіденційною*є інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб’єктів владних повноважень, яка може поширюватися у визначеному ними порядку за їх бажанням, відповідно до передбачених ними умов (ст. 7 Закону). *Таємною*є

інформація, доступ до якої обмежується відповідно до ч. 2 ст. 6 Закону України «Про доступ до публічної інформації», розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю (ст. 8 цього Закону). До *службової інформації* належить, зокрема інформація: 1) яка міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та / або прийняттю рішень; 2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці (ст. 9 цього Закону).

В. А. Ліпкан пояснює, що, зважаючи на визначення конфіденційної інформації, до неї можна віднести лише інформацію особистого характеру (персональні дані) і комерційну таємницю через те, що законодавець закріпив, що інформація, яка містить державну, професійну, банківську таємницю, слідства та іншу передбачену законом таємницю, визнається таємною [30, с. 93]. Не зрозуміло, чому ці види таємниць законодавець зарахував до таємної інформації, оскільки дослідження вітчизняного законодавства показало, що службову, військову, медичну й таємницю нарадчої кімнати слід віднести до таємної інформації. Дискусійним є співвідношення службової та професійної таємниць. Таємниці виникають внаслідок здійснення професійної діяльності, реалізація якої вимагає збереження інформації щодо неї як професійної таємниці.

Термін «таємниця» вживається для позначення більше тридцяти видів інформації з обмеженим доступом. Існуюче розмаїття таємниць передбачає не просто їх видове перерахування, а віднесення їх до певних груп, підгруп. Г. Д. Мепаришвілі зауважує, що доцільно виокремлювати особисті таємниці,

які зберігаються їх носіями та не довіряються представникам будь-яких професій (таємниця житла та особистих документів, зміст листування, телеграфних повідомлень та телефонних розмов), а також професійно довіренітаємниці (адвокатська, лікарська таємниці, грошових внесків, нотаріальних дій, усиновлення та сповіді). І.Л. Петрухін пише, що особисті таємниці утворюють фундамент професійних таємниць. Особистими таємницями є таємниця творчості та спілкування, сімейна, таємниця інтимних взаємин, таємниця житла, щоденників, особистих паперів, поштово-телеграфної кореспонденції, телефонних розмов. Професійними названо таємниці судового захисту, усиновлення, сповіді, досудового слідства, нотаріальну, медичну, таємницю записів актів цивільного стану.

2.3 Загальна характеристика видів інформації з обмеженим доступом

Розглянемо більш детально основні види інформації з обмеженим доступом.

Державна таємниця - вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою.

Основною підставою класифікації секретної інформації є ступінь секретності. Ця категорія характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою. Законодавством передбачено три ступені секретності для інформації, що становить державну таємницю: "***особливої важливості***", "***цілком таємно***", "***таємно***".

Зі ступенем секретності безпосередньо пов'язаний і максимальний строк дії режиму секретності інформації. Він не може перевищувати для

інформації із ступенем секретності *"особливої важливості" - 30 років*, для інформації *"цілком таємно" - 10 років*, для інформації *"таємно" - 5 років*. У деяких випадках Президент України може встановлювати більш тривалі строки дії рішень про віднесення інформації до державної таємниці.

Охорона державної таємниці передбачає впровадження комплексу організаційно-правових заходів, до яких, зокрема, належать:

- єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації;

- обмеження оприлюднення, передачі іншій державі або поширення іншим шляхом секретної інформації:

- спеціальний порядок допуску та доступу громадян до державної таємниці;

- технічний і криптографічний захист секретної інформації.

Форми допуску до державної таємниці встановлюються залежно від ступеня секретності інформації. Законодавство передбачає три форми такого допуску: форма 1 для роботи із секретною інформацією, що має ступені секретності "особливої важливості", "цілком таємно" і "таємно", яка має термін дії 5 років: форма 2-для ступенів секретності "цілком таємно" і "таємно" з терміном дії 7 років: форма 3 - для ступеня секретності "таємно" з терміном дії 10 років.

Згідно зі ст. 22 Закону України "Про державну таємницю" надання допуску громадян до державної таємниці передбачає:

- визначення необхідності роботи громадянина із секретною інформацією;

- перевірю громадянина у зв'язку з допуском до державної таємниці;

- взяття громадянином на себе письмового зобов'язання щодо збереження державної таємниці, яка буде йому довірена;

- одержання у письмовій формі згоди громадянина на передбачені законом обмеження прав у зв'язку з його допуском до державної таємниці;

- ознайомлення громадянина з мірою відповідальності за порушення законодавства про державну таємницю.

Допуск до державної таємниці не надається у разі:

- відсутності у громадянина обґрунтованої необхідності в роботі із секретною інформацією;

- сприяння громадянином діяльності іноземної держави, іноземної організації чи їх представників, що завдає шкоди інтересам національної безпеки України;

- відмови громадянина взяти на себе письмове зобов'язання щодо збереження державної таємниці, яка буде йому довірена;

- наявності у громадянина судимості за тяжкі злочини, не погашеної чи не знятої у встановленому порядку;

- наявності у громадянина психічних захворювань, які можуть завдати шкоди охороні державної таємниці.

За наявності у громадянина відповідним чином оформленого допуску до державної таємниці та відповідної потреби або у зв'язку з виконанням службових обов'язків ухвалюється рішення про надання доступу до державної таємниці.

Рішення про доступ до державної таємниці передбачає надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею.

Службова інформація – це інформація, що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами публічної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень; інформація зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Нині законодавство більшості країн встановлює для службовців заборону на розголошування відомостей, що стали їм відомими у зв'язку із їхньою службовою діяльністю. Але варто відмітити, що в останні декілька десятиліть у більшості країн більшого значення набуває принцип інформаційної відкритості публічного управління і відповідно на службовців все частіше покладається супротивний обов'язок забезпечувати доступ до відкритих документів.

Про проблему поєднання цих принципів писав ще в 1988 році французький вчений Г. Бребан: "службовець не повинен розповідати за межами своєї установи про те, що йому стало відомо за характером служби. Втім, нині це досить серйозна проблема, тому що представники різних кіл громадськості наполягають на створенні так званої гласної адміністрації відповідно до шведської моделі, тобто адміністрації, що не має таємниць, яка є відкритою для громадськості, яка могла б мати доступ до документації, а також знайомитися з мотивами, аргументами і методами роботи управлінського апарату".

Варто відмітити, що на даний час в Україні правовідносини з приводу службової інформації регулюються значним числом нормативно-правових актів, їй присвячені досить багато наукових робіт, але проте загальна ситуація залишається складною. Не можна сказати, що рамки і правова природа даного інституту не визначені зовсім, проте вони визначені у різних нормативних і доктринальних джерелах різним, не завжди сумісним чином, відсутнім загальноприйнятим понятійним апаратом. Зокрема, предмет даного дослідження позначається в різних актах наступними термінами: службова таємниця, конфіденційна службова інформація, службова інформація, інформація для службового користування та ін.

Різні доктрини відбиваються в нормативних правових актах, це призводить до того, що і законодавство, і доктрина є декількома напрямами, які переплітаються та погоджуватись з якими дуже складно. Низький рівень юридичної техніки вносить додаткову плутанину.

Відсутність належного регулювання службової інформації породжує цілий ряд негативних явищ, які можна розділити на два напрями: по-перше, службова інформація використовується як інструмент виведення діяльності органів влади і державних службовців з-під громадського контролю, приховання зловживань. По-друге, службова інформація досить часто є об'єктом протиправних посягань, просочування інформації носить регулярний характер, існує чорний ринок конфіденційної інформації. Важливо відмітити, що обидві названі тенденції мають виразно корупціогенний характер.

В описаних обставинах серед завдань на рахунок протидії корупції, окрім інших напрямів, велике значення має регулювання відносин у сфері службової інформації, проте важливе дотримання балансу між необхідністю збереження в таємниці відомостей, розголошування яких може завдати шкоди суспільно важливим інтересам і розкриттям суспільно важливої інформації.

Так, для позначення службової інформації окрім терміну «службова інформація» використовується цілий ряд інших, в першу чергу, - «службова таємниця».

Поняття «службова інформація» пов'язане, у свою чергу, з поняттями «таємниця». Таємниця може бути визначена як «щось приховуване від інших, відоме не усім» або як «прихована причина чого-небудь». У зарубіжній юридичній літературі таємницю розглядають як «виняткові знання, не відомі зацікавленій в них особі і не досяжні без певних економічних витрат». Це визначення дозволяє виділити два ключові аспекти поняття «таємниця». По-перше, таємниця проявляється в деякому знанні певних відомостей, під якими можуть розумітися як фактичні обставини, так і суб'єктивні навички (досвід). По-друге, таємниця завжди існує відносно певної особи (групи осіб) до тих пір, поки ця особа (група осіб) не придбає яким-небудь чином відомості, що становлять її зміст.

Як вже раніше було сказано, на сьогодні ні в одному законі не дається поняття службової таємниці і в той же час застосовується поняття «службова інформація». Прирівнювання службової інформації до державної таємниці допускають відомі вчені в сфері інформаційного права. Професор І.Л.Бачило в одній зі своїх наукових робіт так торкається службової інформації «... у системі державного управління являється безліч видів інформації: державна таємниця, інша службова інформація, комерційна таємниця, персональні дані фізичних осіб, інформація про юридичних осіб і їх діяльність. Великий обсяг інформації за змістом відноситься не лише до обліково-реєстраційної інформації, але і до інформації науково-технічного змісту, що включає і таку категорію, яка має якості інтелектуальної власності. Усе це створює безліч питань правового та організаційного характеру, пов'язаних із забезпеченням правового режиму цих ресурсів, з одного боку, і їх раціонального використання, як в діяльності самих органів виконавчої влади, так і в діяльності організацій, якимдержава передає функції з розпорядження відкритою інформацією, а при дотриманні правил ліцензування - інформацією обмеженого доступу з іншою. Проблема розмежування відкритої інформації та інформації з обмеженим доступом створює особливий режим роботи службовців, який дотримується в інтересах держави, суспільства і фізичних осіб».

Резюмуючи усе вищесказане про співвідношення і використання термінів «службова інформація» і «службова таємниця», слід констатувати, що самі категорії службової таємниці і службової інформації не співпадають. Службова таємниця може включатися до складу службової інформації, оскільки до останньої відноситься будь-що, яке не є загальнодоступною інформацією. Отже, відомості, що становлять службову інформацію, можуть і не бути конфіденційними, але доступ до них є обмеженим у зв'язку з тим, що вони відомі тільки певному колу осіб і закони, що стосуються інформаційної сфери, не вимагають розкриття цих відомостей (зокрема, Закон "Про ринок цінних паперів"). Необхідно враховувати, що інформація,

яка містить службову таємницю, може мати чималу вартість, але не носити комерційного характеру. Вона може бути відома багатьом фахівцям, працюючим в цій сфері. Але вони, проте, не знають як і в яких об'ємах вона використовується конкретним органом публічної влади.

Таким чином, на нашу думку, службову таємницю необхідно визначити як інформацію з обмеженим доступом, що утворюються в процесі управлінської діяльності органу публічної влади, поширення яких перешкоджає або іншим чином негативно позначається на реалізації наданих цим органам владних повноважень.

До загальних умов режиму інформації, що становлять службову таємницю, мають бути включені:

- дійсна або потенційна конфіденційність інформації;

- відсутність вільного доступу до службової таємниці на законній основі;

- власник інформації зобов'язаний вживати заходи щодо охорони її конфіденційності.

Підсумовуючи, відмітимо, що запропонована нами дефініція службової інформації в широкому розумінні вбільшій мірі відображає ті грані цього поняття, які застосовні в інтересах права.

У більш вузькому значенні службова інформація – це відомості та/або дані, що становлять службову таємницю, яка утворюється в процесі державно-управлінської діяльності, поширення якої порушує права і свободи громадян, перешкоджає реалізації органом або організацією наданих йому повноважень або іншим чином негативно впливає на їх реалізації, а також конфіденційна інформація, отримана органом публічної влади у відповідності з їх компетенцією та у встановленому законодавством порядку.

Конфіденційна інформація – це інформація про фізичну особу (персональні дані) або юридичну особу, доступ та поширення якої можливі лише за згодою її власників (тобто тих, кого ця інформація безпосередньо стосується) та на тих умовах, які вони вкажуть.

До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження. Не допускаються 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 захисту прав людини.

Відповідно до ст. 10 ЗУ "Про доступ до публічної інформації" кожному забезпечується вільний доступ до інформації, яка стосується його особисто. Крім того, кожна особа має право:

- знати у період збирання інформації, але до початку її використання, які відомості про неї та з якою метою збираються,

як, ким і з якою метою вони використовуються, передаються чи поширюються;

- вимагати виправлення неточної, неповної, застарілої інформації про себе, знищення інформації про себе, збирання,

використання чи зберігання якої здійснюється з порушенням вимог закону.

Розпорядник інформації про особу, тобто той, хто цю інформацію збирає, зберігає і використовує, зобов'язаний:

- надавати її безперешкодно і безкоштовно на вимогу осіб, яких вона стосується;
- використовувати її лише з метою та у спосіб, визначений законом;
- вживати заходів щодо унеможливлення несанкціонованого доступу до неї інших осіб;
- виправляти неточну та застарілу інформацію про особу самостійно або на вимогу осіб, яких вона стосується.

Зберігання інформації про особу не повинно тривати довше, ніж це необхідно для досягнення мети, задля якої ця інформація збиралася.

Інформація, яка міститься в договорах, контрактах, листах, звітах, аналітичних матеріалах, виписках з бухгалтерських рахунків, схемах,

графіках, специфікаціях і інших документах, що фігурують в діяльності юридичної особи є конфіденційною інформацією, що належить юридичній особі, адже розголошення даних, що містяться в таких документах, може бути використано конкурентами і, відповідно, завдати економічної та іншої шкоди юридичній особі.

Не можуть бути віднесені до конфіденційної інформації, але поширюються лише за згодою осіб, які обмежили доступ до інформації, а за відсутності такої згоди – лише в інтересах національної безпеки, економічного добробуту та прав людини:

- рішення суб'єктів владних повноважень, які є обов'язковими до виконання;

- інформація про використання бюджетних коштів юридичними особами, що фінансуються з державного, місцевих бюджетів, бюджету Автономної Республіки Крим;

- інформація пов'язана з виконанням обов'язків особами, які вони виконують як делеговані повноваження суб'єктів владних повноважень згідно із законом чи договором, включаючи надання освітніх, оздоровчих, соціальних або інших державних послуг;

- інформація суб'єктів господарювання, які займають домінуюче становище на ринку або наділені спеціальними чи виключними правами, або є природними монополіями щодо умов постачання товарів, послуг та цін на них.

Не можуть бути віднесені до конфіденційної інформація:

- суб'єктів господарювання про стан довкілля;

- суб'єктів господарювання про якість харчових продуктів і предметів побуту;

- суб'єктів господарювання про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, що сталися або можуть статися і загрожують здоров'ю та безпеці громадян;

- інша, що становить суспільний інтерес (суспільно необхідна інформація).

Чинне законодавство не містить переліку видів інформації про особу, які можуть визнаватись конфіденційними, а також не визначає порядку визнання тих чи інших видів відомостей про особу конфіденційною інформацією. Згідно з ч. 5 ст. ЗО Закону України «Про інформацію», громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їхнього професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту. Для окремих категорій громадян законодавством встановлений обов'язок зберігати в таємниці певні відомості про громадян, які їм стали відомі у зв'язку з виконанням професійних чи службових обов'язків, тобто які є їхньою професійною (службовою) таємницею. Наприклад, згідно зі ст. 8 Закону України «Про нотаріат» від 2 вересня 1993 р., нотаріуси та службові особи, які вчиняють нотаріальні дії, зобов'язані додержувати таємниці цих дій. Обов'язок додержання таємниці вчинюваних нотаріальних дій поширюється також на осіб, яким про вчинені нотаріальні дії стало відомо у зв'язку з виконанням ними службових обов'язків (працівники суду, прокуратури, органів дізнання і слідства, податкових органів тощо). Цією ж статтею передбачені й випадки, коли нотаріус може повідомити компетентним органам відомості, що є нотаріальною таємницею.

Згідно зі ст. 46 Закону України «Про інформацію», не підлягають розголошенню відомості, що стосуються лікарської таємниці, грошових вкладів, прибутків від підприємницької діяльності, усиновлення (удочеріння), листування, телефонних розмов і телеграфних повідомлень, а також які становлять іншу, передбачену законом таємницю, крім випадків,

передбачених законом. Відомості, що становлять професійну таємницю певних категорій осіб, завжди повинні визнаватись такими, що є конфіденційною інформацією про особу.

Таким чином, будь-яка інформація про особу може бути віднесена на розсуд особи до конфіденційної, якщо це не заборонено Законом. Але не вся інформація про особу є конфіденційно.

Конфіденційна інформація є підвидом інформації про особу і не вичерпується персональними даними.

Поняття конфіденційної інформації визначено Законами України «Про інформацію» та "Про доступ до публічної інформації", а також багато інших законів прямо визначають інформацію про особу, що є конфіденційною.

Це, зокрема:

відомості про національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, адреса, дата та місце народження (ч.2.ст.11. ЗУ «Про інформацію»);

реєстраційний (ідентифікаційний номер платника податків) номер облікової картки фізичної особи (п.70.15, ст.70 Податкового кодексу);

відомості про місце проживання (ч.8.ст.6 ЗУ «Про свободу пересування та вільний вибір проживання в Україні»);

відомості про страховий стаж, результати медичних обстежень, отримані доходи застрахованої фізичної особи (ст.33 ЗУ «Про загальнообов'язкове державне соціальне страхування у зв'язку з тимчасовою втратою працездатності та витратами, зумовленими похованням»);

відомості про особисте життя громадян, одержані із звернень громадян (ст.10.ЗУ «Про звернення громадян»);

первинні дані, отримані в процесі проведення Перепису населення (ст.16 ЗУ «Про Всеукраїнський перепис населення»);

відомості, що подаються заявником на визнання біженцем або особою, яка потребує додаткового захисту (ч. 10.ст.7 ЗУ «Про біженців та осіб, які потребують додаткового або тимчасового захисту»);

інформація про пенсійні внески, пенсійні виплати та інвестиційний прибуток (збиток), що обліковується на індивідуальному пенсійному рахунку учасника пенсійного фонду, пенсійні депозитні рахунки фізичних осіб, договори страхування довічної пенсії (ч3.ст.53 ЗУ «Про недержавне пенсійне страхування»);

інформація про стан пенсійних активів, облікованих на накопичувальному пенсійному рахунку застрахованої особи (ч.1.ст.98 ЗУ «Про загальнообов'язкове державне пенсійне страхування»);

відомості щодо предмета договору на виконання науково-дослідних або дослідно-конструкторських та технологічних робіт, хід їх виконання та результати (ст.895 Цивільного кодексу)

інформація яка може сприяти ідентифікації особи неповнолітнього правопорушника або яка стосується факту самогубства неповнолітнього (ч.3.ст.62 ЗУ «Про телебачення та радіомовлення»);

інформація про померлого (ст.7 ЗУ Про поховання та охоронну справу»);

відомості про оплату праці працівника (ст.31 ЗУ «Про оплату праці» *Примітка!* Відомості про оплату праці надаються лише у випадках передбачених законодавством, або за згодою чи на вимогу працівника);

заявки та матеріали на видачу патентів (ст. 19 ЗУ «Про охорону прав на винаходи і корисні моделі»);

дані про особу взяту під захист у кримінальному судочинстві (ст.15 ЗУ «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві»);

матеріали заявки фізичної чи юридичної особи на реєстрацію сорту рослин, результати експертизи сорту рослин (ст.23 ЗУ «Про охорону прав на сорти рослин»);

дані про працівника суду або правоохоронного органу, взятого під захист (ст. 10 ЗУ «Про державний захист працівників суду і правоохоронних органів»);

інформація про осіб, які звернулися до кризового центру про допомогу (ч. 3.ст.8 ЗУ «Про попередження насильства в сім'ї);

інформація,що стосується митної вартості товарів, що переміщаються через митний кордон України (ч.1.ст. 263 Митного кодексу);

інформація,що міститься в заяві про державну реєстрацію лікарського засобу та додатка до них (ч.8.ст.9 ЗУ «Про лікарські засоби»);

відомості, що містяться в текстах судових рішень та дають можливість ідентифікувати фізичну особу, зокрема: імена (ім'я, по батькові, прізвище) фізичних осіб; місце проживання або перебування фізичних осіб із зазначенням адреси, номерів телефонів чи інших засобів зв'язку, адреси електронної пошти, ідентифікаційних номерів (коди); реєстраційні номери транспортних засобів (ст.7 ЗУ «Про доступ до судових рішень»).

Зважаючи на викладене слід враховувати, що органи влади не можуть надавати громадянам України інформацію про осіб та членів їх родини без їх згоди.Так, Конституційний суд офіційно розтлумачив положення частини 1 та 2 ст. 32, ч.2, 3 ст. 34 Конституції України згідно подання Жашківської райради (Черкаська обл.), якій було потрібно роз'яснити, що є інформацією про особисте та сімейне життя та чи є така інформація конфіденційною; чи є збір, зберігання, використання та поширення інформації про осіб втручанням в їх особисте та сімейне життя.

Конституційний суд роз'яснив цю норму, повідомивши про те, що «інформацією про особисте та сімейне життя особи є будь-які дані про відносини немайнового та майнового характеру, обставини, події, відносини та ін, пов'язані з особою та членами його родини, за винятком передбаченої законами інформації, яка стосується здійснення особою, яка займає пост, пов'язаний з використанням функцій держави або органами місцевого самоврядування, посадових і службових повноважень. Така інформація про особу є конфіденційною».

«*Збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди державою, органами місцевого*

самоврядування, юридичними або фізичними особами є втручанням в її особисте/сімейне життя. Таке втручання допускається виключно у випадках, визначених законом і лише в інтересах нацбезпеки, економічного добробуту та прав людини», — наголошується в рішенні КСУ.

Ураховуючи проаналізовані вище нормативні та доктринальні дефініції інформації з обмеженим доступом, а також визначені її характерні риси, пропонуємо авторську позицію розуміння інформації з обмеженим доступом: будь-які **відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді, доступ до яких обмежено її власником чи добросовісним користувачем (суб'єктом владних повноважень, фізичною або юридичною особою) на законних підставах.**

Питання для самоконтролю до розділу 2

1. Що таке інформація?
2. Визначіть основні ознаки інформації
3. Охарактеризуйте соціальне значення інформації в сучасних умовах
4. Як поділяється інформація за режимом доступу?
5. У чому відмінність службової інформації від державної таємниці?
6. Розтлумачте зміст конфіденційної інформації
7. Дайте визначення «інформація з обмеженим доступом»

Література

1. Словник іншомовних слів. За редакцією члена-кореспондента АН України О.С. Мельничука. – К. : – 1974. – 775 с.
2. Шеннон К. Работы по теорииинформации и кибернетики / К. Шеннон. – М. : Иностраннаялитература, 1963. – 830 с.
3. Урсул А. Д. Природа информации. Философскийочерк / А. Д. Урсул. – М. : Политиздат,1968. – 287 с.
4. Винер Н. Кибернетика и общество / Н. Винер. – М. : Издательствоиностраннойлитературы, 1958. – 346 с.
5. Марчук Є.К. Стратегічна організація суспільства - рух на випередження // Стратегічна панорама. - 1999. - № 4. - С.13-17
6. Якушин Б.В. Слово. Понятие. Информация (Гноссеологическиеразработкиинформационных систем) / Б.В.Якушин. – М. : Молодаягвардия, 1975. – 296 с.
7. Вачевський М.В. Основи наукової інформації : навч. посіб. для студ. вузів / М.В.Вачевський. – Дрогобич : Відродження, 1995. – 183 с.

8. Герчикова И.Н. Менеджмент : учебник, 3-е изд., перераб. и доп. / И.Н. Герчикова. – М. : Банки и биржи, ЮНИТИ, 1997. – 501 с.

9. Винер Н. Кибернетика, илиуправление и связь в животном и машине / Н. Винер. – М. : Иностраннаялитература, 1958. – 418 с.

10. Политология : энциклопедическийсловарь / под ред. Ю. И. Аверьянова. – М. : Московскийкоммерческийуниверситет, 1993. – 431 с.

11. Інноваційна стратегія українських реформ / А.С. Гальчинський, В.М. Геєць, А.К. Кінах, В.П. Семиноженко. - К.: Знання України, 2002. - 336 с.

12. Минкина В.А. От библиографиитехники к информационномууправлению: на пути к интеллектуальномупреобразованиюинформации // Научно-техническаяинформация. - 2003. - № 6. - С. 2-5

13. Про інформацію : Закон України від 02.10.1992 № 2657-XII. – Електронний ресурс. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12

14. БелкинРафаилСамуилович.Избранныетруды. — М. : Норма, 2008. — 767с.

15. Венгеров А. Б. Категория «информация» в понятийномаппаратеюридлическкой науки / А. Б. Венгеров // Советскоегосударство и право. — 1977. — № 10. — с. 70-71

16. Мацюк В. Я. Використання інформаційного ресурсу підрозділами податкової міліції для прийняття управлінського рішення : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 / В.Я. Мацюк. — Ірпінь, 2004. — 16 с.

17. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : дис. … д-ра юрид. наук : 12.00.07 / Борис Анатолійович Кормич. — О., 2004. — 427 с.

18. Дементій Н. О. Аналіз інформаційних теорій і понять інформації / Н. О. Дементій // http://www.naiau.kiev.ua/tslc/pages/biblio/visnik/2002_2/dementi.htm

19. Копылов В. А. Информационное право : [учеб]. – 2-е изд., перераб. и доп. – М., 2003. – 512 с.

20. Бачило И. Л. Информационное право \ Бачило И. Л., Лопатин В. Н., Федотов М. А.; Под ред. Акад. РАН Б.Н. Топорнина. — СПб. : «Юридический центр Пресс», 2001. — 422 с.

21. Кохановська О. В. Правове регулювання у сфері інформаційних відносин : [монографія] / О. В. Кохановська. — К. : Націон. акад. внутр. справ України, 2001. — 212 с.

22. Антопольский А. А. Правовое регулирование информационных объектов / А.А. Антопольский // Проблемы информатизации. – 1999. – Вып. 3. – С. 51-54

23. Письменський А. А. Информационное право Украины / Письменський А. А. – Харьков : БизнесИнформ, 1996. – 248 с.

24. Марценюк О. Г. Теоретико-методологічні засади інформаційного права України: реалізація права на інформацію : дис. … канд. юрид. наук : 12.00.07 / Олександр Геннадійович Марценюк. — К., 2009. — 266 с.

25. Угода між Кабінетом Міністрів України та Урядом Словацької Республіки про взаємну охорону інформації з обмеженим доступом // Офіційний вісник України. – 2008. – № 99. – Ст. 3282.

26. Угода між Україною та Угорською Республікою про взаємну охорону інформації з обмеженим доступом // Офіційний вісник України. – 2008. – № 24. – Ст. 720.

27. Угода між Україною та Республікою Словенія про обмін та взаємну охорону інформації з обмеженим доступом // Офіційний вісник України. – 2009. – № 29. – Ст. 961.

28. Угода між Кабінетом Міністрів України та Урядом Алжирської Народної Демократичної Республіки про охорону інформації з обмеженим доступом // Офіційний вісник України. – 2009 – № 49. – Ст. 554.

29. Угода між Кабінетом Міністрів України та Урядом Республіки Македонія про взаємну охорону інформації з обмеженим доступом // Офіційний вісник України. – 2011. – № 3. – Ст. 162.

30. Ліпкан, В. А. Адміністративно-правовий режим інформації з обмеженим доступом в Україні: монографія / В. А. Ліпкан, В. Ю. Баскаков / За заг. ред. В. А. Ліпкана. – К. : ФОП О. С. Ліпкан, 2013. – 344 с.

31. Мепаришвили, Г. Д. Охрана тайн личной жизни граждан в советском уголовном процессе : автореф. дис. … канд. юрид. наук : 12.00.09 / Г. Д. Мепаришвили. – М. : Б. и., 1988. – 21 с.

32. Петрухин, И. Л. Личнаяжизнь: пределывмешательства / И. Л. Петрухин. – М. : Юрид. лит., 1989. – 192 с.

РОЗДІЛ 3

ПОНЯТТЯ ТА ПРАВОВИЙ ЗМІСТ ПЕРСОНАЛЬНИХ ДАНИХ ЯК ОБ'ЄКТА ПРАВОВОЇ ОХОРОНИ В УКРАЇНІ

3.1 Поняття персональних даних як об'єкта правової охорони та їх місце у правовідносинах

Ведучи мову про захист персональних даних ми повинні зосередитись на суті тих цінностей, що підлягають захисту у такий спосіб.

Згідно до статті 32 Конституції України 1996 р.: "Ніхто не може зазнавати втручання в його особисте життя, крім випадків, передбачених Конституцією України. 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".

Це право задекларовано і на міжнародному рівні, зокрема ратифікована Україною у 1997 році Конвенція про захист прав і основних свобод людини 1950 року Статтею 8 цієї конвенції закріпили, що кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції. Органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб.

Таким чином, право людини на недоторканість приватного життя передбачає правовий захист відомостей про неї, при якому об'єктом правовідносин є дані про особу.

Особисте життя – це майнові, моральні, культурні й інші зв'язки, які створюються на основі сімейних, дружніх, інших відносин між людьми в сфері особистого життя, продовження роду, влаштування житла, ведення

домашнього господарства, використання вільного часу, участь у культурному житті та ін.

Приватність необхідно розуміти як безпеку, недоторканність особистого життя, інтерес людини щодо збереження в таємниці відомостей про її особу та обставини її особистого життя і одночасно можливість визначати, яку інформацію про особисте життя розголосити.

Загальновизнаними залишаються наступні аспекти приватності:

– територіальну приватність – яку гарантовано конституційним правом на недоторканість житла, закріпленим у ст. 30 Конституції;

– комунікаційна приватність – що гарантується конституційним правом на таємницю телефонних розмов, телеграфної та іншої кореспонденції, яке закріплено у ст. 31 Конституції;

– тілесну (фізичну) приватність – стосується захисту людського тіла від стороннього втручання, що гарантовано конституційною забороною на проведення над людиною будь-яких дослідів, що закріплено у ст. 28 Конституції;

– інформаційну приватність – це можливості особи щодо контролю за збором та обігом відомостей про себе та своє життя, що гарантовано конституційною забороною на збирання, зберігання, використання та поширення конфіденційної інформації про особу (тобто персональних даних) без її згоди, яка закріплена у ст. 32 Конституції.

Право людини на недоторканість особистого життя варто розуміти як забезпечену законом можливість фізичної особи відокремити деяку свою поведінку від публічних процесів, задовольнити свої особисті інтереси, бути захищеною від стороннього втручання, що виникає на підставі загальної здатності набувати особистих немайнових прав.

Вимога конфіденційності інформації про особисте життя, відповідно до ст. 32 Конституції України та Закону України "Про інформацію", полягає у наділенні особи можливістю визначення режиму доступу до інформації про її особу і особисте життя з одночасною забороною збирати, зберігати,

використовувати і поширювати таку інформацію без її дозволу, окрім випадків, передбачених законом.

Законом України «Про захист персональних даних» закріплено визначення персональних даних як «відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована та одночасно надано всім персональним даним, крім знеособлених статусу інформації з обмеженим доступом». Аналогічне визначення персональних даних як «будь-якої інформації, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною» закріплено у ст. 2 ратифікованої Україною 108-ї Конвенції Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних».

Персональні дані, крім знеособлених персональних даних, за режимом доступу законом визнано інформацією з обмеженим доступом. Безсумнівно таке широке визначення персональних даних як об’єкта охорони повинно сприяти досягненню цілей цих нормативних актів, які покликані гарантувати захист персональних даних під час їх обробки, що здійснюється не власниками цієї інформації, а іншими особами, які несуть зобов’язання щодо захисту наданої їм інформації.

Використовуючи положення зазначеної конвенції серед персональних даних виділяються ті, які потребують більшого рівня захисту, а саме: дані про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, а також даних, що стосуються здоров'я чи статевого життя.

За таких умов загальне розуміння інформації про особу як об’єкта правового захисту можливо зрозуміти лише розглянувши її в контексті змісту тих правовідносин, предметом яких є ця інформація.

Якщо ми торкнемося інформації про особу як об’єкта захисту, то в першу чергу звичайно звернемо увагу на Кримінальний кодекс, бо статтею 182 КК передбачено кримінальну відповідальність за незаконне збирання, зберігання, використання або поширення конфіденційної інформації про

особу без її згоди або поширення цієї інформації у публічному виступі, творі, що публічно демонструється, чи в засобах масової інформації. Звідси робимо висновок що персональні дані можуть захищатися в режимі конфіденційної інформації.

Інформація з обмеженим доступом поділяється на конфіденційну, таємну і службову. Питання віднесення персональних даних до певного виду інформації з обмеженим доступом є суттєвим.

І це дійсно так, бо інформація про особу має унікальну властивість перебувати у у статусах різних видів таємної інформації, зокрема таких її видах як: таємниця голосування, листування, адвокатська, нотаріальна, банківська, лікарська таємниця та таємниця усиновлення. По факту, якщо персональні дані потрапляють у стандартних правовідносинах до тих осіб, яким вони необхідні для виконання своїх функцій, але безпосередньої шкоди цим особам від розголошення чужих персональних даних не буде, то це зумовлює зміну статусу такої інформації на таємну. Цим статусом на незацікавлених у захисті осіб покладається обов'язок відповідально ставитись до чужої інформації і чужих інтересів під страхом юридичної відповідальності та із дотриманням окремо регламентованих приписів щодо захисту таємної інформації.

Тут необхідно зауважити, що статус персональних даних і спосіб їх захисту залежить від виду правовідносин у які вона потрапляє. Якщо інформація здобута оперативним шляхом - це державна таємниця, якщо цю саму інформацію про особу отримав адвокат - це адвокатська таємниця, якщо її отримав лікар - то для нього це лікарська таємниця. А з самої своєї появи ці ж персональні дані одночасно могли отримати статус таємниці усиновлення.

Разом з тим, джерелом цих даних є людина і основною метою їх захисту у будь-якому статусі є захист прав та законних інтересів саме особи. Цей захист відбувається в межах певних правовідносини як врегульованих нормами права суспільних відносин, суб'єкти яких є носіями суб'єктивних прав та обов'язків. Ці права та обов'язки становлять правовий статус

суб'єкта правовідносин, який формує забезпечені законом межі його можливої та обов'язкової поведінки.

У правовідносинах, пов'язаних з обігом персональних даних приймають участь такі види учасників:

1. Фізичні особи, які є обов'язковим учасником усіх правовідносин, пов'язаних з обігом їх персональних даних.

2. Уповноважений Верховної Ради України з прав людини як уповноважений державний орган з питань захисту персональних даних.

3. Володільці та розпорядники персональних даних, якими можуть бути:

- органи державної влади та утворені ними підприємства які збирають, зберігають і використовують персональні дані та інформаційні бази, що містять персональні дані на виконання функцій, які покладено законодавством на ці органи;
- громадські організації, які використовують персональні дані з дозволу їх власників для досягнення своїх цілей;
- міжнародні організації, які діють на підставі їх статутів, положення яких узгоджуються між країнами-учасницями цих організацій і які використовують персональні дані з дозволу їх власників для досягнення своїх цілей;
- суб'єкти господарювання, які збирають персональні дані відповідно до чинного законодавства лише для виконання власних статутних завдань.

4. Треті особи, які використовують персональні дані, отримуючи їх із баз та безпосередньо від фізичних осіб.

Правовий статус фізичних осіб в правовідносинах, пов'язаних з обігом персональних даних є виключним. Це ґрунтується на тому, що саме фізична особа є джерелом і власником своїх персональних даних. Саме фізична особа вправі вирішувати чи розголошувати

Загальними цілями правовідносин, в яких приймають участь персональні дані є:

- підтвердження фактів наявності, зміни обсягу чи відчуження прав фізичної особи;
- реалізація та офіційне відновлення прав фізичної особи;
- здійснення функцій державного управління.

Правовідносини, в яких можуть перебувати персональні дані, мають досить широкий характер і врегульовані фактично усіма галузями права.

1. Конституційно-правові відносини передбачають участь персональних даних при реалізації конституційних прав таких як активне і пасивне виборче право, право на звернення до органів державної влади і місцевого самоврядування, права на місцеве самоврядування та інших політичних прав. Для реалізації цих прав створюються навіть відповідні бази даних фізичних осіб такі як списки виборців та єдиний державний реєстр виборців.

2. Фінансово-правові відносини передбачають обов'язкову реєстрацію усіх осіб, що зобов'язані сплачувати податки і збори до державного та місцевих бюджетів. Правовідносини саме у цій галузі права зумовили створення реєстрів фізичних осіб із наданням їм ідентифікаційного коду.

3. Цивільно-правові відносини передбачають обов'язкову участь персональних даних при здійсненні правочинів та відновленні порушених майнових прав для ідентифікації суб'єктів, які прийматимуть в цих процесах участь, набуваючи чи відчужуючи майнові та особисті немайнові права відносно тих чи інших предметів цивільно-правових відносин.

4. Господарсько-правові відносини передбачають участь персональних даних при створенні та реєстрації суб'єктів підприємництва, набутті та відчуженні ними права на управління діяльністю цих суб'єктів.

5. Сімейні відносини передбачають саму появу персональних даних тобто реєстрацію новонароджених, крім того персональні дані необхідні для

персоніфікації та осіб, що вступають у шлюб, отримання батьківських прав, забезпечення прав неповнолітніх.

6. Трудові відносини передбачають необхідність залучення персональних даних для персоніфікації працівників, підтвердження ними кваліфікації та здатності за станом здоров'я виконувати свої функції.

7. Відносини соціального забезпечення передбачають залучення персональних даних для підтвердження права на соціальний захист і визначення розмірів соціальних виплат та інших видів соціального забезпечення.

8. Адміністративно-правові відносини складаються в ході отримання органами державної влади персональних даних від їх власників. Ця інформація також необхідна для персоніфікації особи, що вчинила правопорушення чи намагається в адміністративному порядку відновити свої порушені права. Нормами адміністративного права врегульовано порядок ведення численних обліків із залученням даних про фізичних осіб, що використовуються для досягнення цілей держави (наприклад реєстри власників нерухомості і автотранспорту, реєстрація осіб за місцем проживання). Завдяки адміністративному праву працює і дозвільна система, яка передбачає реєстрацію осіб, що мають право володіння зброєю, керування автотранспортом тощо.

9. Кримінально правові відносини також передбачають необхідність залучення персональних даних, до цілей судочинства у кримінальних справах прямо входить збір персональних даних, зокрема виявлення осіб, які винуваті у скоєнні злочину та отримання даних, що характеризують їх особу. Ці відносини також стають джерелом наповнення обліків фізичних осіб, це облік судимих, криміналістичні обліки тощо.

3.2 Загальні вимоги до обробки персональних даних у базах

Внаслідок ратифікації Україною у 2010 році 108-ї Конвенції Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» наша держава зобов’язалась і впровадила європейські стандарти і правила захисту персональних даних та європейську централізовану модель захисту: із єдиними загальнодержавними правилами та контролюючим органом, яким у нашій державі з 2014 року визначено Уповноваженого Верховної Ради України з прав людини.

Наслідком ратифікації цієї Конвенції стало прийняття Закону України «Про захист персональних даних», згідно із яким обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством.

Підставами для обробки персональних даних є:

1) згода суб’єкта персональних даних на обробку його персональних даних;

2) дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень;

3) укладення та виконання правочину, стороною якого є суб’єкт персональних даних або який укладено на користь суб’єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб’єкта персональних даних;

4) захист життєво важливих інтересів суб’єкта персональних даних;

5) необхідність захисту законних інтересів володільців персональних даних, третіх осіб, крім випадків, коли суб’єкт персональних даних вимагає припинити обробку його персональних даних та потреби захисту персональних даних переважають такий інтерес.

Склад та зміст персональних даних мають бути відповідними, адекватними та не надмірними стосовно визначеної мети їх обробки. Обробка персональних даних здійснюється із застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки.

Персональні дані мають бути точними, достовірними та оновлюватися в міру потреби, визначеної метою їх обробки.

У разі зміни визначеної мети обробки персональних даних суб'єктом персональних даних має бути надана згода на обробку його даних відповідно до зміненої мети, якщо нова мета обробки є несумісною з попередньою.

Не допускається обробка даних про фізичну особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Якщо обробка персональних даних є необхідною для захисту життєво важливих інтересів суб'єкта персональних даних, обробляти персональні дані без його згоди можна до часу, коли отримання згоди стане можливим.

Персональні дані обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, у строк, не більший ніж це необхідно відповідно до їх законного призначення.

Обробка персональних даних в історичних, статистичних чи наукових цілях може здійснюватися лише за умови забезпечення їх належного захисту.

Забороняється обробка «чутливих» персональних даних, тобто інформації про відомості про расове, етнічне та національне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та або організаціях, професійних спілках, релігійних організаціях чи в громадських організаціях світоглядної спрямованості, стан здоров’я, статеве життя, біометричні дані, генетичні дані, місцеперебування та або шляхи пересування особи, факт притягнення до адміністративної чи кримінальної відповідальності, застосування щодо особи заходів в рамках досудового розслідування та заходів, передбачених Законом України «Про

оперативно-розшукову діяльність», вчинення щодо особи тих чи інших видів насильства.

Обробка «чутливих» персональних даних можлива якщо вона:

- здійснюється за умови надання суб'єктом персональних даних однозначної згоди на обробку таких даних;
- необхідна для здійснення прав та виконання обов'язків володільця у сфері трудових правовідносин відповідно до закону із забезпеченням відповідного захисту;
- необхідна для захисту життєво важливих інтересів суб'єкта персональних даних або іншої особи у разі недієздатності або обмеження цивільної дієздатності суб'єкта персональних даних;
- здійснюється із забезпеченням відповідного захисту релігійною організацією, громадською організацією світоглядної спрямованості, політичною партією або професійною спілкою, що створені відповідно до закону, за умови, що обробка стосується виключно персональних даних членів цих об'єднань або осіб, які підтримують постійні контакти з ними у зв'язку з характером їх діяльності, та персональні дані не передаються третій особі без згоди суб'єктів персональних даних;
- необхідна для обґрунтування, задоволення або захисту правової вимоги;
- необхідна в цілях охорони здоров’я, встановлення медичного діагнозу, для забезпечення піклування чи лікування або надання медичних послуг за умови, що такі дані обробляються медичним працівником або іншою особою закладу охорони здоров’я, на якого покладено обов’язки щодо забезпечення захисту персональних даних та на якого поширюється законодавство про лікарську таємницю;
- стосується обвинувачень у вчиненні злочинів, вироків суду, здійснення державним органом повноважень, визначених законом,

щодо виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом;

- стосується даних, які були оприлюднені суб'єктом персональних даних.

Обробка персональних даних в базах здійснюється їх володільцями або розпорядниками. Згідно із Законом України «Про захист персональних даних» володілець персональних даних - фізична або юридична особа, якій законом або за згодою суб'єкта персональних даних надано право на обробку цих даних, яка затверджує мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом.

Розпорядник персональних даних - фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця.

Володільцем чи розпорядником персональних даних можуть бути підприємства, установи і організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичні особи - підприємці, які обробляють персональні дані відповідно до закону.

Розпорядником персональних даних, володільцем яких є орган державної влади чи орган місцевого самоврядування, крім цих органів, може бути лише підприємство державної або комунальної форми власності, що належить до сфери управління цього органу.

Володілець персональних даних може доручити обробку персональних даних розпоряднику персональних даних відповідно до договору, укладеного в письмовій формі.

Розпорядник персональних даних може обробляти персональні дані лише з метою і в обсязі, визначених у договорі.

Володілець бази персональних даних визначає:

- мету обробки, склад персональних даних у базі персональних даних та її місцезнаходження;

- порядок внесення, зміни, поновлення, використання, поширення, знеособлення, знищення персональних даних у базі персональних даних;
- відповідальну особу або структурний підрозділ;
- порядок захисту персональних даних, в тому числі від незаконної обробки та незаконного доступу до них.

Відповідальна особа або структурний підрозділ відповідно до покладених завдань:

- забезпечує ознайомлення працівників володільця та розпорядника бази персональних даних з вимогами законодавства про захист персональних даних, зокрема щодо їхнього обов'язку не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали їм відомі у зв'язку з виконанням професійних, службових чи трудових обов'язків;
- забезпечує організацію обробки персональних даних працівниками володільця та розпорядника бази персональних даних відповідно до їх професійних, службових чи трудових обов'язків в обсязі, необхідному для виконання таких обов'язків;
- організовує роботу з обробки запитів щодо доступу до персональних даних суб'єктів відносин, пов'язаних з обробкою персональних даних;
- забезпечує доступ суб'єктів персональних даних до власних персональних даних;
- інформує керівника володільця та розпорядника бази персональних даних про заходи, яких необхідно вжити для приведення складу персональних даних та процедур їх обробки у відповідність до закону;
- інформує керівника володільця та розпорядника бази персональних даних про порушення встановлених процедур з обробки персональних даних.

Володілець бази персональних даних веде облік:

- фактів надання та позбавлення працівників права доступу до персональних даних та їх обробки;
- спроб та фактів несанкціонованих та/або незаконних дій з обробки персональних даних.

Володілець/розпорядник веде облік операцій, пов’язаних з обробкою персональних даних суб’єкта та доступом до них. З цією метою володільцем/розпорядником зберігається інформація про:

- дату, час та джерело збирання персональних даних суб’єкта;
- зміну персональних даних;
- перегляд персональних даних;
- будь-яку передачу (копіювання) персональних даних суб’єкта;
- дату та час видалення або знищення персональних даних;
- працівника, який здійснив одну із указаних операцій;
- мету та підстави зміни, перегляду, передачі та видалення або знищення персональних даних.

Володілець бази персональних даних може розмежувати режими доступу працівників до обробки персональних даних у базі персональних даних відповідно до їх професійних, трудових чи службових обов'язків.

Володілець бази персональних даних зберігає персональні дані у строк не більше, ніж це необхідно відповідно до мети їх обробки, якщо інше не передбачено законодавством. Знищення персональних даних здійснюється у спосіб, що виключає подальшу можливість поновлення таких персональних даних.

У момент збору персональних даних протягом десяти робочих днів з дня збору персональних даних суб’єкт персональних даних повідомляється про володільця персональних даних, склад та зміст зібраних персональних даних, права такого суб’єкта, визначені законодавством, мету збору персональних даних та осіб, яким передаються його персональні дані.

Володільці чи розпорядники баз персональних даних зобов'язані вносити зміни до персональних даних на підставі вмотивованої письмової вимоги суб'єкта персональних даних.

Дозволяється внесення змін до персональних даних за зверненням інших суб'єктів відносин, пов'язаних із персональними даними, якщо на це є згода суб'єкта персональних даних чи відповідна зміна здійснюється за рішенням суду, що набрало законної сили.

Згідно з Порядком повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації, який затверджено Наказом Уповноваженого Верховної Ради України з прав людини № 1/02-14 від 08.01.2014р. володільці, що здійснюють обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, зобов'язані повідомляти Уповноваженого про такі види обробки.

З метою повідомлення Уповноваженого володілець персональних даних подає до Секретаріату Уповноваженого заповнений бланк заяви за встановленою формою

Заява зокрема містить відомості про:

- володільця персональних даних:
- розпорядника персональних даних:
- персональні дані, що обробляються;
- мету обробки персональних даних (з посиланням на нормативно-правові акти, положення, установчі чи інші документи, які регулюють діяльність володільця персональних даних);
- категорію чи категорії суб'єктів, чиї персональні дані обробляються;
- третіх осіб, яким передаються персональні дані суб'єктів;
- транскордонну передачу персональних даних;

- місце (фактична адреса) обробки персональних даних;
- загальний опис технічних та організаційних заходів, що здійснюються володільцем персональних даних, для забезпечення їх захисту.

Заявники зберігають копію заяви, що була подана до Секретаріату Уповноваженого.

Уповноважений в порядку черговості надходження заяв, оприлюднює на офіційному веб-сайті Уповноваженого відомості із заяви в окремому розділі «Повідомлення про здійснення обробки персональних даних, що становить особливий ризик для прав і свобод суб'єктів персональних даних».

Володілець персональних даних, який повідомив Уповноваженого про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, повідомляє Уповноваженого про кожну зміну відомостей, що підлягали реєстрації.

Протягом 2014 року Уповноваженим опрацьовано понад 3000 повідомлень про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, та повідомлень про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці.

Як вже зазначалося обов'язковим учасником усіх правовідносин, в які включено його персональні дані є власне фізична особа, яка Законом «Про захист персональних даних іменується як «суб'єкт персональних даних».

Суб'єкт персональних даних має право:

- знати про місцезнаходження персональних даних, яка містить його персональні дані, її призначення та найменування, місцезнаходження та/або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом;

- отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані;
- на доступ до своїх персональних даних;
- отримувати не пізніш як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи зберігаються його персональні дані у відповідній базі персональних даних, а також отримувати зміст його персональних даних, які зберігаються;
- пред’являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних;
- пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;
- на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;
- звертатися із скаргами на обробку своїх персональних даних до органів державної влади та посадових осіб, до повноважень яких належить забезпечення захисту персональних даних, або до суду;
- застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних;
- вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди;
- відкликати згоду на обробку персональних даних;
- знати механізм автоматичної обробки персональних даних;

- на захист від автоматизованого рішення, яке має для нього правові наслідки.

Поширення персональних даних передбачає дії щодо передачі відомостей про фізичну особу за згодою суб'єкта персональних даних.

Поширення персональних даних без згоди суб'єкта персональних даних або уповноваженої ним особи дозволяється у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини.

Порядок доступу до персональних даних третіх осіб визначається умовами згоди суб'єкта персональних даних, наданої володільцю персональних даних на обробку цих даних, або відповідно до вимог закону.

Доступ до персональних даних третій особі не надається, якщо зазначена особа відмовляється взяти на себе зобов'язання щодо забезпечення виконання вимог Закону України «Про захист персональних даних» або неспроможна їх забезпечити.

Суб'єкт відносин, пов'язаних з персональними даними, подає запит щодо доступу (далі - запит) до персональних даних володільцю персональних даних.

У запиті зазначаються:

1) прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує фізичну особу, яка подає запит (для фізичної особи - заявника);

2) найменування, місцезнаходження юридичної особи, яка подає запит, посада, прізвище, ім'я та по батькові особи, яка засвідчує запит; підтвердження того, що зміст запиту відповідає повноваженням юридичної особи (для юридичної особи - заявника);

3) прізвище, ім'я та по батькові, а також інші відомості, що дають змогу ідентифікувати фізичну особу, стосовно якої робиться запит;

4) відомості про базу персональних даних, стосовно якої подається запит, чи відомості про володільця чи розпорядника персональних даних;

5) перелік персональних даних, що запитуються;

6) мета та/або правові підстави для запиту.

Строк вивчення запиту на предмет його задоволення не може перевищувати десяти робочих днів з дня його надходження.

Протягом цього строку володілець персональних даних доводить до відома особи, яка подає запит, що запит буде задоволено або відповідні персональні дані не підлягають наданню, із зазначенням підстави, визначеної у відповідному нормативно-правовому акті.

Запит задовольняється протягом тридцяти календарних днів з дня його надходження, якщо інше не передбачено законом.

Суб'єкт персональних даних має право на одержання будь-яких відомостей про себе у будь-якого суб'єкта відносин, пов'язаних з персональними даними крім випадків, установлених законом. Відстрочення доступу суб'єкта персональних даних до своїх персональних даних не допускається.

Відстрочення доступу до персональних даних третіх осіб допускається у разі, якщо необхідні дані не можуть бути надані протягом тридцяти календарних днів з дня надходження запиту. При цьому загальний термін вирішення питань, порушених у запиті, не може перевищувати сорока п'яти календарних днів.

Повідомлення про відстрочення доводиться до відома третьої особи, яка подала запит, у письмовій формі з роз'ясненням порядку оскарження такого рішення.

У повідомленні про відстрочення зазначаються:

1) прізвище, ім'я та по батькові посадової особи;

2) дата відправлення повідомлення;

3) причина відстрочення;

4) строк, протягом якого буде задоволено запит.

Відмова у доступі до персональних даних допускається, якщо доступ до них заборонено згідно із законом.

У повідомленні про відмову зазначаються:

1) прізвище, ім'я, по батькові посадової особи, яка відмовляє у доступі;

2) дата відправлення повідомлення;

3) причина відмови.

Рішення про відстрочення або відмову у доступі до персональних даних може бути оскаржено до суду. Якщо запит зроблено суб'єктом персональних даних щодо даних про себе, обов'язок доведення в суді законності відмови у доступі покладається на володільця персональних даних, до якого подано запит.

Доступ суб'єкта персональних даних до даних про себе здійснюється безоплатно. Доступ інших суб'єктів відносин, пов'язаних з персональними даними, до персональних даних певної фізичної особи чи групи фізичних осіб може бути платним у разі додержання умов, визначених Законом «Про захист персональних даних». Оплаті підлягає робота, пов'язана з обробкою персональних даних, а також робота з консультування та організації доступу до відповідних даних.

Розмір плати за послуги з надання доступу до персональних даних органами державної влади визначається Кабінетом Міністрів України.

Органи державної влади та органи місцевого самоврядування мають право на безперешкодний і безоплатний доступ до персональних даних відповідно до їх повноважень.

Про передачу персональних даних третій особі володілець персональних даних протягом десяти робочих днів повідомляє суб'єкта персональних даних, якщо цього вимагають умови його згоди або інше не передбачено законом.

Повідомлення суб'єкта персональних даних про передачу персональних даних третій особі не здійснюються у разі:

1) передачі персональних даних за запитами при виконанні завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом;

2) виконання органами державної влади та органами місцевого самоврядування своїх повноважень, передбачених законом;

3) здійснення обробки персональних даних в історичних, статистичних чи наукових цілях;

4) повідомлення суб'єкта персональних даних відповідно до вимог законодавства.

Вивчаючи практику виконання володільцями запитів від правоохоронних органів Уповноважений наголошує, що у таких запитах обов'язково мають бути посилання на відкриту оперативно-розшукову справу або кримінальне провадження, конкретні звернення громадян та/або повідомлення про злочин, на підставі яких виникла необхідність в отриманні запитуваної інформації.

У разі відсутності у запиті конкретизації мети та/або достатніх правових підстав для запиту володілець персональних даних має законне право відмовити у наданні запитуваної інформації.

В іншому випадку поширення конфіденційної інформації про особу на запит, що не містить достатнього обґрунтування, а також поширення даних, що не є необхідними для виконання відповідних повноважень, є прямим порушенням права особи на захист персональних даних та тягне за собою накладення адміністративного стягнення.

3.3 Державний контроль в сфері обігу персональних даних

Згідно із Законом України «Про захист персональних даних» Уповноважений Верховної Ради України з прав людини є уповноваженим державним органом з питань захисту персональних даних.

Уповноважений Верховної Ради України з прав людини у зв'язку із цим має такі повноваження:

- отримувати пропозиції, скарги та інші звернення фізичних і юридичних осіб з питань захисту персональних даних та приймати рішення за результатами їх розгляду

  (*Протягом 2014 року до Уповноваженого надійшло 928 звернень щодо питань захисту персональних даних. За скаргами громадян було відкрито 485 проваджень щодо порушення прав на захист персональних даних. Із них у 365 випадках порушень виявлено не було*;
- проводити на підставі звернень або за власною ініціативою виїзні та безвиїзні, планові, позапланові перевірки володільців або розпорядників персональних даних у порядку, визначеному Уповноваженим, із забезпеченням відповідно до закону доступу до приміщень, де здійснюється обробка персональних даних;
- отримувати на свою вимогу та мати доступ до будь-якої інформації (документів) володільців або розпорядників персональних даних, які необхідні для здійснення контролю за забезпеченням захисту персональних даних, у тому числі доступ до персональних даних, відповідних баз даних чи картотек, інформації з обмеженим доступом;
- затверджувати підзаконні нормативно-правові акти у сфері захисту персональних даних;

  (Наказом Уповноваженого Верховної Ради України з прав людини № 1/02-14 від 08.01.2014 р. затверджено:

  Типовий порядок обробки персональних даних;

  Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних;

  Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що

організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації.)

- за підсумками перевірки, розгляду звернення видавати обов'язкові для виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних, у тому числі щодо зміни, видалення або знищення персональних даних, забезпечення доступу до них, надання чи заборони їх надання третій особі, зупинення або припинення обробки персональних даних;
- надавати рекомендації щодо практичного застосування законодавства про захист персональних даних, роз'яснювати права і обов'язки відповідних осіб за зверненням суб'єктів персональних даних, володільців або розпорядників персональних даних, структурних підрозділів або відповідальних осіб з організації роботи із захисту персональних даних, інших осіб;
- звертатися з пропозиціями до Верховної Ради України, Президента України, Кабінету Міністрів України, інших державних органів, органів місцевого самоврядування, їх посадових осіб щодо прийняття або внесення змін до нормативно-правових актів з питань захисту персональних даних;
- надавати за зверненням професійних, самоврядних та інших громадських об'єднань чи юридичних осіб висновки щодо проектів кодексів поведінки у сфері захисту персональних даних та змін до них;
- складати протоколи про притягнення до адміністративної відповідальності та направляти їх до суду у випадках, передбачених законом;

(У 2014 році представниками Уповноваженого було складено 8 протоколів про притягнення до адміністративної відповідальності, з них 4 – відповідно до ч.4 ст. 188[39] Кодексу України про адміністративні правопорушення (далі – КУпАП) (недодержання

встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних) та 4 – відповідно до статті 188[40] КУпАП (невиконання законних вимог Уповноваженого Верховної Ради України з прав людини або представників Уповноваженого Верховної Ради України з прав людини).

- інформувати про законодавство з питань захисту персональних даних, проблеми його практичного застосування, права і обов'язки суб'єктів відносин, пов'язаних із персональними даними;
- організовувати та забезпечувати взаємодію з іноземними суб'єктами відносин, пов'язаних із персональними даними, виконанням Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до неї, інших міжнародних договорів України у сфері захисту персональних даних;
- брати участь у роботі міжнародних організацій з питань захисту персональних даних.

Уповноважений Верховної Ради України з прав людини здійснює контроль за додержанням вимог законодавства про захист персональних даних шляхом проведення перевірок фізичних осіб, фізичних осіб - підприємців, підприємств, установ і організацій усіх форм власності, органів державної влади та місцевого самоврядування, що є володільцями та/або розпорядниками персональних даних

Контроль за додержанням суб'єктами перевірки законодавства про захист персональних даних здійснюється шляхом проведення планових та позапланових перевірок. Планові та позапланові перевірки є виїзними та безвиїзними.

Планові перевірки проводяться здійснюються з періодичністю не частіше одного разу на рік відповідно до річних або квартальних планів, які

затверджуються Уповноваженим до 1 грудня року, що передує плановому, або до 25 числа останнього місяця кварталу, що передує плановому.

У плані зазначаються категорії суб'єктів перевірок. План проведення перевірок після його затвердження розміщується на офіційному веб-сайті Уповноваженого.

Позапланові перевірки суб'єктів перевірки можуть проводитись за наявності однієї або декількох підстав/приводів, зокрема:

- за власною ініціативою Уповноваженого;
- при безпосередньому виявленні порушень вимог законодавства про захист персональних даних Уповноваженим, в тому числі і в результаті здійснення дослідження системних проблем щодо забезпечення права на приватність, повагу до приватного та сімейного життя;
- при наявності інформації про порушення вимог законодавства про захист персональних даних в повідомленнях, опублікованих в засобах масової інформації, оприлюднених в мережі Інтернет;
- обґрунтовані звернення фізичних та юридичних осіб з повідомленням про порушення фізичною особою, фізичною особою - підприємцем, підприємством, установою і організацією усіх форм власності, органом державної влади чи місцевого самоврядування, що є володільцями та/або розпорядниками персональних даних вимог законодавства про захист персональних даних;
- виявлення недостовірності у відомостях (даних), наданих суб'єктом перевірки на письмовий запит Уповноваженого щодо здійснення безвиїзної перевірки, та/або якщо такі відомості (дані) не дають змоги оцінити виконання суб'єктом перевірки вимог законодавства про захист персональних даних;
- контроль за виконанням суб'єктом перевірки приписів щодо усунення порушень вимог законодавства про захист персональних даних, виданих за результатами проведення перевірок.

Виїзна перевірка проводиться Уповноваженим та/або на підставі виданого ним іменного доручення керівником Секретаріату Уповноваженого чи іншими його працівниками або представниками Уповноваженого;

Доручення видається у письмовій формі на визначений у ньому строк.

До участі в перевірці в установленому законодавством порядку можуть бути залучені працівники органів державної влади, в тому числі органів державного управління, органів виконавчої влади та правоохоронних органів. В разі залучення вказаних осіб вони дають письмове зобов’язання про нерозголошення персональних даних, які стануть їм відомі в результаті проведення перевірки.

Виїзні перевірки здійснюються в робочий час суб’єкта перевірки, встановлений правилами внутрішнього трудового розпорядку.

Уповноважена посадова особа при проведенні перевірки має право:

- безперешкодно входити на об'єкт перевірки за службовим посвідченням і мати безперешкодний доступ до місць зберігання інформації, у тому числі й до комп'ютерів, магнітних носіїв інформації тощо.
- отримувати на свою вимогу та мати доступ до будь-якої інформації (документів) володільців або розпорядників персональних даних, які необхідні для здійснення контролю за забезпеченням захисту персональних даних, у тому числі доступ до персональних даних, відповідних баз даних чи картотек, інформації з обмеженим доступом.
- отримувати засвідчені у встановленому законодавством порядку копії документів.
- вимагати в межах своєї компетенції у керівника та/або посадових осіб суб'єкта перевірки надання завірених підписом письмових пояснень.
- звертатись у зв'язку з реалізацією своїх повноважень та відповідно до законодавства до органів прокуратури, інших правоохоронних органів.

- складати та підписувати протоколи про притягнення до адміністративної відповідальності за виявлені порушення законодавства про захист персональних даних
- складати та підписувати приписи про запобігання або усунення порушень законодавства про захист персональних даних.

Уповноважена посадова особа при проведенні перевірки зобов'язана:

- повідомити керівника суб'єкта перевірки або уповноважену ним особу про свої обов'язки та повноваження, причину та мету перевірки, права, обов'язки керівника та посадових осіб суб'єкта перевірки;
- ознайомити керівника суб'єкта перевірки або уповноважену ним особу з результатами проведеної перевірки та/або протоколом про адміністративні правопорушення;
- визначати перелік необхідних для перевірки документів та строки їх надання;

Посадові особи суб'єкта перевірки, в тому числі керівник суб'єкта перевірки або уповноважена ним особа, під час здійснення перевірки зобов'язані:

- безперешкодно допускати уповноважену посадову особу (осіб) на об'єкт перевірки та надавати доступ до документів та інших матеріалів, потрібних для проведення перевірки;
- надавати необхідні документи, та іншу інформацію, завірені підписом письмові пояснення, а також засвідчені в установленому законодавством порядку копії документів, що необхідні проведення перевірки;
- виконувати вимоги уповноваженої посадової особи (осіб) з питань додержання вимог законодавства про захист персональних даних.

Посадові особи суб'єкта перевірки, в тому числі керівник суб'єкта перевірки або уповноважена ним особа, під час здійснення перевірки мають право:

- перевіряти наявність в уповноваженої посадової особи (осіб) службового посвідчення та підстав для проведення перевірки;
- бути присутніми під час здійснення перевірки;
- одержувати та ознайомлюватись за результатами проведеної перевірки з актом та/або протоколом про адміністративне правопорушення;
- надавати в письмовій формі свої пояснення та зауваження до акта та/або протоколу про адміністративні правопорушення;
- оскаржувати в установленому законом порядку неправомірні дії уповноваженої посадової особи (осіб).

За результатами здійснення планової або позапланової перевірки Уповноважений та/або уповноважена посадова особи складає у двох примірниках акт перевірки додержання вимог законодавства про захист персональних даних, який підписується Уповноваженим або уповноваженою посадовою особою (особами), яка проводила перевірку, та керівником суб'єкта перевірки або уповноваженою ним особою.

Акт повинен містити один із таких висновків:

- про відсутність у діяльності суб'єкта перевірки порушень вимог законодавства про захист персональних даних;
- про виявлені у діяльності суб'єкта перевірки порушення вимог законодавства про захист персональних даних, їх детальний опис із посиланням на норми чинного законодавства, які порушено.

В Акті викладаються всі виявлені під час перевірки факти невиконання (неналежного виконання) суб'єктом перевірки вимог законодавства про захист персональних даних. Забороняється вносити до акта перевірки відомості про порушення, які не підтверджено документально.

У разі ненадання суб'єктом перевірки документів, необхідних для проведення перевірки, в Акті робиться запис про це із зазначенням причин.

Якщо суб'єкт перевірки не погоджується з Актом, він підписує його із зауваженнями. Зауваження суб'єкта перевірки щодо здійснення уповноваженими посадовими особами контролю за дотриманням вимог законодавства про захист персональних даних є невід'ємною частиною Акта.

У разі відмови керівника суб'єкта перевірки або уповноваженої ним особи підписати Акт уповноважена посадова особа вносить до такого Акта відповідний запис.

Перший примірник Акта вручається керівнику суб'єкта перевірки або уповноваженій ним особі, про що ним (нею) ставиться підпис на другому примірнику Акта, який зберігається в Секретаріаті Уповноваженого.

У випадку відмови керівника суб'єкта перевірки або уповноваженої ним особи отримати другий примірник Акта він направляться суб'єкту перевірки протягом 5 робочих днів рекомендованим листом з повідомленням про вручення.

До примірника Акта, який зберігається в Секретаріаті Уповноваженого обов'язково додаються матеріали перевірки - копії документів, витяги з документів, належним чином засвідчені суб'єктом перевірки, пояснення, протоколи та інші документи.

На підставі Акта перевірки, під час якої виявлено порушення вимог законодавства про захист персональних даних, складається припис про усунення порушень вимог законодавства у сфері захисту персональних даних, виявлених під час перевірки.

У приписі зазначаються:

- підстава для видачі припису;
- заходи необхідні для усунення порушень, виявлених під час перевірки;
- строк виконання припису;
- строк інформування суб'єктом перевірки Уповноваженого про усунення виявленого порушення;

- підпис уповноваженої посадової особи (осіб), яка проводила перевірку.

Припис складається у двох примірниках: перший примірник не пізніше 5 робочих днів з дня складання Акта перевірки надсилається суб'єкту перевірки чи уповноваженій ним особі рекомендованим листом з повідомленням про вручення, а другий примірник залишається в Секретаріаті Уповноваженого.

Суб'єкт перевірки повинен протягом визначеного у приписі строку (не менше ніж 30 календарних днів) вжити заходів щодо усунення порушень, зазначених у приписі, та письмово поінформувати Уповноваженого про усунення порушень разом із наданням копій документів, що це підтверджують.

Контроль за своєчасністю та повнотою виконання вимог, зазначених у приписі, здійснюється шляхом вивчення вказаних копій документів та, у разі необхідності, шляхом проведення позапланової перевірки.

У разі невиконання припису протягом вказаного у ньому строку Уповноважений або уповноважена посадова особа складає протокол про адміністративне правопорушення, передбачене статтею 188^{40} Кодексу України про адміністративні правопорушення

У разі виявлення під час перевірки суб'єкта перевірки ознак кримінального правопорушення Уповноважений направляє необхідні матеріали до правоохоронних органів.

Протягом 2015 року представниками Уповноваженого Верховної Ради України з прав людини було проведено 62 планові та позапланові перевірки володільців персональних даних. З огляду на результати проведених перевірок основними порушеннями при обробці персональних даних є:

– невідповідність внутрішніх положень та документів володільця персональних даних вимогам чинного законодавства про захист персональних даних;
– відсутність обліку працівників, які мають доступ до персональних

даних суб'єктів персональних даних;

- не ведеться або ведеться частково/не в повному обсязі облік операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них;
- у працівників, які мають доступ до персональних даних не відбирається зобов'язання не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних обов'язків;
- відсутність повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних та про створення (визначення) відповідального структурного підрозділу або відповідальної особи, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, у випадку коли таке повідомлення вимагається відповідно до закону;
- майже всі володільці отримують згоди на обробку персональних даних від працівників для реалізації прав та обов'язків у сфері трудових відносин, в той час як обробка персональних даних працівників здійснюється на підставі дозволу, наданого володільцю персональних даних, відповідно до закону виключно для здійснення його повноважень, а тому, окрема згода на обробку таких відомостей не вимагається;
- склад та зміст персональних даних, що обробляється в багатьох випадках є надмірним стосовно визначеної мети їх обробки;
- не дотримання принципу строковості обробки/зберігання, а саме обробка персональних даних здійснюється довше, ніж це необхідно для законних цілей, у яких вони збиралися або надалі оброблялися.

Варто зазначити, що Україна, виконуючи вимоги ЄС щодо отримання безвізового режиму, сформувала централізовану систему захисту персональних даних, яка у доповненні галузевими режимами захисту цієї

інформації у якості таємної надає людині початкові можливості захистити свої права в досудовому і судовому порядку Проте з огляду на величезні масиви вже зібраних на сьогодні персональних даних та чисельність їх володільців основні ризики і основний тягар застосування механізмів захисту залишаються покладеними на суб'єкта персональних даних.

Питання для самоконтролю до розділу 3

1. Наведіть перелік видів приватності.
2. Дайте визначення персональним даним.
3. Наведіть перелік учасників правовідносин, пов'язаних з обігом персональних даних.
4. В яких правових джерелах закріплено загальні принципи обробки персональних даних?
5. Назвіть підстави для обробки персональних даних.
6. Наведіть перелік «чутливих» персональних даних.
7. У чому полягають відмінності правового статусу володільця та розпорядника персональних даних?
8. Перерахуйте права суб'єкта персональних даних у зв'язку із обробкою його персональних даних у базі.
9. У яких випадках не здійснюються повідомлення суб'єкта персональних даних про передачу персональних даних третій особі?
10. Які повноваження надано Уповноваженому Верховної Ради України з прав людини як уповноваженому державному органу з питань захисту персональних даних?
11. Назвіть види перевірок законодавства про захист персональних даних.
12. За які правопорушення встановлено адміністративну відповідальність у сфері обігу персональних даних?
13. Розкрийте структуру акта перевірки додержання вимог законодавства про захист персональних даних.
14. Розкрийте порядок винесення та виконання припису про усунення порушень вимог законодавства у сфері захисту персональних даних

Література

1. Конституція України // Відомості Верховної Ради України, 1996 р., N 30, ст. 141.
2. Конвенція Ради Європи "Про захист прав людини та основних свобод" (Рим, 04.09.1950р.) та Протокол № 11 // Голос України. – 2001. – № 3 (2503). – С. 6–8.

3. Право на приватність: conditio sine qua non / Харківська правозахисна група; Худож.-оформлювач О.Герчук – Харків: Фоліо, 2003. – 216 с.

4. Закон України "Про інформацію" від 13.01.2011р. // Офіційний вісник України від 18.02.2011 - 2011 р., № 10, стор. 21, стаття 445, код акту 54789/2011

5. Закон України «Про захист персональних даних» // Офіційний вісник України від 09.07.2010 - 2010 р., № 49, стор. 199, стаття 1604

6. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних [Електронний ресурс] http://zakon0.rada.gov.ua/laws/show/994_326

7. Кримінальний кодекс України // Офіційний Вісник України 2001, N 21, ст. 920.

8. Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації: затв. Наказом Уповноваженого Верховної Ради України з прав людини № 1/02-14 від 08.01.2014р. [Електронний ресурс] http://zakon3.rada.gov.ua/laws/show/v1_02715-14#n11

9. Типовий порядок обробки персональних даних у базах персональних даних: затв. Наказом Уповноваженого Верховної Ради України з прав людини № 1/02-14 від 08.01.2014р. [Електронний ресурс] http://zakon3.rada.gov.ua/laws/show/v1_02715-14#n11

10. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини "Про стан додержання та захисту прав і свобод людини і громадянина в Україні".- К., 2015.- 552 с.

11. Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних затв. Наказом Уповноваженого Верховної Ради України з прав людини № 1/02-14 від 08.01.2014р. [Електронний ресурс] http://zakon3.rada.gov.ua/laws/show/v1_02715-14#n11

12. Результати перевірок: інформація з офіційного сайту Уповноваженого Верховної Ради України з прав людини станом на 20.06.2017 р. [Електронний ресурс] http://www.ombudsman.gov.ua/ua/page/zpd/kontrol/rezultati-perevirok/

13. Закон України «Про доступ до публічної інформації» // Голос України від 09.02.2011 - № 24

14. Роз'яснення Уповноваженого Верховної Ради України з прав людини до Типового порядку обробки персональних даних від 08.01.2014 р. [Електронний ресурс] - http://zakon0.rada.gov.ua/laws/show/n0001715-14

15. Постанова Пленуму Верховного Суду України N 4 від 31.03.95р. «Про судову практику в справах про відшкодування моральної (немайнової) шкоди»

16. Рекомендація 1506 (2001) Парламентської Асамблеї Ради Європи "Свобода слова та інформації в засобах масової інформації в Європі"

17. Жорж М. Саттон Г. Аналіз закону України «Про захист персональних даних».- Страсбург, 2012. – 45 с.

18. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015. – 220 с.

19. Посібник з європейського права у сфері захисту персональних даних. — К.: К.І.С., 2015. — 216 с.

20. Пікерт В. Європейські стандарти щодо свободи висловлювань (стаття 10 ЄКПЛ) стосовно законодавства про захист честі й гідності і практика їх застосування. – //Свобода висловлювань і приватність. – № 1, 2001. – С. 21-24.

21. Брижко В.М. Правовий механізм захисту персональних даних: Монографія / За заг. ред. д.е.н., професора, заслуженого діяча науки і техніки України М.Я. Швеця та д.ю.н., професора Р.А. Калюжного. – К.: Парламентське видавництво, 2003. – 120 с.

22. Правила защиты для файлов персональных данных в Совете Европы. Приложение: Комиссар по защите данных. Страсбург, от 01.10.1985 г.

23. Директива 95/46/ЄС Європейського парламенту та Ради Європейського Союзу “Про захист осіб у зв’язку з обробкою персональних даних та вільним обігом цих даних” від 24.10.1995 р. [Електронний ресурс] www.evropa.eu.int/ISPO/legal/en/dataprot /directiv/directiv.html.

24. Директива 97/66/ЄС Європейського парламенту та Ради Європейського Союзу “Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі” від 15.12.1997 р. [Електронний ресурс] www.evropa.eu.int/ISPO/legal /en/dataprot/protection.html

25. Передача персональных данных между третьими сторонами и третьими странами, согласно Конвенции № 108 СЕ, не обеспечивающими адекватный уровень защиты. Проект Джерома Хает, профессора права, Директора СЕЈЕМ (Центр изучения мультимедиа) от 21 января 2001 г. Рассмотрен рабочей Группой Консультативного Комитета СЕ, 6–ая встреча, Страсбург, 7–9 февраля 2001 г.

26. Баранов А.А., Брыжко В.М., Базанов Ю.К. Защита персональных данных. – К.: Национальное агентство по вопросам информатизации при Президенте Украины, 1998. – 128 с.

27. Баранов А.А., Брыжко В.М., Базанов Ю.К. Права человека и защита персональных данных. – Харьков: ХПГ–Фолио (при содействии Национального фонда поддержки демократии США), 2000. – 280 с.

28. Брижко В.М. Персональні дані та право власності. // Українське право: Українська правнича фундація. – 2002. – № 1. – С. 152–157.

29. Брижко В.М. Правовий механізм захисту персональних даних: Монографія / За заг. ред. д.е.н., професора, заслуженого діяча науки і техніки

України М.Я. Швеця та д.ю.н., професора Р.А. Калюжного. – К.: Парламентське видавництво, 2003. – 120 с.

30. Гарстка Х. Требования к адекватной защите персональных данных, сформулированные в директиве по защите персональных данных Европейского Союза (Выступление Генерального уполномоченного ФРГ по защите персональных данных) / Семинар “Неприкосновенность частной жизни в эпоху современных технологий”, 1999 [Електронний ресурс] www.libertarium.ru/immuni ty_doc3

31. Дидук А.Г. Правовой режим конфиденциальной информации: гражданско-правовой аспект Дисс. канд. юр. наук: 12.00.03 /Харьковский национальный университет внутренних дел.-Харьков, 2008.-243 с.

32. Європа на шляху до інформаційного суспільства. Матеріали Європейської комісії 1994–1995 рр. – К.: ДКЗІ, 2000. – 176 с.

33. Иванский В.П. Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования: Монография. – М.: Издательство РУДН, 1999. – 276 с.

34. Копылов В.А. Информационное право: Учебник. – 2-е изд., перераб. и доп. – М.: Юристъ, 2002. – 512 с.

35. Пазюк А.В. Захист прав людини стосовно обробки персональних даних: міжнародні стандарти. – К.: МГО Прайвексі Юкрейн, 2000. – 83 с.

36. Пазюк А.В. Международно-правовая защита права человека на приватность персонифицированной информации: Дисс. канд..юр. наук:12.00.11 Киевский национальный университет имени Тараса Шевченко.- Киев, 2004.- 205 с.

37. Романов Р. Громадянин і держава: сучасні проблеми ідентифікації особи в Україні. – Харків: Свобода висловлювань і приватність (інформаційний бюлетень Харківської правозахисної групи “Права людини”), 1999. – № 3–4.

38. Секей И. Принципы информационного самоопределения и разрешение проблем с помощью законодательства (венгерская модель) (Выступление Комиссара по защите данных Венгрии) // Семинар “Неприкосновенность частной жизни в эпоху современных технологий”, 1999 [Електронний ресурс] www.libertarium.ru/libertarium/im munity_doc2

39. Смирнов С. Приватность. – М.: Права человека, 2002. – 96 с.

40. Томин С.В. Основні етапи роботи з джерелами особистісної інформації у процесі розкриття та розслідування злочинів: Автореф дис. канд..юр. наук: 12.00.09 / Одеська національна юридична академія, Одеса, 2007.- 22с.

41. Устименко Н.В.Тайны личной жизни человека и их гражданско-правовая охрана: Дисс. канд..юр. наук: 12.00.03 / Национальная юридическая академия Украины им. Я. Мудрого Харьков, 2001.-204 с.

42. Хартия Глобального информационного общества (Окинава). – М.: Дипломатический вестник. – 2000. – № 8. – С. 51–56.

43. Цимбалюк В.С., Гавловський В.Д. Інформаційне право. Навчально-методичний комплекс. – К.: Інститут економіки управління та господарського права,. 1999. – 183 с.

44. Шомье Ж. Банки данных. Пер. с франц. под ред. Б.Щукина. – М.: Энергоиздат, 1981.

РОЗДІЛ 4
СУЧАСНІ ТЕНДЕНЦІЇ ВИКОРИСТАННЯ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В УСТАНОВАХ

4.1 Загрози від несанкціонованого витоку інформації з обмеженим доступом

Значна кількість нормативно-правових актів, які введені в дію в нашій державі і спрямовані на врегулювання суспільних відносин пов'язаних із використанням різних видів інформації, наочно демонструє важливість даного питання для країни. Згадаємо тільки закони України: «Про інформацію», «Про державну таємницю», «Про основи національної безпеки», «Про доступ до публічної інформації», «Про захист персональних даних» «Про захист інформації в інформаційно-телекомунікаційних системах» тощо.

Поряд з реалізацією прав громадян на доступ до відкритої інформації, значна кількість норм цих законодавчих актів спрямована на захист різних категорій інформації з обмеженим доступом на підприємствах, установах і організаціях (далі - установи), несанкціонований виток якої може завдати шкоди особі, суспільству і державі.

Збільшення уваги до захисту інформаційної сфери, зокрема, в Україні, не випадково, якщо враховувати світові збитки та негативні, а часом і трагічні наслідки від витоку подібної інформації.

Проведення аналітичних досліджень стосовно світових тенденцій можливих каналів витоку інформації з обмеженим доступом в установах здійснюється значною кількістю різних, в тому числі, міжнародних організацій.

Як правило, такі дослідження ґрунтуються на зборі, накопиченні та опрацюванні відомостей щодо подібних фактів витоку інформації з обмеженим доступом. Тут потрібно зважати на джерела отримання інформації та, відповідно, достовірність даних, що використовуються.

Наприклад, аналітичний центр компанії «InfoWatch» з 2004 року формує базу інформаційних витоків.

В 2008 році за ініціативою компанії «PricewaterhouseCoopers» (PwC) відбулось широкомасштабне дослідження «The Global State of Information Security – 2008». За даними аналітиків цієї компанії у дослідженні взяли участь 7 тисяч фахівців з інформаційної безпеки із різних країн. З них понад 2000 фахівців представляли держави Європи.

Попереднє дослідження «Global State of Information Security 2006» ґрунтувалось на опитуваннях 13 тисяч компаній з 63 країн світу.

Завдяки проведенню подібної аналітичної роботи різні суб'єкти діяльності здатні враховувати загальні тенденції та новітні загрози існуванню інформації з обмеженим доступом й можливі нові, уразливі канали витоку такої інформації.

Так, проведені аналітичні та статистичні дослідження компаній «InfoWatch», «InsightExpress», «Perimetrix», «Ponemon Institute», «PricewaterhouseCoopers» (PwC), «WatchGuard Technologies» дозволяють виділити найбільш поширені причини несанкціонованого витоку інформації.

Перш за все виділимо цілеспрямовані дії «організації-конкурента». Саме ця причина за прогнозами може завдати найбільшої шкоди власнику інформації з обмеженим доступом. Одночасно, на практиці, далеко не завжди вдається визначити справжнього винуватця, який спровокував виток інформації.

У повідомленнях ЗМІ часто з'являється інформація про те, що в різних країнах світу все більше виникає фірм, які пропонують послуги бізнес-шпигунства. Вартість таких послуг може коливатись від 500 до 50 тисяч доларів і більше. Здебільшого клієнтів подібних фірм цікавлять відомості про роботу підприємства-конкурента, його плани, оригінальні ідеї, організацію виробничого процесу тощо.

Зокрема, нещодавно було підтверджено факт промислового шпигунства з боку британської команди «Макларен» щодо конструктивних

новинок «Феррарі». На підставі цього англійська команда була дискваліфікована зі змагань та оштрафована на суму у 100 млн. доларів.

Проте на цьому полювання за секретами «Феррарі» не скінчилось. Вже через рік, технічний директор «Феррарі» Альдо Коста зробив заяву про те, що його команда ініціювала службове розслідування за фактом витоку інформації, про яку знало тільки обмежене коло осіб. Це було зроблено після того, як у лютому 2012 року видання «Autosprint» опублікувало інформацію про інноваційні отвори в носовій частині боліда, додавши ряд ескізів зазначеного «ноу-хау».

Великий відсоток несанкціонованого витоку інформації відбувається з приводу навмисних або недбалих, необережних дій осіб допущених до інформації, яка потребує збереження. Недаремно людський фактор в змозі звести нанівець найкращі заходи безпеки інформації.

В березні 2009 року, за повідомленням «Channel 4 News», стало відомо про виток медичних відомостей (персональні дані, результати аналізів тощо) з однієї із лабораторій «Laboratory Corporation of America» (LabCorp). Тисячі документів з персональними даними просто випали із вантажної машини під час транспортування.

Фінансовий сюрприз у січні 2010 року отримали клієнти берлінського банку «LBB». Декілька десятків тисяч клієнтів банку були змушені заблокувати свої рахунки зважаючи на ризик доступу до них зловмисників. Подія сталась через витік даних у США яку допустила компанія «Hertland Payment Systems», яка обробляла платежі за банківськими картками.

Іноді розголошення важливої інформації може стати підставою для смертельного вироку. На початку 2012 року, як зазначала сеульська газета «Chosun llbo», за звинуваченням у витоку секретної інформації було розстріляно колишнього міністра транспорту КНДР. Виток інформації, щодо пересування спеціального потягу в якому знаходився лідер Північної Кореї, за висновком слідства, став причиною для здійснення терористичного акту.

У 2009 році поліція вже Південної Кореї заарештувала колишнього працівника «LG Electronics» за звинуваченням у передаванні китайській стороні секретних даних про завод з виробництва плазмових дисплеїв. Згідно із приблизними підрахунками шкода може сягнути розміру у 1,4 млрд. доларів.

Виток інформації з обмеженим доступом не завжди може призвести безпосередньо до трагічних наслідків й суттєвих економічних збитків.

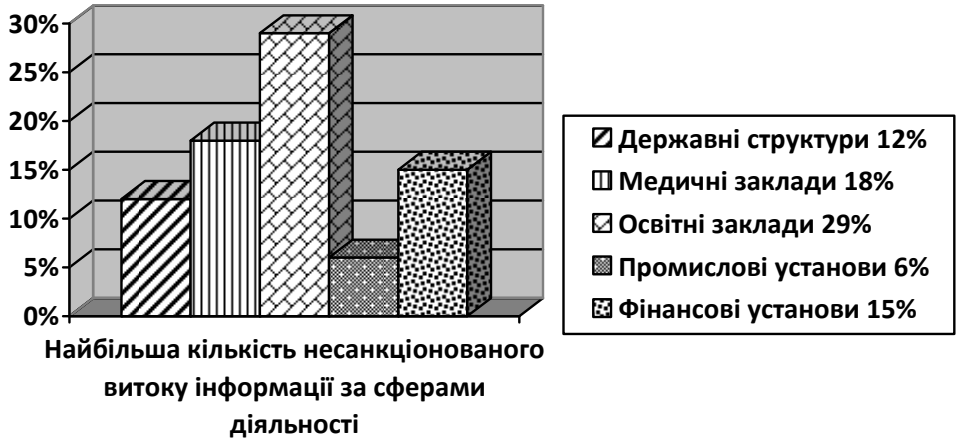
Світові ЗМІ у серпні 2010 року наголошували на великому скандалі, який був пов'язаний із продажем японським офіцером комерційній структурі персональних даних стосовно десятків тисяч військовослужбовців. Разом з тим, результати такого витоку, в дійсності, не нанесли передбачуваних збитків, якщо не зважати, що вони були використані в рекламних цілях. Військовослужбовці стали регулярно отримувати значну кількість різних рекламних пропозицій.

Безумовним лідером щодо фактів несанкціонованого витоку інформації, останніми роками, залишаються персональні дані. Що, зрозуміло не випадково, оскілки подібні масиви інформації використовує значна кількість організацій у повсякденній діяльності.

Варто уваги співвідношення витоків інформації з обмеженим доступом за різними категоріями у світі визначене компанією «InfoWatch»:

Згідно результатів досліджень компанії «Perimetrix» стосовно типів організацій «світових лідерів» щодо несанкціонованого витоку інформації

були визначені: освітні заклади, медичні заклади, фінансові установи за якими йдуть державні установи управлінської сфери й промислові установи.



Видання «The Salt Lake Tribune» повідомило про крадіжку резервного носія інформації, який містив персональні дані 2,2 млн. чоловік із медичного відділення Університету штату Юта (University of Utah Hospitals & Clinics). Публікація у «Cnews» додає, що понад 60 відсотків викрадених записів містили окрім різних персональних даних, номери соціального страхування, які визначені у США конфіденційною інформацією.

Викрадення відбулось завдяки недбалому відношенню кур'єра до збереження інформації. У порушення вимог інструкції з безпеки, носій інформації з обмеженим доступом не було передано до сховища, а залишено на ніч у автомобілі поблизу дома де мешкав кур'єр. Саме звідти відомості й були викрадені. Зазначається, що цей кур'єр до цього мав 18-ти річний стаж сумлінної роботи.

Аналітичний центр компанії «Perimetrix» зафіксував цілу низку витоку інформації з обмеженим доступом з установ (переважно персональні дані), які здійснюють освітню діяльність та державних установ управлінської сфери. Наведемо тільки окремі приклади:

Організація	Сфера діяльності	Причина витоку	Приблизна кількість	Приблизні втрати

			постраждалих	
Rochester Institute of Technology	освіта	викрадення ноутбука	12745 чоловік	2,3 млн. доларів
Reynoldsburg City Schools	освіта	викрадення ноутбука	4259 чоловік	750 тыс. доларів
Prince William County Public Schools	освіта	веб-виток	2600 чоловік	600 тыс. доларів
Iowa County Recorders Association	Державна структура	веб-виток	підраховується (попередньо декілька тисяч)	підраховується
National Offender Management Service	Державна структур	втрата носія інформації	5000 чоловік	1,3 млн. доларів

Якщо додати, що в таблиці визначені далеко не найбільші втрати, цілком слушним постає питання, як все такі обраховуються подібні збитки стосовно, зокрема, витоку персональних даних.

Справа в тому, що порахувати швидко подібні витрати, хоча б приблизним чином, можливо лише в тих країнах де нормативно-визначена процедура дій у випадку витоку такої інформації.

Так, згідно до законодавства США компанія де стався подібний виток зобов'язана повідомити усіх постраждалих. Потім організуються, так звані, call-центри, створюються служби спілкування з інвесторами, ЗМІ, здійснюється службове розслідування тощо. Перераховані заходи потребують значних фінансових затрат.

Компанія «Ponemon Institute» склала приблизний кошторис обрахування частки подібних збитків стосовно втрачених персональних даних:

Дії (заходи) у випадку витоку	**Приблизний кошторис**

персональних даних	
вияв та розслідування витоку (внутрішнє розслідування, послуги консультантів та аудиторів)	11,27 дол. за кожний втрачений запис
повідомлення постраждалих (пошта, телефон, Internet, друковані видання)	25,19 дол. за один запис
спілкування із ЗМІ, інвесторами, судові розгляди, послуги адвокатів, зовнішні і внутрішні call-центри	47,39 дол. на один приватний запис

Одночасно з тим, найбільшу шкоду наносять не ці витрати на встановлення і усунення недоліків, а зниження привабливості торгівельної марки, погіршення репутації та втрата клієнтів, зниження конкурентоспроможності.

Аналітики компанія «InfoWatch» вважають, що зниження конкурентоспроможності становить 25,2%, а втрата клієнтів – 36,9% від втрат комерційних установ пов'язаних із витоком інформації з обмеженим доступом.

Необхідно зважати на ще один важливий аспект для ряду європейських країн, а також США. Наявність чужих імен, прізвищ у сукупності із особливо чутливою інформацією, якою є номер соціального страхування або номер водійського посвідчення, може надати змоги зловмиснику неправомірно отримати кредитну картку. Тому охорона персональних даних у цих країнах потребує особливої уваги.

Колишній співробітник соціальної служби у Лос-Анджелесі зробив визнання щодо неправомірного використання персональних даних майже 200 осіб, з метою отримання соціальних виплат у розмірі близько 2 млн. доларів.

62-х річний працівник відділу соціального забезпечення Лос-Анджелесу Тренг ван Дін у період 1999 – 2010 років займався контролем за соціальними виплатами населенню. Використовуючи персональні дані клієнтів (імена, фінансова інформація, номери соціального страхування) порушник реєстрував несправжні податкові обрахунки у 2009 та 2010 роках. Уся фіктивна звітність знаходилась під його контролем, він же надавав

доручення на здійснення платежів. 197 сфальсифікованих звітів дістали виплату у розмірі 2212996 доларів, з яких зловмисник встиг отримати 667034 долара.

Разом з тим, компанії які самі здійснюють провідні аналітичні дослідження в інформаційній сфері можуть припустити серйозні витоки інформації. За даними видання «Інформаційна безпека» на початку 2011 року офіс компанії «PricewaterhouseCoopers» (PwC) у Чикаго повідомив про виток 77 тисяч персональних даних на державних службовців штату Аляска. Причому повідомлення було здійснено не відразу, а тільки через два місяці після встановлення витоку.

Досить цікаві дані були отримані за результатами опитування «Harris Interactive». За цими показниками кожен п'ятий співробітник організації здійснює крадіжку конфіденційної інформації.

Аналітичний центр компанії «InfoWatch», повідомив, що у грудні 2011 року один з Нью-йоркських банків порушив у суді справу стосовно колишніх працівників банку за крадіжку відомостей, які містили інформацію з обмеженим доступом.

Як зазначалось у позові, четверо колишніх працівників банку, напередодні свого звільнення, скопіювали захищену базу даних. У відомостях окрім комерційної таємниці містились персональні дані (імена, адреси, телефонні номери, адреси електронних скриньок тощо) клієнтів. Звільнення працівників було пов'язано із запрошенням на роботу до іншої фінансової компанії.

За інформацією видання «Los Angeles Times» американський співробітник швейцарського банку «UBS» Бредлі Біркенфельд розголосив способи відкриття банківських рахунків у Швейцарії з можливістю уникнення оподаткування. Тим самим було нанесено суттєвий удар по конфіденційності і репутації швейцарських банків.

У 2010 році компанія «Kroll», яка займається консалтингом в галузі ризиків та електронною безпекою повідомила про суттєве збільшення

протягом року звернень від організацій-клієнтів з проханнями щодо вияву витоків інформації. Річ Планскі, керуючий директор по секретній інформації та розслідуванням зазначав, що почастішали випадки неправомірного розповсюдження інформації ображеними співробітниками установ і організацій у зв'язку з кризою і погіршенням економічного становища та зростанням кількості звільнень.

Витоки інформації з обмеженим доступом із державних структур також мають специфічні особливості. Фахівці виділяють певні особливості неправомірного отримання інформації з обмеженим доступ зацікавленими організаціями від різних державних структур управлінської сфери. З цією метою можуть застосовуватись наступні способи введення до державних структур «своїх чиновників».

Перші, так звані «парашутисти» – це особи, яких зацікавлена компанія умисно влаштовує на роботу у необхідну державну структуру. Як правило, вони продовжують отримувати платню й за попереднім місцем роботи. Такі посадовці надають своїм «утримувачам» необхідну інформацію й намагаються впливати на рішення в їх інтересах. Після закінчення своєї місії «парашутисти» повертаються до свого місця роботи.

Наступні – «вихідці». Після працевлаштування на державну службу продовжують підтримувати тісні контакти - надавати потрібну інформацію своїй «колишній» фірмі. З часом можливий перехід у статус «парашутиста».

«Челноки» – постійно кочують між державною службою й комерційним сектором. Така категорія чиновників розглядає роботу у державних структурах як можливість збільшення свого матеріального достатку, отримання необхідних зв'язків, та доступу до важливої інформації.

Фахівці підкреслюють, що й колишні державні чиновники користуються великим попитом в комерційних структурах. Зокрема їх часто роблять відповідальними за напрям GR (Government relations management). Тобто – за зв'язки з органами державної влади.

Інший великий відсоток неправомірного витоку інформації з обмеженим доступом з різних організацій припадає на технічні канали витоку. До цього, в тому числі, можливо віднести дії хакерів, віруси, апаратні та програмні збої тощо.

Відразу слід згадати подію року – 2010, виток величезного масиву різної інформації з обмеженим доступом до якої були причетні ресурси Wikileaks. Історію цього «популярного» зараз ресурсу прийнято відраховувати з 4 жовтня 2006 року. Та й сучасні збитки, особливо на території України, від дій так званого «вірусу Petya_A» всім відомі.

За технічними каналами витоку йдуть крадіжки обладнання, а також персональних комп'ютерів, яке саме по собі має цінність та може містити інформацію з обмеженим доступом. За підрахунками аналітиків у період 2010 – 2015 років у США, Великобританії та ряду європейських країн кожен четвертий витік інформації з обмеженим доступом був пов'язаний з викраденням комп'ютерної техніки.

Поширення такої причини як виток інформації з обмеженим доступом через викрадення персональних комп'ютерів становить все більшу проблему. Це пов'язано з сучасними особливостями використання персональних комп'ютерів, особливо ноутбуків, мобільної техніки співробітниками компаній.

Дуже часто зникає межа яка розділяє особисте життя співробітника з його корпоративною діяльністю що й стає головною причиною можливого витоку інформації з обмеженим доступом.

Американське аналітичне агентство «InsightExpress» вважає, що близько 80% всіх корпоративних витоків інформації з обмеженим доступом відбувається завдяки наступним основним причинам:

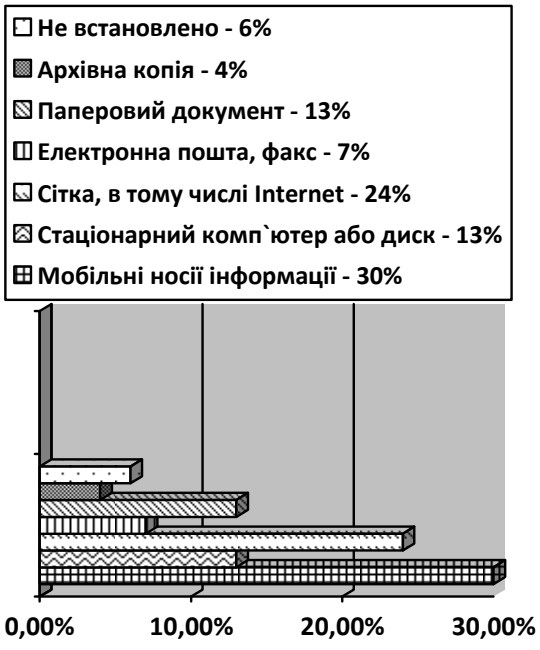
спілкування зі знайомими на предмет професійної інформації;

спільне використання зі знайомими засобів комп'ютерної, мобільної техніки де може знаходитись професійна інформація;

використання офісної техніки для особистих потреб, включаючи доступ до різних ресурсів мережі Internet;

винос офісних носіїв інформації за межі організацій тощо.

Проведені міжнародними аналітичними центрами дослідження дозволяють визначити розподіл випадкового витоку інформації з обмеженим доступом за каналами (носіями) витоку:



Згідно даних порталу інформаційної безпеки «Content Security» ступінь загрози витоку інформації з обмеженим доступом з установ співвідноситься наступним чином:

розголошення – 32%;

несанкціонований доступ шляхом підкупу або схилення працівника конкурентами – 24%;

відсутність в організації необхідного контролю та жорстких умов забезпечення збереження інформації – 14%;

традиційний обмін виробничим досвідом – 12%;

безконтрольне використання інформаційних систем – 10%;

наявність передумов виникнення серед співробітників конфліктних ситуацій, пов’язаних з відсутністю виробничої дисципліни, психологічною

невідповідністю, випадковим підбором кадрів, відсутністю роботи щодо єднання колективу – 8%.

Окремо слід виділити виток інформації за невстановленими причинами. Кількість таких випадків досить значна.

У 2009 році компанія «GS Caltex» одна з най великих постачальників нафти у Південній Кореї оголосила про величезний виток інформації. У сміттєвих баках поблизу караоке-бара в районі Гангем (Gangnam) було знайдено два оптичних диска, які містили персональні дані 12 млн. чоловік. Витік інформації, в тому числі, завдав шкоди високопоставленим корейським чиновникам і навіть зіркам корейського шоу-бізнесу.

Компанія «InfoWatch» провела статистичне дослідження за три попередні роки стосовно співвідношення видів витоку інформації, узагальнені результати наведемо в таблиці:

Вид витоку інформації	**2009 рік**		**2010 рік**		**2011 рік**	
	Кількість	%	Кількість	%	Кількість	%
Умисний виток	154	29	241	45,5	375	51
Випадковий виток	376	71	223	42,1	320	43,5
Не встановлено	дані відсутні	дані відсутні	66	12,5	40	5,4

За результатами проаналізованих витоків інформації з обмеженим доступом, які були навмисно або не навмисно здійснені співробітниками організацій виділені наступні відомості, що більш за все становлять предмет зацікавленості:

документи, які характеризують фінансовий стан та плани організації, в тому числі, фінансові звіти, різна бухгалтерська документація, бізнес-плани, договори тощо;

персональні дані працівників та клієнтів організації;

технологічні та конструктивні розробки («ноу-хау») організації;

внутрішні документи, службові записки, записи нарад, презентації «тільки для співробітників» організації тощо;

технічні відомості, які дозволять здійснювати несанкціонований доступ до мереж організації, відомості стосовно реалізації засобів захисту інформації.

Аналітичний центр «InfoWatch», на початку 2013 року, зареєстрував виток комерційної таємниці з «Apple», яка може коштувати компанії близько 2,3 млн. дол. Колишній менеджер «Apple» Пол Девайн визнав у суді, що протягом трьох років передавав інформацію з обмеженим доступом зацікавленим особам у Сінгапурі. Відомості містили прогнози продажів, цінові орієнтири та неопубліковані технічні характеристики продуктів. Як вважають аналітики «InfoWatch» несанкціоноване використання подібної інформації може надати суттєвої переваги конкурентам «Apple» при укладанні угод за більш вигідними умовами.

Слід зазначити, що останнім часом у ЗМІ, на перший погляд, з'являється значна кількість інформації про факти несанкціонованого витоку інформації з обмеженим доступом. Разом з тим, якщо враховувати відомості «SECURIT Analytics» в дійсності у ЗМІ фігурує лише невеличка кількість подібних інцидентів. Згідно із підрахунками «SECURIT Analytics» це становить у кращому випадку 0,1% від реальної кількості витоків інформації з обмеженим доступом.

Серед причин цього можливо визначити – невідповідність законодавства. Тільки окремі країни вимагають від установ оприлюднення факту витоку інформації відразу після встановлення такої події.

Крім того, досить часто, недосконалі заходи захисту інформації не дозволяють тривалий час взагалі виявити виток інформації, який відбувся.

Відповідно до результатів дослідження компанії «PricewaterhouseCoopers» (PwC), 40% організацій навіть не знають

справжньої кількості інцидентів стосовно витоків їх інформації з обмеженим доступом за минулий рік.

Повертаючись до нагальних потреб пов'язаних із захистом інформації з обмеженим доступом, необхідно зазначити, що прийняття відповідних нормативно-правових актів, які повинні унормувати поводження з різними категоріями інформації з обмеженим доступом є важливою запорукою щодо зменшення таких витоків у цілому.

Потрібно зважати й на необхідність чіткого визначення відповідальності за сам факт витоку інформації з обмеженим доступом навіть у тому випадку, коли були виконані вимоги відповідних інструкцій із захисту інформації. Це, в свою чергу, повинно сприяти та стимулювати постійний розвиток та функціональність системи режимних заходів, які повинні запроваджуватись з метою захисту інформації з обмеженим доступом та враховувати новітні загрози.

Доцільно враховувати досвід інших країн світу стосовно широкого проведення загально просвітницької роботи в суспільстві з приводу важливості й особливостей захисту інформації з обмеженим доступом.

Зокрема, в Канаді 28 січня визнано днем захисту даних. Останніми роками канадська асоціація адміністраторів з професійного доступу до персональної інформації (CAPAPA), яка є провідною асоціацією в Канаді у січні місяці проводить огляд усіх заходів, пов'язаних з охороною персональних даних в Канаді.

Заходи відбуваються у головних центрах країни: Ванкувері, Вікторії, Галіфаксі, Оттаві, Торонто, Едмонтоні за підтримкою федеральних та місцевих спеціально уповноважених із захисту інформації державних установ та організацій приватного сектору.

За висновком голови канадської національної асоціації Шарон Польскі, такі заходи необхідні для висвітлення питань щодо прав громадян у інформаційній сфері, особливостей реалізації заходів спрямованих на захист персональних даних та отриманні додаткової інформації.

4.2. Особливості кадрового забезпечення підрозділів захисту інформації з обмеженим доступом в установах

Діяльність підрозділів захисту інформації в різних установах спрямована на вирішення значної низки завдань, пов'язаних із збереженням інформації з обмеженим доступом. Уразливість даної категорії інформації передбачає розробку та застосування ряду відповідних режимних заходів під час здійснення всіх видів інформаційної діяльності установи. При цьому аналітиками визнається, що людський чинник є найголовнішим у організації роботи підрозділів захисту інформації. Саме через не врахування цього фактору досить часто трапляється значна кількість витоків інформації з обмеженим доступом. Звідти актуальними завжди є питання щодо швидкого та якісного підбору співробітників для таких структурних підрозділів в різних установах.

В дійсний час у нашій державі підготовку фахівців з питань інформаційної безпеки здійснює певна кількість навчальних закладів. Подальше працевлаштуванням окремих таких випускників, а також фахівців, які вже мають досвід практичної роботи у сфері захисту інформації останнім часом все більше забезпечується так званими спеціалізованими кадровими агентствами. При цьому, якщо в нашій державі даний напрям працевлаштування ще розвивається, ряд провідних країн світу вже впевнено забезпечує його реалізацію у міжнародних масштабах.

Перші приватні агентства з найму з'являються в Європі ще на початку XIX столітті, а саме, на території Німеччини. Трохи пізніше подібні заклади створюються в Англії та Франції. Вже в середині XIX століття у 1848 році, до цієї діяльності приєднується США. У Бостоні організовується «біржа зайнятості».

Подальший розвиток суспільних відносин, економічне зростання держав, поява складних державних й недержавних організаційних структур необхідність захисту різних категорій інформації з обмеженим доступом призводять до вироблення уніфікованих підходів до кадрового питання.

Сучасний пошук кваліфікованих фахівців, в тому числі для підрозділів захисту інформації, містить елементи маркетингового аналізу та часто використовує підходи, що раніше були прерогативою спецслужб.

Зростання кількості різноманітних кадрових агентств дозволяє говорити про появу нової галузі економіки, яка розвивається великими темпами.

В обігу з'являється нове слово «рекрутинг» або «рекрутмент» похідне від французького «recruit» («рекрутувати») тобто набирати кого-небудь на роботу або наймати на службу. В XVII столітті на території Франції цей захід активно використовувався з метою поповнення збройних сил.

Сучасні найбільш відомі в світі «рекрутингові» структури розташовані на території США, Великобританії, Канади, Австралії, Швейцарії.

Багато з цих кампаній мають вже досить великий «послужний список». Варто згадати «Egon Zehnder», «Ward Howell» які почали свою діяльність у 1951 році, «Heidrick & Struggles», засновану в 1953 році, «MRI», яка працює з 1965 року, «Korn/Ferry» – з 1969 року, «Amrop», «Morgan Hunt» – з 1986 року тощо.

Вітчизняний «кадровий сленг» поповнюється й іншими закордонними «ноу-хау». Все частіше застосовується поняття «аутсорсинг» (англ. Outsourcing, out - зовнішнє, source - джерело).

Виділяють три основні види аутсорсинга, які коротко можливо визначити наступним чином:

«IT – аутсорсинг» - полягає в передаванні та обслуговуванні спеціалізованим агентствам (ректуринговій кампанії) інформаційних систем, що може включати: технічну підтримку; обслуговування корпоративної поштової системи, web-сервера та сайту; захист інформації; адміністрування комп'ютерних систем; розробка, впровадження та обслуговування корпоративних програмних продуктів й т.п.;

«виробничий аутсорсинг» - реалізується шляхом передавання у зовнішнє керівництво спеціалізованому агентству (ректуринговій кампанії) частини або усього виробничого циклу;

«аутсорсинг бізнес-процесів» - передавання спеціалізованому агентству (ректуринговій кампанії) функцій структурних підрозділів організації замовника, що не є головними для даної організації. Це може бути: реклама, управління персоналом, транспорт, прибирання офісу, охорона і т.п.

До переваг аутсорсингових кампаній відносять можливість установі-замовнику використовувати сторонній висококваліфікований досвід, який був накопичений при вирішенні аналогічних проблем. Зважаючи на свою спеціалізацію подібні світові кампанії здійснюють інвестиції саме в цю галузь, отримуючи відповідні нові знання, підвищуючи рівень кваліфікації задіяного персоналу та впроваджуючи новітні технічні досягнення.

Згідно даних окремих інформаційних агентств, сукупний обсяг світового ринку «аутсорсингу» можливо співвіднести з обсягами ринків автомобілебудування, електроніки та фармацевтики.

Одним з напрямів «аутсорсингу бізнес-процесів» є, так званий, «кадровий аутсорсинг», що передбачає фактично передавання функцій кадрового відділу установи іншому агентству, яке спеціалізується виключно на вирішенні кадрових питань. «Кадровий аутсорсинг» може включати підбір кадрів, роботу з документацією й юридичне супроводження даного процесу.

До переліку кадрових послуг відноситься: підбір й адоптація персоналу; з'ясування необхідності організації навчання; оптимізація організаційної структури до якої підбирається персонал; впорядкування системи оплати персоналу та забезпечення компенсаційних виплат за особливі умови праці; проведення аналітичних досліджень спрямованих на виявлення ефективності діяльності персоналу й з'ясування морального клімату в колективі.

Робота з документацією включає: ведення усієї кадрової документації; розробка штатного розкладу, посадових інструкцій, й інструкцій з інших питань; організацію управлінсько-розпорядчого діловодства, створення розпорядчих документів за усіма напрямами діяльності установи чи організації тощо.

Останніми роками в Україні все більше з'являється подібних кадрово-пошукових структур. З метою підбору кадрів рекрутингові агентства створюють власні бази даних. Наприклад, рекламуючи свою діяльність київська консалтингова компанія, ООО «НАВИГАТОР» зазначала, що нею створена унікальна база даних, яка включає інформацію стосовно 35000 різних фахівців.

Агентство «Recruit Alliance» засноване у 2000 році наголошувало, що під час реалізації своєї діяльності використовує базу кандидатів, яка нараховує 250000 тисяч фахівців, більшість з яких не користуються Internet ресурсами щодо пошуку роботи з міркувань конфіденційності.

З 2008 року агентство «Capital Human Resources» (CHR) здійснювала програму підбору молодих фахівців та студентів. З цією метою у ряді ВНЗ Києва були відкриті представництва CHR, які реєстрували найбільш талановитих студентів з перспективою подальшого працевлаштування. За даними агентства була сформована база, яка вміщувала понад 5000 подібних кандидатів.

Існують вузькопрофільні агентства, які спеціалізуються на окремій галузі й, відповідно, підбір фахівців здійснюється виключно за певною спрямованістю.

Переважно, оптимальний термін підбору кандидата кадровим агентством знаходиться в межах 2 – 6 тижнів, у залежності від складності пошуку. Більш великий час пошуку потрібен для підбору «ексклюзивних фахівців».

Інтернет видання Recruiting.net.ua в березні 2011 року повідомило результати 10 конкурсу читачів «Kyiv Post» щодо кращого «рекрутингового

агентства» «Best of Kyiv». Ним стало «Hudson Global Resources», яке обійшло минулорічного переможця «Brain Source International».

Чинний переможець займається постійним «рекрутингом» іноземних та українських менеджерів середньої та вищої ланки для роботи в різних галузях, що включає банківську справу, фінансові та професійні послуги, інженерну галузь, будівництво, нерухомість, інформаційні технології та телекомунікації, енергетику, авто, фармацевтику, охорону здоров'я, продовольчі продажі. Як підкреслювали представники «Hudson Global Resources», переваги компанії полягають у її «глибокій спеціалізації». На кожну із галузей спеціалізації працює окрема команда фахівців-консультантів.

Навіщо потрібна та чим вигідна аутсорсинговим агентствам спеціалізація? На це питання можливо дати, принаймні дві відповіді. По-перше, «глибока» або «вузька» спеціалізація в певній галузі такого агентства повинна сприяти забезпеченню надійного та якісного виконання ним своїх обов'язків. По-друге, виконання споріднених та однотипних операцій для більшості клієнтів, при спеціалізації агентства, призводить до зменшення вартості послуг у цілому.

Оплата послуг агентствам з пошуку персоналу провадиться на підставі укладеної угоди між ним та зацікавленій у фахівцях організації чи установі, яка виступає в ролі замовника. При цьому в угоді може бути обумовлено, що оплата буде здійснена тільки у випадку успішного підбору необхідних фахівців.

Також, доцільно передбачити підбір декількох оптимальних кандидатів, які не тільки відповідають необхідним вимогам, але й мають високу мотивацію стосовно працевлаштування саме в організації замовника та здатних швидко увійти до її корпоративного середовища. До угоди, при необхідності, можливо включити супроводження кадровою компанією кандидата на період випробувального терміну, а також гарантія безкоштовної

заміни іншим кандидатом впродовж цього терміну. Випробувальний термін, в середньому, встановлюється в межах 60 – 180 днів.

«Супроводження» кандидата необхідно для його швидкої адаптації на новому місці роботи. Для реалізації цього, на практиці в тому або іншому обсязі, вирішують наступні завдання:

надання новачку первинної інформації про установу (історія установи, напрями діяльності, основні завдання, розклад робочого дня; певні відомості про безпосередніх керівників тощо);

інформування про специфічні особливості діяльності установи;

реалізація наочних прикладів вирішення функціональних завдань;

сприянні створенню належного морального клімату в колективі з метою зменшення відчуження новачка.

Що стосується розміру виплат кадровим агентствам за підбір кандидата, сума часто співвідноситься із певним відсотком річної заробітної плати підібраного фахівця. Як правило, в межах 14 – 25%. При цьому, в переважній більшості вартість послуг не є фіксованою й встановлюється ринковим шляхом у ході переговорів із замовником.

Під час визначення вартості роботи кадрового агентства враховується:

терміновість замовлення;

складність поставлених завдань та вимоги до кандидатів, обмеження у пошуку, привабливість установи-замовника та роботи, яка пропонується, розміри оплати праці кандидата;

способи пошуку, які можуть бути ефективними відповідно до даного замовлення;

обсяг та успішність попереднього досвіду роботи з даним замовником;

неординарність замовлення та етапність оплати;

кількість та виняткова наявність подібних фахівців на ринку праці.

Подібні агентства реалізують пошук фахівців, в тому числі, спрямованих на роботу пов’язану із забезпеченням збереження інформації з обмеженим доступом. Підбір здійснюється починаючі від співробітників

служб фізичної охорони режимних об'єктів, діловодів, які забезпечують ведення документації, що містить інформацію з обмеженим доступом, фахівців з питань технічного захисту інформації й закінчуючи керівниками різного рівня для даних підрозділів.

Для реалізації пошукових запитів агентства можуть застосовувати різні способи. В практиці роботи міжнародних кадрових служб, що використовують й українські агентства виділяють чотири основних напрями пошуку:

прямий пошук керівників для достатньо відповідальних посад – «Executive search»;

безпосередній пошук конкретних, кращих фахівців («охота за головами») – «Head hunting»;

підбір адміністративних працівників середньої управлінської ланки – «Management Recruitment»;

загальний або регіональний пошук придатних кандидатів – «Regional Recruitment».

Кожен з цих напрямів має свою історію та особливості формування. Згадаємо тільки окремі з них. Найбільш складним пошуком кандидатів для заміщення вакантних посад вважаються прямий пошук керівників для достатньо відповідальних посад («Executive search») та безпосередній пошук конкретних кращих фахівців («охота за головами» («Head hunting»)).

У США ці заходи набули найбільшої актуальності напередодні другої світової війни. Реалізацію цих заходів додали до своєї діяльності ряд великих консалтингових компаній, зокрема «Deloitte & Touch», «Ernst & Young».

Згодом у 1946 році в Нью-Йорку відкривається компанія «Boyden», яка почала підбір кандидатів для достатньо відповідальних посад. Через два роки засновується «Manpower», на теперішній час це одна з найкрупніших компаній світу з підбору кадрів. Її близько 3500 офісів розташовані в майже 60 країнах світу, а кількість клієнтів перевищує 400 тисяч.

Слід додати, що пошуки за напрямами «Executive search» й «Head hunting» завжди вважались найбільш витратними. Для пошуку подібних фахівців, зрозуміло, не використовується звичайна реклама та об'яви. В хід йдуть усі можливі «секретні способи» для отримання «коштовного кандидата».

За визначенням аналітиків, у США та Європі початкова ціна для пошуку подібних кандидатів починається з 50000 доларів.

Свої особливості щодо підбору кандидатів існують й на вітчизняному ринку праці, проте враховано й багато запозичень із багаторічного світового досвіду.

Київська консалтингова компанія, ООО «НАВИГАТОР», яка булла заснована в червні 1999 року використовувала наступні методи оцінки та відбору кандидатів:

попередній аналіз документів та резюме;

телефонна співбесіда;

ретельна особиста співбесіда за технологіями структурованого, проективного або CASE-інтерв'ю, оцінка відповідності вимогам замовника, вияв мотивації або лояльності кандидата;

збір та оцінка відзивів та рекомендацій;

психодіагностика та/або тестування кандидатів за необхідністю;

порівняльний аналіз усієї інформації та відбір остаточних кандидатів з використанням методики СВА (відбір за компетенцією);

організація зустрічі кандидатів із замовником.

Інше рекрутингове агентство «Recruit Alliance» під час підбору фахівців застосовувало:

прямий та дистанційний пошук;

можливості регіональних представництв;

внутрішню базу кандидатів;

співробітництво з професійними спілками;

напрацьовані контакти з фахівцями у різних галузях;

розміщення вакансій в Internet та ЗМІ.

В травні 2004 року була утворена Асоціація регіональних кадрових агентств України (АРКА) – Всеукраїнська професійна спілка провідних агентств із підбору персоналу.

Серед її основних цілей та завдань було визначено:

розвиток ефективної, надвеликої в країні, розгалуженої структури рекрутингових агентств;

формування цивілізованого ринку кадрових послуг в Україні;

сприяння розвитку бізнесу своїх клієнтів у регіони;

надання підприємствам-замовникам послуг нового формату: комплексний підбір персоналу у всіх регіонах України з урахуванням специфіки місцевих ринків праці;

сприяння міжнародній ротації фахівців;

обмін досвідом, інформацією та технологіями;

розробка та підтримання єдиних професійних та етичних стандартів;

підвищення кваліфікації співробітників агентств учасників АРКА;

взаємодія з державними та галузевими міжнародними організаціями.

Безпосередня організація пошуку кандидатів на заміщення вакантних посад в підрозділі захисту інформації з обмеженим доступом, в тому числі, з використанням можливостей кадрових агентств, повинна включати розробку формалізованих вимог до працівників, які підбираються.

Наприклад, для працівників державник установ розробляються довідники кваліфікаційних характеристик професій. Які періодично оновлюються та доповнюються з урахуванням різних чинників.

На підприємствах і установах не державної форми власності формалізовані вимоги до посад підрозділів захисту інформації з обмеженим доступом, як правило, готуються так званою службою персоналу (відділ кадрів) спільно з керівником зацікавленого підрозділу.

Співпраця кадрового органу з безпосереднім керівником, де знаходиться вакантна посада дає змогу врахувати й оформити загальні

вимоги до посади й співвіднести їх з специфічними особливостями притаманними тій ділянці роботи, яку буде виконувати підібраний кандидат.

Забезпечення такої співпраці може бути досягнуто шляхом подачі, зокрема, керівником підрозділу захисту інформації відповідної заявки на вакантну досаду до служби персоналу (відділу кадрів) установи.

Оптимальна заявка повинна містити назву вакантної посади й структурного підрозділу, рівень підпорядкованості посади, вимоги до кандидата, в тому числі специфічні, зважаючи на необхідність забезпечення або дотримання режимних вимог при використанні інформації з обмеженим доступом. Важним в запиті є акцентування на отриманні від майбутнього кандидата характеристик та рекомендацій з попередніх місць роботи.

Крім переваг використання послуг різних кадрових агентств необхідно враховувати й ряд загальних аспектів, які в подальшому можуть негативно вплинути на діяльність організації замовника чи створити їй певні проблеми. Особливо це стосується тих моментів де задіяна інформація з обмеженим доступом.

Незважаючи на те, що аутсорсингові компанії повинні гарантувати збереження довіреної їм інформації з обмеженим доступом, й нести за це належну відповідальність, зрозуміло, що загроза витоку вразливої інформації існує. За інформацією Інтернет видання Recruiting.net.ua, в кінці 2010 року один з великих міжнародних рекрутингових порталів, що займається працевлаштуванням кадрів у фінансовій сфері eFinancialCareers.com, повідомив про несанкціонований виток приватних даних своїх клієнтів.

Також, вартість послуг кадрових компаній досить висока й, іноді суттєво перевищує витрати організації у порівнянні з витратами на власну кадрову службу.

Не можна забувати й про те, що така кадрова компанія потенційно може збанкротувати Далі, поява додаткових проблем з пошуку іншої аутсорсингової компанії та передачі їй всіх справ з урахуванням збереження інформації з обмеженим доступом.

Якщо установа планує встановлювати серйозні та довгострокові стосунки з аутсорсинговим агентством доцільно враховувати його імідж та репутацію на ринку праці. Непогано отримати та проаналізувати певну первинну інформацію. Зокрема, чи не відбувався витік інформації з обмеженим доступом за участю агентства, можливі відгуки про його діяльність а також ресурсну базу (моніторинг різних ЗМІ, Internet- ресурси. відгуки установ, що скористались послугами даного агентство, та кандидатів, які були працевлаштовані).

Проведений аналіз діяльності різних спеціалізованих кадрових структур щодо підбору фахівців для підрозділів захисту інформації з обмеженим доступом дозволяє виявити загальні тенденції спрямовані на вирішення проблеми так званого «людського чинника». В основі підбору зазначених фахівців лежить врахування індивідуальних, професійних, соціально-психологічних, психофізіологічних якостей кандидата на роботу в підрозділи захисту інформації з обмеженим доступом.

Зокрема, ефективність професійної діяльності в сфері охорони інформації з обмеженим доступом значною мірою зумовлена ступенем засвоєння спеціальних теоретичних знань, рівнем розвитку професійно важливих умінь.

Крім того, підґрунтям для пошуку кандидатів для підрозділів захисту інформації з обмеженим доступом є врахування вимог, які висуваються до конкретної посади.

Подальшою важливою складовою щодо реалізації потенціалу підібраного фахівця стає забезпечення необхідних умов для його швидкої адаптації на певному підприємстві в межах своїх посадових обов’язків.

4.3. Використання заходів моніторингу у сфері захисту інформації з обмеженим доступом

Потреба у здійсненні охорони важливих інформаційних ресурсів не викликає жодних сумнівів. У реалізації заходів захисту різних видів

інформації з обмеженим доступом зацікавлені й задіяні як державні органи, так і фізичні й юридичні особи. Для забезпечення охорони інформаційних ресурсів використовуються певні напрацьовані комплекси заходів.

Не даремно провідні країни світу вкладають значну кількість коштів на створення достатньо ефективних систем щодо захисту важливої інформації, оскільки її неправомірне використання завдасть набагато більше збитків. За інформацією міжнародних видань фірми США витрачають до 20% від загального доходу тільки на захист від інформаційного шпигунства.

Зважаючи на існування постійних загроз в інформаційній сфері актуальними завжди стають заходи спрямовані не тільки на пасивну охорону інформації з обмеженим доступом (виконання стандартних, давно встановлених режимних заходів) але й заходи покликані попередити саму можливість неправомірного витоку даної інформації (запобіжні дії з врахуванням новітніх загроз).

Попередження витоку інформації з обмеженим доступом, врахування можливих загроз її існуванню найбільш складна проблема організації надійного захисту. Провідна роль для вирішення цієї проблеми безперечно належить правильно застосованому аналітичному інструментарію. Підтвердженням цього є визначення В.Афанасьєвим головної мети інформаційного забезпечення, яке полягає в тому, щоб на основі первинних даних отримати вторинну, опрацьовану інформацію, яка становить підґрунтя для прийняття рішення. Кінцевий результат аналітичної роботи лежить в основі прийнятих управлінських рішень власників інформації з обмеженим доступом або суб'єктів, що відповідають за збереження такої інформації.

На теперішній час в різних сферах суспільної діяльності все активніше застосовуються можливості моніторингу, який включає цілу систему спостережень та аналітичної обробки отриманих показників. Саме за результатами проведеного моніторингу приймаються виважені управлінські рішення.

Дійсно використання моніторингу в різних сферах діяльності безперечно надає цілий ряд переваг. Але перш ніж розглянути можливість використання моніторингу стосовно сфери захисту інформації з обмеженим доступом доцільно згадати, що ж розуміється під загальним поняттям моніторинг.

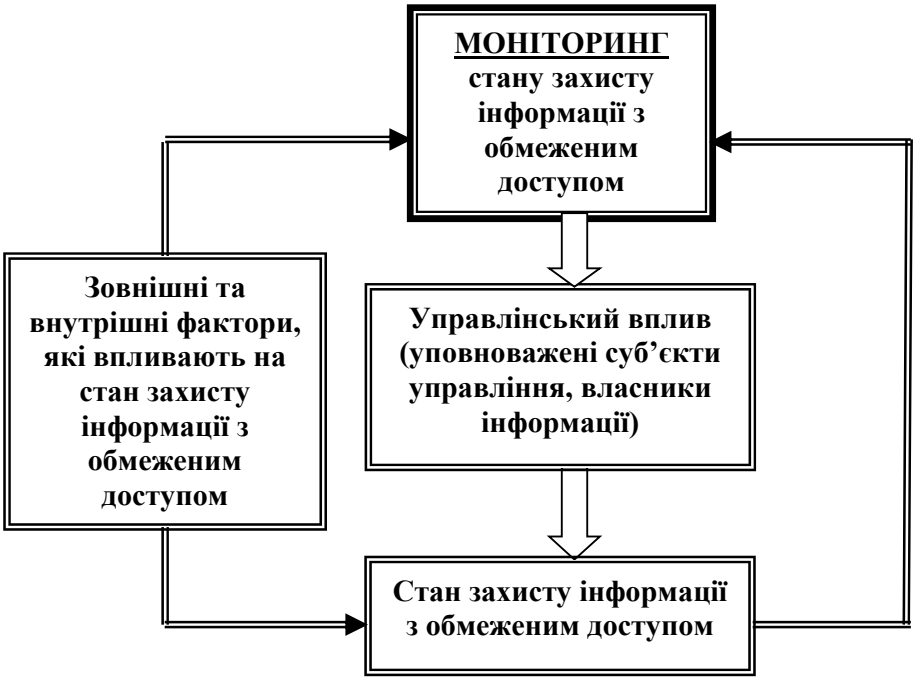
Моніторинг походить від англійського Monitoring – контроль, та від латинського Monitor – той, хто попереджає, застерігає, радник, консультант. Юридична енциклопедія тлумачить моніторинг як « ... регулярне спостереження за станом природних технічних і соціальних процесів з метою їх оцінки, контролю та прогнозування. Порядок проведення моніторингу регулюється відповідними правилами. Інформація, отримана за допомогою моніторингу, кладеться в основу рішень, що приймаються державними органами, політичними партіями, громадськими організаціями тощо».

Разом з тим, в дійсний час спостерігається дещо спрощене розуміння можливостей проведення моніторингу. На думку ряду науковців поняття «моніторинг», почало широко вживатися останнім часом як синонім системного контролю за процесами і явищами, що відбуваються у світі, окремому регіоні чи державі, сфері або галузі суспільного життя, науки тощо, а також як вид діяльності, яка вивчає, аналізує та прогнозує суспільні явища.

Дослідження факторів, які впливають на стан, захисту інформації з обмеженим доступом в цілому, невід’ємно пов'язано з процесом пізнання їх сутності та змісту, а також з прогнозуванням можливих результатів розвитку несприятливих умов, що по суті являє собою справжній моніторинг.

Так, організація режимних заходів, наприклад, щодо охорони комерційної таємниці залежить від врахування цілого комплексу факторів, зокрема: які відомості відносяться до комерційної таємниці; змісту завдань, покладених на установу; специфіка її діяльності; наявні сили та засоби за допомогою яких здійснюється захист.

Окрім зазначеного, існує ще значна кількість чинників, що потребують врахування: розвідувальна діяльність конкурентів; несанкціоновані дії співробітників власної організації; непродумана політика установи в галузі безпеки тощо (що захищати? від кого? коли? як?). Умовно визначення ролі моніторингу в системі захисту інформації з обмеженим доступом можливо наочно представити наступним чином:



З урахуванням визначеного місця моніторингу в системі захисту інформації з обмеженим доступом, можливо сформулювати основні його завдання:

забезпечення постійного інформаційного відстеження стану та розвитку факторів, які впливають на стан захисту інформації з обмеженим доступом;

вияв та обґрунтування характеру проблем, які виникають в процесі розвитку цих факторів;

постановка та вибір реальних і значимих цілей та напрямків діяльності суб'єктів, які діють у сфері захисту інформації з обмеженим доступом.

Результатом здійснення моніторингу стану захисту інформації з обмеженим доступом є інформація, яка може бути представлена в залежності від її обробки:

первинна інформація (дані спостережень), яку одержують повноважені суб'єкти внаслідок спостережень;

узагальнені дані, що стосуються певного інтервалу часу;

комплексні показники, одержані внаслідок узагальнення за певними параметрами;

оцінки стану захисту інформації з обмеженим доступом та джерел негативного впливу на неї;

прогнози стану захисту інформації з обмеженим доступом на певний період;

науково обґрунтовані рекомендації, необхідні для прийняття рішень уповноваженими суб'єктами управління чи власниками інформації.

Крім того, моніторинг стану захисту інформації з обмеженим доступом, для об'єктивного зображення суті та коректної діагностики цього стану повинен відповідати, як мінімум, двом принциповим вимогам, бути:

- системним, тобто незалежно від змісту та масштабу моніторинг повинен дати всебічну характеристику аспектів проблем, які розглядаються у їх взаємозв'язку (це має особливо важливе значення на стадії аналізу та діагностики);

- структурно повним та логічно завершеним**,** це передбачає, що незалежно від змісту та масштабу моніторинг повинен містити загальнообов'язкові стадії збору тільки певної інформації, її аналіз та оцінку (діагностику) проблеми.

З урахуванням результатів моніторингу стану захисту інформації з обмеженим доступом повинна формуватись організаційна структура служб безпеки підприємств, чи інших уповноважених суб'єктів, здійснюватись управління їх діяльністю, вноситись корективи в розстановку сил, в форми та методи їх використання та взаємодії.

Для того, щоб результати моніторингу були правильними та обґрунтованими, а також слугували надійним джерелом інформації, необхідної для здійснення діяльності уповноважених суб'єктів, він повинен бути оптимально організований. При цьому велике значення має дотримання загально методологічних принципів пізнання та управління, зокрема: об'єктивність; науковість; всебічність; безперервність тощо.

Результати подібного моніторингу повинні лежати в основі інформаційного забезпечення управлінської діяльності уповноважених суб'єктів, які діють у сфері захисту інформації з обмеженим доступом. Врахування потребує те, що без інформації та аналізу управління прийме вольовий характер і виконання його функцій буде базуватись на суб'єктивних факторах.

Основу для проведення сучасного моніторингу повинна становити різна інформація в тому числі статистична. Оскільки узагальнені дані відносно кількісних та якісних характеристик певних явищ, в тому числі в сфері обігу інформації з обмеженим доступом неможливо всебічно проаналізувати без використання статистичної інформації.

В свою чергу використання статистичної інформації пов'язано із застосуванням статистичних методів та методик їх обробки.

Слід зазначити, що статистичні показники, за допомогою яких досліджуються визначені фактори, повинні відображатися не тільки у вигляді обліково-оціночних показників – тобто числових значень які визначають обсяги розповсюдження, чи рівні розвитку певних процесів і можуть бути виражені сукупністю числових значень та (або) інтегральним значенням а й у вигляді аналітичних показників, що допомагають аналізувати статистичну інформацію і характеризують якісні особливості розвитку та стану процесів, що досліджуються. При цьому якісні оцінки показників («норма», «краще», «гірше» тощо) передбачають наявність стійких уявлень щодо еталону, порівняння з яким дозволяє визначити ступінь наближення або відхилення від еталону.

Проте, як показує практика, отримання максимальної аналітичної обробки значної кількості цифрових показників можливо за умов застосування різних математичних методів які представлені у прикладній статистиці та дозволяють максимально обробити для використання отримані дані. Зрозуміло, що такі методи можливо і необхідно використовувати щодо статистичних даних у сфері обігу інформації з обмеженим доступом.

Очевидно, що уповноважені суб'єкти, які використовують статистичну інформацію для прийняття управлінських рішень у межах своєї компетенції, потребують саме результатів спеціальної обробки інформації – аналізу та оцінювання. Дослідження впровадження моніторингів в інших сферах дає змогу визначити можливу загальну структурну побудову для сфери захисту інформації з обмеженим доступом:

Кожний з представлених компонентів загальної структурної побудови моніторингу має свої особливості реалізації.

Збір інформації – полягає у необхідності збору інформації, яка необхідна для функціонування уповноважених суб'єктів управління, що можливо здійснити з врахуванням пріоритетів діяльності установи пов'язаної із захистом інформації з обмеженим доступом. Дана складова моніторингу включає три етапи: отримання інформації; первинна оцінка інформації; передача інформації до інформаційної бази. Збір інформації може відбуватись з врахуванням основних каналів можливого неправомірного витоку інформації з обмеженим доступом.

Наприклад, в сфері охорони комерційної таємниці доцільно проводити збір інформації з врахуванням спрямованості діяльності організації, що може включати аналіз: друкованих публікацій та Internet видань; виставкових центрів й рекламних оголошень; виступи на конференціях і симпозіумах тощо. Інший напрям може стосуватись збору відомостей про: діяльність фірм-партнерів та конкурентів; ходу виконання науково-дослідних або інших робіт тощо.

Важливим моментом при зборі інформації є й інші способи її отримання. Іноземні компанія використовують досить великий арсенал таких заходів, до яких може бути віднесено: візуальне спостереження; ознайомлення з документами та виробами (легальне придбання або крадіжка); підслуховування; нагляд з використанням технічних засобів; опитування і т.п.

Комплектування інформаційної бази – полягає у систематизації отриманої інформації в певну інформаційну систему, що в свою чергу характеризується відповідним оцінюванням наявної інформації на предмет важливості, достатності, об'єктивності тощо.

З врахуванням того, що можливо використання різних видів інформації з обмеженим доступом, важливою умовою стає забезпечення необхідних режимних вимог та швидкості у пошуку необхідної інформації, що передбачає:

закріплення регламенту проведення робіт з інформаційною базою;

визначення порядку введення інформації до інформаційної бази;

забезпечення контролю за цілісністю інформаційної бази;

забезпечення розмежування доступу до інформаційної бази користувачів;

своєчасне повідомлення користувачів, які встановили обмеження доступу до інформації, про звернення до неї інших користувачів;

здійснення аналізу потоку запитів і стану інформаційного фонду;

підготовка рекомендацій щодо корекції інформаційної бази тощо.

До загальних засад комплектування інформаційної бази можливо віднести: безперервність та системність комплектування; достатність ресурсів; інформаційна, технологічна та технічна сумісність інформаційних систем, які будуть використовуватись; відповідності інформації, що накопичується в інформаційній базі до компетенції користувачів;

Одне з проблемних питань комплектування інформаційної бази, в сучасних умовах, може бути пов'язане з тенденцією до зростання обсягів інформації. Тому, порядок забезпечення комплектування інформаційної бази повинен постійно вдосконалюватись через пошук та впровадження нових форм, методів і засобів її здійснення.

Задоволення потреб суб'єктів управління – полягає у правильному виконанні запитів уповноважених суб'єктів управління відповідно до їх компетенції. В залежності від характеру обробки інформації можливо розрізняти наступні варіанти вирішення вказаної задачі: видача різних аналітичних довідок; підготовка статистичних відомостей; підготовка оглядів за результатами обробки статистичної інформації з використанням методів прикладної статистики тощо.

Визначення показників і режимів спостережень – полягає у визначенні необхідної та достатньої кількості показників, для проведення моніторингу стану захисту інформації з обмеженим доступом.

Режими спостережень характеризують повноту охоплення моніторингом необхідного обсягу, при цьому доцільно розрізняти:

загальні спостереження – завданнями яких є проведення спостережень за широким колом показників;

проблемно-орієнтовані спостереження завданнями яких є проведення спостережень за певними проблемами у сфері охорони інформації з обмеженим доступом. Подібні спостереження можуть проводитись, наприклад, за організацією спеціального діловодства, яке включає низку заходів (облік, зберігання, використання, знищення, транспортування, ознайомлення тощо) щодо поводження з документальними матеріалами, які містять інформацію з обмеженим доступом.

Визначення регламентів збору, обробки та використання інформації – реалізація цього елемента полягає у визначенні термінів, тобто нормуванні – проведення збору, обробки та використання інформації щодо захисту інформації з обмеженим доступом (наприклад, річне, квартальне, щомісячне отримання інформації).

Нормативно-правове забезпечення – потребує закріплення основних правових положень моніторингу стану захисту інформації з обмеженим доступом, а також напрямів за якими буде провадитись цей моніторинг. Нормативного закріплення основних заходів, форм, методів та принципів реалізації спостережень за станом захисту інформації з обмеженим доступом з метою моніторингу.

Науково-методичне забезпечення – передбачає залучення наукових кадрів або відповідних установ з метою підвищення ефективності моніторингу в цілому або за певними складовими. Результатом такого залучення може стати розробка, зокрема, техніко-економічного підґрунтя певних заходів моніторингу стану захисту інформації з обмеженим доступом, комплексне поєднання окремих складових у єдину систему, а також розроблення пропозицій щодо необхідних обсягів та джерел фінансування (бюджетних або позабюджетних).

Матеріально-технічне забезпечення – дозволяє підтримувати дієздатність заходів моніторингу. Наприклад, інформація з обмеженим

доступом обробляється виключно за допомогою сертифікованої техніки (програмної продукції, програмних засобів).

Фінансове забезпечення – ще одна важлива складова ефективної реалізації моніторингу стану захисту інформації з обмеженим доступом.

З досвіду проведення, наприклад, моніторингу у фінансовій сфері, подібні нормативно-правові документи повинні містити: функціональні (посадові) обов'язкі працівників, відповідальних за проведення моніторингу; основних вимог до кваліфікації працівника, відповідальної особи за проведення моніторингу; встановлення правил проведення моніторингу та програм його здійснення тощо. Зокрема, діяльність працівників, відповідальних за проведення моніторингу може передбачати співпрацю з іншими структурами організації та їх фахівцями, надання методичних вказівок щодо подання необхідної інформації тощо.

Отже, моніторинг стану захисту інформації з обмеженим доступом по суті являє складну систему, яка повинна забезпечити кінцевого користувача (уповноважених суб'єктів) певним набором аналітичної продукції для вирішення завдань в даній сфері, тобто становити основу для розробки необхідних попереджувальних режимних заходів.

Механізм впровадження моніторингу стану захисту інформації з обмеженим доступом може включати:

розробку цілісної і комплексної системи аналізу стану захисту інформації з обмеженим доступом в межах повноважень власника інформації;

запровадження уніфікованої технології збирання та опрацювання необхідної статистичної інформації;

при наявності, проведення інвентаризації галузевих (або інших) баз даних на предмет наявності в них інформації, яка може бути використана для цілей моніторингу;

запровадження прогресивних технологічних підходів до формування та обробки інформаційних ресурсів;

введення в структуру бюджетних видатків витрати на моніторинг тощо.

Використання вище перерахованих факторів повинно дозволити за результатами проведення моніторингу стану захисту інформації з обмеженим доступом:

виявляти тенденції, які відбуваються у сфері захисту інформації з обмеженим доступом в межах повноважень власника інформації;

виявляти невідповідності в плануванні та реалізації діяльності суб'єктів управління в цій сфері;

приймати виважені управлінські рішення уповноваженими суб'єктами;

визначати повноту охоплення моніторингом сфери в межах прав власника інформації або суб'єктів уповноважених реалізовувати заходи охорони інформації з обмеженим доступом;

створювати нормативно-правові акти спрямовані на підвищення ефективності захисту різних видів інформації з обмеженим доступом тощо.

Питання для самоконтролю до розділу 4

1. Визначте основні, можливі загрози для існування інформації з обмеженим доступом в установах.
2. Охарактеризуйте можливу шкоду від несанкціонованого витоку інформації з обмеженим доступом в установі.
3. Наведіть приклади та проаналізуйте наслідки від витоку інформації з обмеженим доступом у відомих установах.
4. Визначте, яким чином може бути обрахована та до чого привести шкода від несанкціонованого витоку інформації з обмеженим доступом.
5. Охарактеризуйте основні, можливі варіанти підбору фахівців для підрозділів захисту інформації в установах.
6. Виділить основні види кадрового аутсорсингу та поясніть їх особливості реалізації.
7. Проаналізуйте особливості діяльності кадрових агентств, які спеціалізуються на підборі персоналу для установ.
8. Які способи для пошуку кандидатів для підрозділів захисту інформації з обмеженим доступом можуть використовувати кадрові агентства?

9. Виділить та проаналізуйте можливі проблемні питання, що можуть виникнути під час співпраці установи з кадровим агентством.

10. Проаналізуйте можливі переваги під час використання заходів моніторингу у сфері захисту інформації з обмеженим доступом.

11. Визначте, яким чином може бути запроваджено заходи моніторингу в установі, стосовно захисту інформації з обмеженим доступом?

12. Охарактеризуйте складові моніторингу стану захисту інформації з обмеженим доступом в установі.

Література

1. Афанасьев В.Г. Научное управление обществом / В.Г.Афанасьев – М.: Политиздат, 1975. – 267 с.

2. Панченко В.М. Сучасні тенденції розвитку технології контент-моніторингу в Україні // В.М.Панченко. Інформаційна безпека людини, суспільства, держави, 2011. – 2 (6). – С. 147 – 155

3. Саати Т., Кернс К. Аналитическое планирование. Организация систем: Пер. с англ. / Т.Саати, К.Кернс. – М.: Радио и связь, 1991.– 224 с.

4. Устинов В.А. Экономика управления предприятием. Учебное пособие / В.А.Устинов. - М.: ГАУ, 2004. – 232 с.

5. Юридична енциклопедія - 3 том: К., Вид-во ”Українська енциклопедія” ім. М.П. Бажана – 2001. – 534 с.

6. Андрощук Г.А., Крайнев П.П. Экономическая безопасность предприятия: защита коммерческой тайны: Монография / Г.А. Андрощук, П.П. Крайнев. – К.: Издательский Дом ”Ин Юре”, 2000. – 400 с.

7. Ассоциация Региональных Кадровых Агентств Украины: лучшие кадры всей страны [Електронний ресурс]. – Режим доступу: http: //www.arka.com.ua/

8. Владимирова Л.П. Прогнозирование и планирование в условиях рынка: Учебное пособие / Л.П. Владимирова. - М.: Издательский Дом ”Дашков и К0”, 2007, - 307 с.

9. Ильин А.И. Планирование на предприятии. / А.И. Ильин. - Минск: ООО ”Новое знание”, 2009, - 634 с.

10. Князєв С.О. Несанкціонований витік інформації з обмеженим доступом: сучасні світові тенденції / С.О. Князєв // Інформаційна безпека людини, суспільства, держави. – 2012. - № 2 (9).– С. 105 – 112

11. Князєв С.О. Основи організації планування діяльності підрозділу захисту інформації з обмеженим доступом / С.О. Князєв // Бизнес и безопасность. – 2010. - № 4 (78). – С.66 – 70

12. Князєв С.О. Кадрове забезпечення підрозділів захисту інформації з обмеженим доступом // Бизнес и безопасность. – К., 2011. - № 2 (82). – С.100 – 103

13. Князєв С.О. Використання моніторингу в сфері захисту інформації з обмеженим доступом // Бизнес и безопасность. – К., 2009. - № 5 (73). – С.92 – 94

14. Князєв С.О. Іноземний досвід захисту важливих інформаційних ресурсів // Бизнес и безопасность. – К., 2009. - № 3 (71). – С.27 – 29

15. Мескон М., Основы менеджмента. / М. Мескон, М. Альберт, Ф. Хедоури. - М.: ”Дело”, 1992, - 576 с.

16. Питерс Г. В поисках эффективного управления: опыт лучших компаний / Г. Питерс, Р. Уотермен. - М.: Прогресс, 1986, - 326 с.

17. «НАВИГАТОР»: Межрегиональная рекрутинговая кампания. Подбор руководителей, региональных представителей и редких специалистов на всей территории Украины [Електронний ресурс]. – Режим доступу: http://navigator.lg.ua/

18. НАВИГАТОР предлагает профессиональный подбор персонала по технологии Рекрутинг полного цикла [Електронний ресурс]. – Режим доступу: http://navigator.lg.ua/article.php?textname=met

19. Работодателю – подбор молодых специалистов. Capital Human Resources (CHR) [Електронний ресурс]. – Режим доступу: http://chr.com.ua/

20. Recruit Alliance: Recruiting agency. О кампании [Електронний ресурс]. – Режим доступу: http:// recruit-alliance.kiev.ua/ru/

21. Recruiting.net.ua. Путеводитель на рынке рекрутинговых услуг [Електронний ресурс]. – Режим доступу: http://www.recruiting.net.ua/

22. Recruiting.net.ua. Растет востребованность услуг кадровых операторов /[Електронний ресурс]. – Режим доступу: http://www.recruiting.net.ua/

23. Алексенцев А.И. Понятие и назначение комплексной системы защиты информации // Вопросы защиты информации. - 1996. - № 2. - с. 2 - 3

24. В Канаде празднуют День защиты информации // InfoWatch // http://www.infowatch.ru/

25. Доля А. Враг внутри // CIO / Компьютерра // http://www.cio-world.ru/bsolutions/374431/

26. Доля А. Сколько стоит утечка информации на самом деле? // CNEWS // http://safe.cnews.ru/

27. Доля А. Цифровое досье на каждого гражданина // Экспресс-электроника, 2008 // http://electronica.finestreet.ru/

28. Зотов К. Коллеги опаснее хакеров? // http://2074.ru/news/675-print.html

29. Идов Р. Утечки информации: экономические эффекты // Корпоративный менеджмент. – М., 2012

30. Инсайд 2010: Самые громкие и самые глупые утечки // CNews // http://www.cnews.ru/

РОЗДІЛ 5
ОСОБЛИВОСТІ ПОВОДЖЕННЯ З ІНФОРМАЦІЄЮ З ОБМЕЖЕНИМ ДОСТУПОМ В ПРОЦЕСІ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ

5.1 Поняття, ознаки, принципи та види підприємницької діяльності

Підприємництво як різновид творчої, пошукової, ризикованої соціальної діяльності в більшості країн світу з ринковою економікою вважається одним із найпрестижніших. Адже саме цей вид діяльності у відповідних умовах найкращим чином виявляє людську суть, допомагає працівникові реалізуватися як особистості. Підприємництву властивий значний індивідуалізм, високий рівень стимулювання співробітників, можливість якнайповнішої реалізації потенціалу кожного з них. Займаючись самостійною підприємницькою діяльністю, працівник зростає професійно й інтелектуально, що має реальний позитивний ефект для всього суспільства. Історія доводить, що швидкий прогрес економіки, інших сфер буття можливий переважно через розвиток господарської ініціативи членами суспільства.

Конституція України закріплює підприємництво як одне з найважливіших прав людини і громадянина. Згідно з нею кожен має право на підприємницьку діяльність, не заборонену законом. У свою чергу держава забезпечує захист конкуренції у цій сфері (ст. 42).

Це право означає, що кожний сам вільний обирати, орієнтуючись на свої бажання й можливості, чим займатися: стати, скажімо, підприємцем, менеджером на акціонерному підприємстві або розпочати індивідуальну трудову діяльність. Людина може визначитися, що потрібно їй особисто, і заздалегідь вирішити, коли і що треба робити, що від кого і в якому обсязі й на яких умовах вимагати для реалізації своїх економічних прав та інтересів. Проте приватна ініціатива не може суперечити суспільній користі та моралі, завдавати шкоди правам людини та її гідності, загрожувати особистій та

економічній безпеці.

Держава гарантує вільне підприємництво і вільність договорів всім підприємцям, незалежно від обраних ними організаційних форм діяльності, рівні права, а також створює рівні можливості для доступу до матеріально-технічних, фінансових, трудових, інформаційних, природних та інших ресурсів.

Водночас підприємницька діяльність депутатів, посадових і службових осіб органів державної влади та органів місцевого самоврядування обмежується законом, а монопольна підприємницька діяльність і недобросовісна конкуренція не допускається.

Згідно зі ст. 42 Господарський кодекс України (далі - ГК України) **підприємництво** — це самостійна, ініціативна, систематична, на власний ризик господарська діяльність, що здійснюється суб'єктами господарювання (підприємцями) з метою досягнення економічних і соціальних результатів та одержання прибутку.

Визначення підприємництва й відокремлення його від інших видів діяльності, спрямованих на отримання прибутку або доходу, мають як теоретичне, так і суто практичне значення. Наприклад, ст. 164 Кодексу України про адміністративні правопорушення (далі – КУАП) передбачає відповідальність, зокрема, за зайняття підприємницькою діяльністю без державної реєстрації. Якщо ж не буде доведено, що діяльність, яка провадилася, була саме підприємницькою, притягти особу до відповідальності за вищевказаною статтею неможливо. Для чіткого розмежування підприємництва та інших видів діяльності необхідно з’ясувати його ознаки.

Характеристика (ознаки) підприємницької діяльності (підприємництва).

1. *Підприємництво є самостійною діяльністю.*

Це означає, що, по-перше, підприємництво в Україні може здійснюватися в будь-яких організаційних формах, передбачених законами, на вибір підприємця (ст. 45 ГК України). Фізичні особи мають також можливість зареєструватись як суб'єкти підприємницької діяльності й вести обрану справу без створення організації, тобто юридичної особи.

Державна реєстрація юридичних осіб та фізичних осіб – підприємців, засвідчення факту створення або припинення юридичної особи, набуття або позбавлення статусу підприємця фізичною особою, а також вчинення інших реєстраційних дій, передбачених цим Законом, здійснюється шляхом внесення відповідних записів до Єдиного державного реєстру (ст. 4 Закону України «Про державну реєстрацію юридичних осіб та фізичних осіб - підприємців»).

По-друге, зважаючи на передбачений ч. 1 ст. 44 ГК України принцип вільного вибору підприємцем видів підприємницької діяльності, підприємці мають право проводити самостійно будь-яку діяльність відповідно до потреб ринку, на власний розсуд приймаючи відповідні рішення, що не суперечать законодавству.

2. *Підприємництво є ініціативною діяльністю.*

Це означає, що зайняття підприємницькою діяльністю є добровільним волевиявом. Жоден державний орган, недержавна організація, посадова особа не можуть примусити будь-кого займатися підприємництвом. Проте це не означає, що особа не може бути примушена до виконання добровільно взятих на себе зобов'язань (наприклад, за договором, укладеним у процесі підприємницької діяльності) або зобов'язань, які передбачені державою і випливають зі здійснення особою підприємницької діяльності (приміром, сплачувати податки).

3. *Підприємництво є систематичною діяльністю.*

Проте чітких критеріїв систематичності, регулярності (тобто, скільки разів потрібно зайнятися діяльністю, аби вона вважалася підприємницькою)

законодавством не встановлено.

4. *Підприємництво є діяльністю на власний ризик.*

Це означає, що за порушення договірних зобов'язань, кредитно-розрахункової чи податкової дисципліни, вимог до якості продукції та інших правил провадження господарської діяльності підприємство та приватний підприємець самостійно несуть відповідальність, передбачену законодавством України. Тобто суб'єкт підприємницької діяльності бере на себе як її позитивні, так і негативні наслідки. Підтвердженням цього є положення Цивільний кодекс України (далі – ЦК України), що встановлюють самостійну відповідальність фізичної особи — суб'єкта підприємницької діяльності (ст. 52) та юридичної особи (ст. 96) за зобов'язаннями, пов'язаними з їх підприємницькою діяльністю.

За загальними правилами ч. 3 ст. 96 цього Кодексу учасник (засновник) юридичної особи не відповідає за зобов'язаннями юридичної особи, а юридична особа не відповідає за зобов'язаннями її учасника (засновника), крім випадків, встановлених установчими документами та законом.

Як бачимо законодавство розрізняє відповідальність юридичної особи за наслідки своєї господарської діяльності (ризик) і відповідальність її засновника.

5. *Підприємництво є господарською діяльністю.*

Це означає, що, попри усю свою специфіку, підприємницька діяльність є складовою ширшого за обсягом поняття «господарська діяльність».

Згідно зі ст. 3 ГК України під господарською діяльністю розуміється діяльність суб'єктів господарювання у сфері суспільного виробництва, спрямована на виготовлення та реалізацію продукції, виконання робіт чи надання послуг вартісного характеру, що мають цінову визначеність. Категорія «господарська діяльність» є поняттям економічним, тому деяким її складовим неможливо дати суто юридичну характеристику.

Відповідно до Закону України «Про господарські товариства» ними визнаються підприємства, організації, установи, створені на засадах угоди

юридичними особами і громадянами з об'єднанням майна для підприємницької діяльності з метою одержання прибутку. Проте, до кола господарських товариств поки що не належать державні підприємства, організації та установи.

Підприємство як основна організаційно-правова форма підприємницької діяльності являє собою статутний суб'єкт самостійного господарювання, що має права юридичної особи і здійснює виробничу, науково-дослідну й комерційну діяльність з метою одержання прибутку (доходу). У своєму складі підприємство не має інших юридичних осіб.

Підприємства можуть об'єднуватись в асоціації, корпорації, консорціуми, концерни. Можливі й інші об'єднання за галузевою, територіальною чи іншою ознакою. Організації також мають право здійснювати підприємницьку діяльність.

Відмінність підприємства від організації полягає в тому, що перші виробляють якусь продукцію (товар), тоді як другі зазвичай виконують певні роботи (скажімо, будівельні, науково-дослідні, проектні тощо), надають послуги.

6. *Підприємницька діяльність здійснюється суб'єктами господарювання (підприємцями).*

Іншими словами, вона провадиться фізичними та юридичними особами, зареєстрованими як суб'єкти підприємницької діяльності у порядку, встановленому законодавством. Це означає, що підприємництвом можуть займатися як юридичні, так і фізичні особи, котрі набули статусу суб'єкта підприємницької діяльності відповідно до Закону України «Про державну реєстрацію юридичних осіб, фізичних осіб — підприємців та громадських формувань».

Проте наявність у визначенні підприємницької діяльності вищевказаного положення призводить до колізії з положеннями нормативно-правових актів, що встановлюють відповідальність за порушення порядку зайняття підприємницькою діяльністю. Адже з нього випливає, що

діяльність, яка здійснюється особами, не зареєстрованими як суб'єкти підприємницької діяльності, не можна відносити до підприємницької, а тому вищезазначені положення ст. 164 КУАП фактично не можуть застосовуватися.

7. *Внаслідок підприємницької діяльності досягаються економічні й соціальні результати.*

Підприємницька діяльність суттєво впливає на розвиток економіки і соціальної сфери. Серед економічних результатів найбільш вагомим є утворення конкурентного середовища, насичення ринку товарами й послугами, значна активізація міжнародних економічних стосунків.

Водночас ринкова переорієнтація спричиняє й нові проблеми. Наприклад, поширюються тіньові операції, котрі, як правило, супроводжуються уникненням від оподаткування, дефіцитністю державного бюджету, дестабілізуючи тим самим офіційну економіку. Через поширення цієї негативної тенденції гальмуються соціальні програми, поглиблюється майнове розшарування населення, ідейно-політичне протистояння в суспільстві.

Слід утім, зазначити, що малий і середній бізнес дає нові робочі місця, значно стимулює підвищення кваліфікації працівників, їхню ініціативу і творчість, загалом сприяє виживанню населення в кризові періоди. Поступове зміцнення суб'єктів підприємництва, їх прибутковість закладає додаткову фінансову базу для такої соціально корисної діяльності, як благодійництво, спонсорство, меценатство. Отже підприємництво несе безперечні позитивні й окремі негативні наслідки, що суттєво впливають на розвиток суспільства. Історичний досвід свідчить, що за наявності якісної правової бази ринкова організація економіки є найбільш ефективним і перспективним шляхом суспільного прогресу.

8. *Метою підприємницької діяльності є отримання прибутку.*

Якщо метою тієї чи іншої діяльності не є отримання прибутку, вона не може бути віднесена до підприємницької. Ця мета, як правило, знаходить

своє відображення в установчих документах суб'єкта підприємницької діяльності і простежується, виходячи з характеру його діяльності. За цією ж ознакою підприємницька діяльність відмежовується від розглянутого нами вище поняття господарської діяльності, де отримання прибутку не ставиться за основну мету.

Згідно зі ст. 44 ГК України підприємництво здійснюється на основі таких принципів:

1) *вільного вибору підприємцем видів підприємницької діяльності.*

Відповідно до ст. 1 Закону України «Про господарські товариства» останні можуть займатись будь-якою підприємницькою діяльністю, котра не суперечить законодавству України;

2) *самостійного формування підприємцем програми діяльності, вибору постачальників і споживачів продукції, що виробляється, залучення матеріально-технічних, фінансових та інших видів ресурсів, використання яких не обмежено законом, встановлення цін на продукцію та послуги відповідно до закону, вільного найму підприємцем працівників.*

Застосування цього принципу уточнюється положеннями спеціального законодавства про зайнятість, що містить положення, якими обмежуються трудові права іноземних громадян та осіб без громадянства. Ст. 3 Закону України «Про зайнятість населення» вимагає від них отримання дозволу на працевлаштування у державному центрі зайнятості України (див. також Порядок видачі, продовження дії та анулювання дозволу на застосування праці іноземців та осіб без громадянства, затверджений Постановою Кабінету Міністрів України від 25 травня 2013 №437);

3) *комерційного розрахунку та власного комерційного ризику* ***(див. ознаку № 4 підприємницької діяльності);***

4) *вільного розпорядження прибутком, що залишається у підприємця після сплати податків, зборів та інших платежів*, передбачених законом. На практиці приписами шляхом встановлення правил щодо

цільового використання коштів суб'єкта підприємницької діяльності — юридичної особи, обмеженнями на проведення операцій у готівкових коштах та ін.;

5) *самостійного здійснення підприємцем зовнішньоекономічної діяльності, використання належної йому частки валютної виручки на свій розсуд*.

Цей принцип обмежується, зокрема, положеннями ст. 1 Закону України «Про порядок здійснення розрахунків в іноземній валюті», які вимагають обов'язкове зарахування на валютні рахунки підприємців в уповноважених банках виручки резидентів у іноземній валюті у зазначені в контрактах, терміни виплати заборгованостей, але не пізніше 180 календарних днів з дати митного оформлення (виписки вивізної вантажної митної декларації) продукції, що експортується.

Існують також різні підстави класифікації підприємницької діяльності.

За *предметом діяльності* учасників відповідних правовідносин підприємницьку діяльність можна класифікувати на:

1. Виробничу підприємницьку діяльність, тобто таку, в процесі якої виробляється певна продукція.
2. Невиробничу підприємницьку діяльність:

- виконання робіт, надання послуг;
- торгівля;
- інша невиробнича діяльність, зокрема на фінансовому ринку.

За *суб'єктом* - учасником відповідних правовідносин підприємницька діяльність поділяється на:

1. Підприємництво без створення юридичної особи (просте). Воно здійснюється фізичними особами, що набули в установленому порядку статусу суб'єкта підприємницької діяльності.

2. Підприємництво зі створенням юридичної особи (складне).

Цей вид підприємницької діяльності за характером *обмежень*,

установлених чинним законодавством, в інтересах держави й суспільства, можна поділити на: вільну, дозвільну (ліцензовану) й державну.

Вільна характеризується тим, що підприємець має право без жодних обмежень самостійно провадити будь-яку діяльність, котра не суперечить чинному законодавству (за принципом «дозволено все, що не заборонено законом»).

Діяльність, провадження якої потребує певної згоди державних органів у вигляді спеціального дозволу (ліцензії), що видається Кабінетом Міністрів України або уповноваженим ним органом, називається дозвільна. Такий порядок зумовлений міркуваннями безпеки окремих громадян, так і суспільства в цілому. Перелік видів діяльності, що підлягають ліцензуванню, міститься у Законі України «Про ліцензування видів господарської діяльності».

Дозвільною є також діяльність, щодо якої встановлено законодавством певні обмеження, які, у свою чергу, можна поділити на:

- пов'язані з організаційно-правовою формою підприємництва;
- пов'язані з формою власності суб'єкта підприємництва (наприклад, діяльність у сфері виготовлення й реалізації військової зброї та боєприпасів не можуть провадити приватні підприємці).
- пов'язані із необхідністю придбання патенту (види діяльності, що підлягає патентуванню, а також порядок патентування визначаються Податковим кодексом України). Державна підприємницька діяльність - це діяльність, яку можуть провадити виключно державні підприємства (наприклад, виготовлення та реалізація наркотичних засобів, військової зброї та боєприпасів, вибухових речовин).

Нарешті, за *функціональною ознакою* підприємницька діяльність поділяється на такі види: виробництво продукції; виконання робіт; надання послуг; торговельна діяльність.

5.2 Поняття, зміст, загрози та складові безпеки підприємницької діяльності

Безпека – це стан захищеності особи, суспільства, держави від зовнішніх і внутрішніх загроз, що ґрунтується на діяльності людей, суспільства, держави, світової спільноти з виявлення, ослаблення, усунення, відбиття небезпек та загроз, здатних знищити їх, позбавити фундаментальних матеріальних і духовних цінностей, завдати неприпустимого збитку, закрити шлях до виживання і розвитку.

Безпека підприємства - стан захищеності життєво важливих і законних інтересів підприємства від зовнішніх і внутрішніх загроз у різних протиправних формах, що забезпечує його стабільний розвиток відповідно до статутних завдань.

Безпека як функція (діяльність) організації передбачає виконання суб'єктами і силами безпеки конкретних видів діяльності, спрямованих на протидію, тобто запобігання загрозам і їх усунення.

Важливою складовою безпеки бізнесу є економічна безпека підприємства. Її забезпечення є завданням як підрозділів безпеки, так і інших структурних одиниць підприємства.

Стан безпеки організації можна визначити через відповідні критерії показники (індикатори). З одного боку, вони сигналізують про зону безпеки, а з другого - про розвиток небезпеки внаслідок реалізації загроз, якими можуть бути:

- зростання кредитних ризиків;
- фінансові кризи;
- зниження інвестиційної та інноваційної активності і науково-технічного та технологічного потенціалу підприємства;
- нестабільність правового регулювання відносин у фіскальній сфері;
- критичний стан основних виробничих фондів підприємства;
- висока залежність діяльності підприємства від кон'юнктури зовнішніх ринків, контрагентів;

- промислове шпигунство;
- рейдерство тощо.

Види заходів безпеки:

загальні - запобігання можливим загрозам, розроблення й дотримання нормативів безпеки (здійснює управлінський персонал);

спеціальні - припинення загрози конфіденційними методами й методами роботи в надзвичайних ситуаціях (здійснюють працівники).

Загрози безпеці підприємства - це дія дестабілізуючих природних, інших об'єктивних, і/або суб'єктивних факторів, що можуть завдати потенційної чи реальної шкоди підприємству.

Загрози безпеці підприємства можна класифікувати за такими підставами:

1) за місцем виникнення: зовнішні та внутрішні;
2) за природою виникнення: політичні, кримінальні, конкурентні;
3) за ймовірністю виникнення: явні, приховані;
4) за поширенням: загальні, локальні;
5) за відношенням до людської діяльності: об'єктивні (зумовлені природними явищами); суб'єктивні (зумовлені діяльністю людини);
6) за можливістю прогнозування: прогнозовані, не прогнозовані;
7) за наслідками: катастрофічні, значні, незначні;
8) за сферою вияву: економічні (наприклад, змінам економічних чинників у ході реалізації інвестиційного проекту), політичні (виникнення різноманітних адміністративно-законодавчих обмежень діяльності), соціальні (страйки, запровадження під тиском робітників незапланованих соціальних програм тощо), екологічний (екологічні катастрофи, стихійні лиха - землетруси, лісові пожежі, повені тощо) та інші (рейдерство, крадіжки майна, нечесність партнерів тощо).

До об'єктів та предметів захисту від потенційних загроз належать:

– персонал;

– кошти;

– матеріальні засоби;

– інформаційні ресурси з обмеженим доступом, що становлять службову та комерційну таємницю;

– засоби і системи інформатизації;

– технічні засоби і системи охорони й захисту матеріальних та інформаційних ресурсів.

Безпека підприємства традиційно включає такі складові:

– фінансову;

– інтелектуальну й кадрову;

– інформаційну;

– техніко-технологічну;

– політико-правову;

– екологічну:

– силову.

Фінансова складова безпеки підприємства відображає фінансово-економічний стан підприємства, який характеризується ступенем його прибутковості та оборотності капіталу, здатності розраховуватися за борговими зобов'язаннями.

У процесі оцінки поточного рівня забезпечення фінансової складової безпеки підприємства підлягають аналізу:

– фінансова звітність і результати роботи підприємства (організації) - платоспроможність, фінансова незалежність, структура й використання капіталу та прибутку;

– конкурентний стан підприємства (організації) на ринку - частка ринку, якою володіє суб'єкт господарювання; рівень застосовуваних технологій і менеджменту;

– ринок цінних паперів підприємства (організації) - оператори та інвестори цінних паперів, курс акцій тощо.

Важливою передумовою охорони фінансової складової економічної безпеки є планування комплексу необхідних заходів та оперативна реалізація запланованих дій у процесі фінансово-економічної діяльності суб'єкта господарювання.

Інтелектуальна й кадрова складові безпеки підприємства. Належний рівень безпеки підприємства значною мірою залежить від персоналу, інтелекту та професіоналізму працівників.

Негативно впливають на інтелектуальну складову:

– звільнення провідних висококваліфікованих фахівців;
– зниження частки інженерно-технічних працівників і науковців у загальній чисельності працівників;
– зниження винахідницької та раціоналізаторської активності персоналу;
– зниження освітнього рівня працівників.

Загрози кадровій складовій безпеки підприємства можна поділити на внутрішні та зовнішні.

Внутрішні:

– невідповідність фаху працівників вимогам до них;
– недостатній фах працівників;
– слабка організація системи управління персоналом;
– неефективна система мотивації;
– помилки у плануванні ресурсів кадрового капіталу капіталу;
– зниження кількості раціоналізаторських пропозицій та ініціатив;
– відхід кваліфікованих працівників;
– працівники зорієнтовані на вирішення виключно внутрішніх тактичних завдань підрозділу, а не всього колективу;
– відсутність корпоративної політики або її слабкість;
– неякісна перевірка кандидатів на роботу.

Зовнішні:

– кращі умови праці та мотивація у конкурентів;
– переманювання працівників конкурентами;

– тиск на працівників ззовні;
– потрапляння працівників у різні види залежності;
– інфляційні процеси.

Отже, основними показниками кадрової безпеки є:

– чисельність персоналу та його динаміка;
– кваліфікація та інтелектуальний потенціал;
– ефективність використання персоналу;
– якість мотиваційної системи.

Охорона інтелектуальної та кадрової складових економічної безпеки охоплює взаємозв'язані й водночас самостійні напрями діяльності того чи іншого суб'єкта господарювання:

– робота з персоналом, спрямована на підвищення ефективності діяльності всіх категорій персоналу;
– збереження й розвиток інтелектуального потенціалу, тобто сукупності прав на інтелектуальну власність або на її використання (у тому числі патентів і ліцензій), систематичне підвищення знань і кваліфікації працівників.

На першій стадії процесу охорони цієї складової економічної безпеки здійснюється оцінка загроз негативних чинників і можливої шкоди від них.

З-поміж основних негативних впливів на економічну безпеку підприємства виокремлюють недостатню кваліфікацію працівників тих чи інших структурних підрозділів, їхнє небажання або нездатність приносити максимальну користь підприємству. Це може зумовлюватися низьким рівнем управління персоналом, браком коштів на належну оплату праці окремих категорій працівників чи нераціональним їх витрачанням.

Процес планування та управління персоналом, спрямований на охорону належного рівня економічної безпеки, має охоплювати організацію системи підбору, найму, навчання й мотивації потрібних працівників, включаючи матеріальні та моральні стимули, престижність професії, волю до творчості, соціальне забезпечення.

Техніко-технологічна складова безпеки підприємства.

Важливим елементом налагодження нормального рівня економічної безпеки є оцінка ефективності запобіжних - зіставлення загальних витрат на них і можливих втрат підприємства.

Процес охорони техніко-технологічної складової економічної безпеки, як правило, передбачає здійснення кількох послідовних етапів.

Перший етап охоплює моніторинг ринку технологій (збирання та аналіз інформації щодо особливостей технологічних процесів на підприємствах, котрі виготовляють аналогічну продукцію; аналіз науково-технічної інформації стосовно нових розробок у даній галузі, а також технологій, здатних здійснити інтервенцію на галузевий технологічний ринок).

Другий етап - це аналіз конкретних технологічних процесів і пошук внутрішніх резервів удосконалення технологій, що застосовуються.

На третьому етапі ***здійснюються:***

а) аналіз товарних ринків за профілем продукції, що виготовляється підприємством, та ринків товарів-замінників;

б) оцінка перспектив розвитку ринків продукції підприємства;

в) прогнозування можливої специфіки необхідних технологічних процесів для випуску конкурентоспроможних товарів.

Четвертий етап присвячується переважно розробці технологічної стратегії розвитку підприємства (виробника продукції), а саме:

- виявлення перспективних товарів із групи (номенклатури, асортименту), що виготовляється підприємством;
- планування комплексу технологій для виробництва перспективних товарних позицій;
- фінансування технологічного розвитку підприємства на засадах оптимізації витрат за програмою технологічного розвитку для вибору альтернатив, опрацювання власних розробок або придбання патентів і необхідного устаткування на ринку;
- розробка загального плану технологічного розвитку підприємства (з

відображенням у ньому вибору альтернативного варіанта технологічного розвитку, строків та обсягів фінансування, відповідальних виконавців);

- складання плану власних корпоративних науково-дослідних робіт відповідно до плану технологічного розвитку підприємства.

На п'ятому етапі оперативно реалізуються плани технологічного розвитку підприємства у процесі його виробничо-господарської діяльності.

Шостий етап, завершальний - аналізу результатів практичної реалізації заходів щодо охорони техніко-технологічної складової економічної безпеки на підставі спеціальної карти розрахунків ефективності таких заходів.

Політико-правова складова безпеки підприємства — це захист від надмірного податкового тиску, нестабільного законодавства, неефективної роботи юридичного відділу підприємства.

Правова складова полягає у всебічному правовому забезпеченні діяльності підприємства, дотриманні чинного законодавства.

Правову небезпеку становлять:

- недостатня правова захищеність інтересів підприємства в договірній та іншій діловій документації;
- низька кваліфікація працівників юридичної служби та помилки у підборі персоналу цієї служби;
- порушення прав підприємства і його працівників;
- навмисне чи ненавмисне розголошення комерційно важливих відомостей;
- порушення норм патентного права.

Загальний процес охорони політико-правової складової безпеки здійснюється за типовою схемою, яка охоплює такі елементи (дії):

– аналіз загроз негативних впливів;

– оцінка поточного рівня правового забезпечення;

– планування комплексу заходів, спрямованих на підвищення цього рівня;

– планування роботи юридичних підрозділів підприємства;

– оперативна реалізація запропонованого комплексу заходів щодо організації належного рівня безпеки.

Передусім детально аналізують загрози внутрішніх і зовнішніх негативних впливів на політико-правову складову безпеки та причини їхнього виникнення, а саме:

– внутрішні негативні чинники (неефективне фінансове планування та управління активами; малопродуктивна ринкова стратегія; помилкова цінова й кадрова політика);

– зовнішні негативні чинники (спекулятивні операції на ринку цінних паперів; цінова та інші форми конкуренції; лобіювання конкурентами нераціональних продуманих рішень органів влади);

– форс-мажорні обставини (стихійне лихо, страйки, збройні конфлікти) або наближені до таких (несприятливі законодавчі акти, ембарго, блокада, зміна курсу валют тощо).

Основними причинами виникнення внутрішніх негативних впливів можуть бути:

а) низька кваліфікація працівників юридичної служби підприємства та помилки у підборі персоналу цієї служби;

б) недостатнє фінансування юридичного забезпечення діяльності;

в) небажання чи нездатність підприємства активно впливати на зовнішнє політико-правове середовище його діяльності.

Останнє, зазвичай, виявляється у слабкому правовому опрацюванні договірних відносин даного суб'єкта господарювання з іншими, невмінні захищати інтереси підприємства в конфліктних ситуаціях, неефективному плануванні юридичного забезпечення бізнесової діяльності.

Причини виникнення зовнішніх негативних впливів здебільшого мають подвійний характер: аполітичний; законодавчо-правовий.

До першої групи причин можна віднести:

а) зіткнення інтересів суспільних груп (верств) населення з економічних, національних, релігійних та інших мотивів;

б) воєнні конфлікти (дії);

в) економічна й політична блокада, ембарго;

г) фінансові та політичні кризи світового (міжнародного) характеру.

У другій групі причин зазвичай виокремлюють:

а) здійснення власних політичних та інших цілей партіями (суспільними рухами), що перебувають при владі;

б) зміна положень чинного законодавства з питань власності, господарського і трудового права, оподаткування тощо.

Оцінка реального стану політико-правової безпеки підприємства (організації) провадиться в кількох напрямках:

– рівень організації та якості робіт щодо охорони цієї складової загального рівня економічної безпеки;

– бюджетно-ресурсне забезпечення робіт;

– ефективність діяльності відповідних підрозділів суб'єктів господарювання.

Інформаційна складова безпеки підприємницької діяльності полягає у здійсненні ефективного інформаційно-аналітичного забезпечення господарської діяльності підприємства. Відповідні служби виконують при цьому певні функції, які в сукупності складають процес створення та захисту інформаційної складової безпеки.

До таких функцій належать:

– збирання усіх видів інформації, що має стосунок до діяльності суб'єкта господарювання (щодо всіх видів ринків, політичних події і тенденцій макроекономічного розвитку світової та національної економік, корисної науково-технічної інформації);

– аналіз одержуваної інформації з обов'язковим дотриманням загальноприйнятих принципів (систематизації, безперервності надходження, усебічного характеру аналітичних процесів) і методів (локальних із специфічних проблем, загальнокорпоративних) організації робіт;

– прогнозування тенденцій розвитку науково-технологічних,

економічних і політичних процесів на підприємстві (в організації), в країні та у світі стосовно конкретної сфери бізнесу (діяльності), а також показників, яких необхідно досягти суб'єкту господарювання (наприклад, фінансові прогнози, прогнози об'єктів виробництва й технологічного розвитку);

– оцінка рівня економічної безпеки за всіма складовими та в цілому, розробка рекомендацій для підвищення цього рівня на конкретному підприємстві;

– інші види діяльності з розробки інформаційної складової економічної безпеки (зв'язки із громадськістю, формування ділової репутації та привабливого іміджу фірми, захист таємної та конфіденційної інформації).

На підприємство постійно надходять потоки інформації, яку поділяють на:

1) відкриту офіційну;
2) вірогідну нетаємну, одержану через неформальні контакти працівників з носіями такої інформації;
3) вірогідну таємну, отриману через неформальні контакти працівників з носіями такої інформації.

Дослідження показують, що 90-95% усієї необхідної інформації можна отримати легально, вивчаючи виступи учасників різноманітних наукових і виробничих форумів, відкриті публікації, експонати різних виставок, ярмарків, презентацій, дані товарних і фондових бірж, оголошення про наявні вакансії, конкурси на заміщення посади тощо. Тому на підприємстві слід запровадити правові норми захисту таємниць, а також систему контролю за збереженням комерційної таємниці. Оперативна реалізація заходів з розроблення та охорони інформаційної складової економічної безпеки здійснюється послідовним виконанням певного комплексу таких робіт:

– збирання різних видів необхідної інформації;
– оброблення та систематизація добутої інформації;
– аналіз цієї інформації;
– захист інформаційного середовища підприємства, що традиційно

охоплює:

1) заходи захисту від промислового шпигунства з боку конкурентів чи інших юридичних та фізичних осіб;

2) технічний захист приміщень, транспорту, кореспонденції, переговорів, різної документації від несанкціонованого доступу зацікавлених юридичних і фізичних осіб до закритої інформації;

3) збирання інформації про потенційних ініціаторів промислового шпигунства та проведення необхідних запобіжних заходів з метою припинення відповідних спроб;

4) зовнішня інформаційна діяльність.

Проблему охорони екологічної безпеки суспільства від суб'єктів господарювання, що здійснюють виробничо-комерційну діяльність, можна вирішити тільки через розробку і ретельне дотримання національних (міжнародних) норм мінімально допустимого вмісту шкідливих речовин, які потрапляють у навколишнє середовище, а також екологічних параметрів продукції, що виготовляється. Підприємства добровільно не будуть цього робити, бо такі заходи потребують додаткових витрат на очисні споруди та на відповідні ефективні екологічно чисті технології. Єдиним чинником, що спонукає їх до належної екологізації виробництва, є застосування відчутних штрафів за порушення екологічного законодавства.

При цьому індикаторами екологічної складової економічної безпеки є, з одного боку, нормативи граничних допустимих концентрацйії шкідливих речовин, установлені національним законодавством, а з іншого, - аналіз ефективності заходів для забезпечення такої екологічної складової.

На підставі загальних стратегічних рекомендацій, опрацьованих за результатами аналізу карти розрахунку ефективності здійснюваних заходів, планується комплекс заходів для розробки екологічної складової економічної безпеки на перспективу. План забезпечення екологічної складової є частиною загального плану (програми) досягнення належного рівня економічної безпеки в цілому. Він має вигляд логічного сценарію здійснення необхідного

комплексу заходів у календарній послідовності з додаванням розрахунку ефективності практичної реалізації цих заходів.

Алгоритм процесу охорони екологічної складової економічної безпеки полягає у проведенні таких послідовних дій:

1) розрахунок карти ефективності здійснюваних заходів для охорони екологічної складової економічної безпеки на підставі звітних даних про фінансово-господарську діяльність підприємства;

2) аналіз виконаних розрахунків і розробка рекомендацій для підвищення ефективності здійснюваних заходів;

3) розробка альтернативних сценаріїв реалізації запланованих заходів;

4) вибір пріоритетного сценарію на підставі порівняння розрахунків ефективності запланованих заходів;

5) передання обраного планового сценарію у складі загального плану охорони економічної безпеки в підрозділи, які здійснюють функціональне планування фінансово-господарської діяльності підприємства;

6) практичне здійснення запланованих заходів у процесі діяльності підприємства.

Силова складова безпеки підприємства полягає у захисті кожного працівника від загроз життю, здоров’ю та матеріальному благополуччю, а також захист майна підприємства від кримінальних посягань. До основних негативних впливів на цю складову належать фізичні й морально-психологічні впливи на конкретних осіб з метою заподіяти шкоду їх здоров'ю, майну, репутації, що становить загрозу нормальній діяльності підприємства.

На практиці за силову безпеку відповідає служба охорони підприємства, яка здійснює фізичний захист його керівників, організовує пропускний режим, охороняє будівлі, приміщення, лінії зв’язку та обладнання від несанкціонованого доступу, забезпечує режим секретності

документації.

Явища (дії), що негативно впливають на рівень силової складової безпеки підприємства зумовлюються кількома причинами. Основними з них є:

- нездатність підприємств-конкурентів досягти переваг коректними методами ринкового характеру, тобто за рахунок підвищення якості власної продукції, зниження поточних витрат на виробництво (діяльність), удосконалення маркетингових досліджень ринку тощо;
- кримінальні мотиви одержання юридичними (фізичними) особами доходів через шантаж, шахрайство, крадіжки, тощо;
- некомерційні мотиви посягань на життя та здоров'я керівників і працівників підприємства, а також на його майно.

Такі мотиви можуть зумовити намагання негативного впливу (фізичного та/або морального характеру) на працівників фірми. Спроби фізичного усунення керівників, вищих менеджерів і провідних фахівців спричиняються переважно зіткненням комерційних інтересів підприємств конкурентів, конфліктами їхнього керівництва з кримінальними суб’єктами, а також політичними мотивами. Спроби морального тиску на працівників здійснюються, як правило, з метою змусити їх учинити дії, що завдаватимуть шкоди економічній безпеці та ефективному функціонуванню фірми. У кінцевому підсумку сукупність негативних дій щодо силової складової безпеки можна стисло сформулювати так:

1) фізичні та моральні впливи особистого спрямування (проти конкретної особи);

2) негативні дії, спрямовані на завдання шкоди майну, зменшення активів підприємства, втрату ним фінансової незалежності;

3) негативний вплив на інформаційне середовище підприємства (у тому числі промислове шпигунство).

В умовах ринкової конкуренції інформація стає цінним капіталом. Розвиток підприємництва в Україні зумовили значне збільшення обсягів

комерційної таємниці суб'єктів господарювання, охорона якої стає одним із пріоритетів їхньої діяльності.

Перехід України до ринкової економіки, розвиток підприємництва і конкуренції викликають необхідність правового захисту інформації, розголошення якої може завдати шкоди суб'єктам господарювання. Якщо у розвинутих країнах комерційна таємниця охороняється законодавством як цінний товар, то в Україні й до тепер повноцінний правовий механізм її захисту.

Окремі консультативні організації пропонують структурувати інформацію про суб'єктів господарювання з метою визначення режимів доступу до неї. Інформацією про підприємство вважається сукупність відомостей, що закріплені у документах або інших носіях та містять інформацію про будь-які події та факти, пов'язані з діяльністю підприємства. Підприємство має проводити свою діяльність на принципах прозорості та відкритості.

Інформація, яка отримується, обробляється, зберігається, поширюється та використовується на підприємстві, є його власністю, якщо інше не передбачено чинним законодавством або договором. За режимом доступу інформація про підприємство поділяється на відкриту та інформацію з обмеженим доступом.

Відкрита інформація - це будь-які відомості, що є у володінні, користуванні або розпорядженні підприємства та не віднесені до категорії інформації з обмеженим доступом. Відкрита інформація вільно поширюється серед акціонерів та інших осіб.

Підприємство забезпечує доступ до відкритої інформації через:

– публікації в офіційних друкованих виданнях,
– поширення через засоби комунікації;
– надання на запити зацікавлених осіб.

Інформація з обмеженим доступом відповідно до Положення про інформацію на підприємстві та порядок її надання поділяється на

конфіденційну й таємну (комерційну таємницю).

Конфіденційна інформація - це відомості технічного, фінансового та комерційного характеру, що перебувають у володінні, користуванні чи розпорядженні підприємства, не є загальнодоступними та поширення яких відбувається за бажанням підприємства відповідно до порядку, встановленого його внутрішніми документами. Перелік відомостей, що є конфіденційними, а також перелік осіб, котрі мають доступ до конфіденційної інформації, встановлюється спостережною радою підприємства за його поданням правління та зберігається у правлінні підприємства. Конфіденційна інформація надається за рішенням правління та за умови письмового попередження осіб яким вона надана, про обов'язок її нерозголошення, збереження.

Посадові особи підприємства зобов'язані не допускати розголошення підприємствами, установами, організаціями - діловими партнерами підприємства, а також працівниками підприємства, особами, що закінчили трудові відносини з ним та претендентами на роботу на підприємстві конфіденційної інформації, що стала їм відома під час переговорів, співбесід, спільної або трудової діяльності.

Інформація, що визнана конфіденційною, надається на підставі чинного законодавства України, рішення органів управління підприємства чи запиту зацікавленої особи (заявника).

Єдина відмінність полягає в тому, що при отриманні конфіденційної інформації особа, що її отримує, повинна підписати відповідне зобов'язання про нерозголошення, яке засвідчується головою правління або уповноваженою ним посадовою особою та зберігається на підприємстві.

Інформація не вважається конфіденційною, якщо вона:

– є загальновідомою;
– стала загальновідомою не з вини особи, якій вона надана;
– стала відомою з будь-яких інших джерел до або після надання її особі;
– згідно з чинним законодавством не може бути віднесена до

конфіденційної.

Доступ до *таємної інформації* (комерційної таємниці) мають лише посадові особи та працівники підприємства, зазначені у відповідному переліку.

Порядок розробки, зберігання, розповсюдження, використання, знищення та розмноження інформації, що є конфіденційною або таємною, регулюється спеціальними внутрішніми нормативними актами.

Положенням про інформацію на підприємстві та порядок її надання також передбачено, що посадові особи підприємства у межах наданої їм компетенції повинні забезпечувати своєчасну та якісну підготовку, публікування та надання інформації. Посадові особи несуть передбачену чинним законодавством відповідальність за повноту та достовірність інформації, що поширюється.

Посадові особи, котрі відповідають за зберігання інформації з обмеженим доступом, несуть матеріальну, дисциплінарну, адміністративну та кримінальну відповідальність за розголошення такої інформації, якщо воно сталося з їхньої вини й завдало матеріальної та іншої шкоди підприємству.

На сучасному етапі демократичних перетворень Україна визнає людину, її життя і здоров'я, честь і гідність, недоторканність і безпеку найвищою соціальною цінністю.

При цьому стаття 21 Конституції України визначає, що «усі люди є вільні і рівні у своїй гідності та правах. Права і свободи людини є невідчужуваними та непорушними».

Кожна людина має право на вільний розвиток своєї особистості, якщо при цьому не порушуються права і свободи інших людей, та має обов'язки перед суспільством, в якому забезпечується вільний і всебічний розвиток її особистості (стаття 23 Конституції України).

До невід’ємних засад правового статусу людини як учасника інформаційних відносин належить і стаття 34 Конституції України:

«Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань.

Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб - на свій вибір. Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя».

Стаття 23 Закону України «Про інформацію» дає визначення поняття «інформація про особу».

Інформація про особу - це сукупність документованих або публічно оголошених відомостей про особу.

Основними даними про особу (персональними даними) є: національність, освіта, сімейний стан, релігійність, стан здоров'я, а також адреса, дата і місце народження.

Джерелами документованої інформації про особу є видані на її ім'я документи, підписані нею документи, а також відомості про особу, зібрані державними органами влади та органами місцевого й регіонального самоврядування в межах своїх повноважень.

Обмеження доступу до інформації про особу здійснюється на підставі такої норми ст. 23 Закону України «Про інформацію»: «забороняється збирання відомостей про особу без її попередньої згоди за винятком випадків, передбачених законом». Кожна особа має право на ознайомлення з інформацією, зібраною про неї.

Конфіденційна інформація про особу є одним із специфічних видів інформації з обмеженим доступом. Її правовий статус визначається Законом України «Про інформацію», а офіційне тлумачення викладене у Рішенні Конституційного Суду України №5-зп від 30 жовтня 1997 року (справа

К.Г.Устименка). Зокрема, зазначається, що частину четверту статті 23 Закону України «Про інформацію» треба розуміти так, що забороняється не лише збирання, а й зберігання, використання та поширення конфіденційної інформації про особу без її попередньої згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту, прав та свобод людини.

До конфіденційної інформації про особу належать, зокрема, такі свідчення про особу: освіта, сімейний стан, релігійність, стан здоров'я, дата і місце народження, майновий стан, інші персональні дані.

Конституцією України встановлено головні засади захисту особи від втручання в її особисте і сімейне життя. Зокрема, гарантовано таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції. Для іноземців та осіб без громадянства в Україні встановлено національний режим захисту цих прав. Законодавством України передбачена також кримінальна відповідальність за порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через електронно-обчислювальну техніку.

ЦК України це право відносить до особистих немайнових прав та передбачає судовий порядок його захисту від протиправних посягань. Цим кодексом визначено також право власності адресата на надіслані на його адресу листи, телеграми тощо. Проте на їх публікацію повинен надати згоду і суб’єкт, який їх надіслав. Якщо кореспонденція стосується особистого життя іншої фізичної особи, для її використання, зокрема шляхом опублікування, потрібна згода цієї особи. Визначено також, що кореспонденція, яка стосується фізичної особи, може бути долучена до судової справи лише у разі, якщо в ній містяться докази, що мають значення для вирішення справи. Інформація, яка міститься в такій кореспонденції, не підлягає розголошенню.

Право на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції може бути обмежено рішенням суду за наявності підстав, передбачених ст. 6 Закону України «Про оперативно-розшукову

діяльність», з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо. За забезпеченням законності цих обмежень здійснюється прокурорський нагляд. Законодавство зобов'язує операторів, провайдерів телекомунікацій вживати відповідно до законодавства технічних та організаційних заходів із захисту поштових відправлень, телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом про організацію телекомунікаційних мереж та інформації, що передається цими мережами.

Стан здоров'я особи також включено до переліку персональних даних, які підлягають захисту. Механізми правового захисту такої інформації встановлено ст. 286 ЦК України та Законом України «Основами законодавства України про охорону здоров'я». Фізична особа має право на таємницю даних про стан свого здоров'я, факт звернення за медичною допомогою, діагноз, а також про відомості, одержані при її медичному обстеженні. Чинним законодавством заборонено вимагати та подавати за місцем роботи або навчання інформацію про діагноз та методи лікування фізичної особи. Фізична особа зобов'язана утримуватися від поширення цієї інформації, яка стала їй відома у зв'язку з виконанням службових обов'язків або з інших джерел.

Офіційним тлумаченням окремих статей закону України «Про інформацію» до основних персональних даних віднесено майновий стан особи.

Таємність інформації про майновий стан особи та факти розпорядження нею своїм майном захищені також інститутом таємниці вчинення нотаріальних дій. Так, відповідно до ст. 8 Закону України «Про нотаріат» нотаріуси, інші посадові особи, які вчиняють нотаріальні дії, та особи, яким про вчинені нотаріальні дії стало відомо у зв'язку з виконанням ними службових обов'язків, зобов'язані додержуватися таємниці цих дій, у зв'язку із чим довідки про вчинені нотаріальні дії та документи видаються

тільки громадянам та юридичним особам, за дорученням яких або щодо яких вони вчинялися.

Закон допускає видачу довідок про вчинювані нотаріальні дії на письмову вимогу компетентних державних органів у зв'язку з кримінальними, цивільними або господарськими справами, що знаходяться у їх провадженні, чи у зв'язку із необхідністю визначення правильності стягнення державного мита та об’єктів оподаткування.

Порушення права фізичної особи на конфіденційну інформацію може стати підставою для захисту такою особою своїх прав у судовому порядку. Такі судові розгляди становлять матеріальну й репутаційну загрозу для суб'єкта господарювання. Розуміння ж вищим менеджментом і співробітниками безпекових підрозділів підприємства нормативно-правових і організаційних аспектів стосовно конфіденційної інформації фізичної особи сприятиме нейтралізації подібних потенційних загроз.

5.3 Захист інформації з обмеженим доступом на підприємстві

Захист інформації - це комплекс організаційних, правових, технічних та криптографічних заходів, спрямованих на забезпечення прав на володіння, розпорядження та управління інформацією, яка підлягає захисту; запобігання витоку і втраті інформації; збереження повноти, достовірності, цілісності інформації, яка підлягає захисту, її масивів і програм оброблення; збереження конфіденційності або секретності інформації за правилами, встановленими законодавчими та іншими нормативно-правовими актами.

Завданнями підрозділу захисту інформації є:

— забезпечення безпеки інформації структурних підрозділів та персоналу компанії у процесі інформаційної діяльності та взаємодії між собою, а також у стосунках із зовнішніми вітчизняними та іноземними організаціями;

— дослідження технологій опрацювання інформації з метою виявлення можливих каналів витоку;

— формування моделі загроз;
— розроблення політики безпеки інформації та заходів щодо її реалізації:
— організація та координація робіт, пов’язаних із захистом інформації на підприємстві;
— підтримка необхідного рівня захищеності інформації, ресурсів і технологій;
— розроблення проектів нормативних і розпорядчих документів на підприємстві;
— участь у підготовці персоналу та користувачів комп’ютерних систем;
— реєстрація, збирання та зберігання даних про всі події, які мали місце у системі, та зменшення негативного впливу на функціонування комп’ютерних систем.

У Стародавньому Римі діяв закон, що передбачав чималий штраф за примус чужих рабів до видачі таємниць свого хазяїна. Традиція вести торговельні книги, таємниця яких була різновидом комерційної таємниці, існувала в античному світі. Торговці й банкіри зобов'язані були вести такі книги, відображаючи в них свою діяльність. Дані торговельних книг були конфіденційними й розкривалися винятково для уточнення податків, у справах про спадкування майна, у випадках банкрутства або з метою правосуддя. Таким чином, держави ще на ранніх стадіях свого розвитку створювали закони, які захищали інтереси підприємців від можливого витоку секретів.

Історично так склалося, що комерційно важливу інформацію визначали різними термінами. У поняття «виробнича таємниця» включали внесення чого-небудь нового у процес створення благ; під «фабричною таємницею» розумівся як предмет патенту (першими ввели Англія, Франція й Німеччина), так і будь-яку особливість виробництва (еквівалент сучасного поняття «ноу-хау»); «торговельну таємницю» становили, наприклад, місця реалізації товарів, списки постачальників тощо.

Закони Російської імперії містили норми, що передбачали охорону фабричного секрету, торговельної таємниці й таємниці кредитних установ, які були засобами закріплення певного положення підприємства серед конкурентів. Порушення, пов'язані з розголошенням таємниці, попереджувались забороною службовцем оголошувати відомі їм таємниці підприємства, недопущенням сторонніх до торговельних книг та іншими заходами. За подібні порушення законодавство передбачало й застосування кримінальних покарань або стягнення збитків за цивільними позовами.

Правове регулювання системи захисту виробничої й комерційної таємниці царської Росії було скасовано радянською владою в листопаді 1917 року. У СРСР на державному рівні комерційна таємниця тривалий час не сприймалася як така і вважалася рудиментом капіталістичного ладу.

В умовах планової економіки СРСР протиправні посягання на економічну інформацію підприємств і організацій з боку вітчизняних суб'єктів господарювання були виключені оскільки не мали сенсу. Захист цієї інформації від посягань іноземних організацій цілком забезпечували спецслужби країни.

У 1990 році в СРСР була здійснена спроба визначення комерційної таємниці та відповідальності за її розголошення у статті 33 закону «Про підприємства». Цей закон мав також визначити загально - правові, економічні та соціальні основи організації підприємств різних форм власності та їх діяльності в умовах «розвитку товарно-грошових відносин і регульованого ринку». При цьому комерційною таємницею підприємства вважалися пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами та іншою діяльністю підприємства відомості, що не є державною таємницею, розголошення (передача, витік) яких може завдати шкоди його інтересам.

Зі здобуттям Україною незалежності починає формуватися окремий правовий інститут комерційної таємниці.

В останні роки зміни в політичному житті й економіці України стали

підґрунтям для виникнення значної кількості недержавних підприємств і організацій - самостійних суб'єктів господарювання. Їх новий статус, серед іншого, спричинив проблему захисту належної їм інформації з обмеженим доступом економічного характеру (комерційної, банківської таємниці та конфіденційної інформації).

Поряд із традиційними загрозами, які існують у сфері формування, зберігання й поширення інформаційних ресурсів, зростає небезпека несанкціонованого втручання в роботу інформаційних систем не тільки з метою отримання закритої інформації, а і для порушення її цілісності та знищення, дезорганізації інформаційної системи держави, суб'єктів підприємництва тощо. Виникла й така небезпека, пов'язана з новими явищами, як «інформаційна експансія», «інформаційна зброя», «інформаційна війна», що стали реаліями сучасності. Усе це вимагає не тільки застосування традиційних, практично перевірених заходів охорони інформаційних ресурсів, що містять відомості, віднесені до інформації з обмеженим доступом, а й розробки та впровадження заходів і засобів правового, організаційного, інженерно-технічного й криптографічного захисту вказаної інформації.

У теперішній час в Україні, як і в інших країнах світу, у процесі підприємницької діяльності, при створенні нових технологій, у результаті інтелектуальної праці виникають насичені найрізноманітнішими відомостями інформаційні об'єкти, що становлять комерційну цінність. Це можуть бути методики робіт, перспективні технічні рішення, результати маркетингових досліджень тощо, спрямовані на досягнення підприємницького успіху.

Проблема захисту комерційної таємниці має багато аспектів. Серед них найважливішими є визначення правового положення комерційної таємниці як соціального ресурсу, юридичне закріплення права на комерційну таємницю та створення правових гарантій його реалізації, регулювання відносин, які виникають у сфері обігу комерційної таємниці.

У країнах, де використовуються інформаційні об'єкти, які становлять комерційну цінність, немає єдиного підходу до визначення поняття такої інформації. Застосовуються різні термінологічні сполучення: «ділові секрети», «виробничі секрети», «торговельні секрети», «конфіденційна інформація», «комерційна таємниця» тощо.

Згідно із статтею 505 ЦК України **комерційною таємницею** вважається інформація, секретна в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових не є відомою та легкодоступною для осіб, які зазвичай мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

Досягнення успіху в підприємницькій діяльності дуже часто пов'язане з використанням комерційної таємниці й неможливістю її використання конкурентами. Виокремлюють такі основні мотиви неправомірного використання комерційної таємниці конкурентами:

- для поліпшення виробничої та комерційної діяльності організації (конкурента), що протиправно заволоділа комерційною таємницею, підвищення конкурентоспроможності продукції та ефективності виробництва, обрання оптимальної стратегії реалізації продукції та ділових переговорів;

- для завдання шкоди власнику комерційної таємниці, протидії реалізації його продукції, руйнування виробничих та торговельних зв'язків, впливу на його ділові переговори та угоди; зниження його інвестиційних можливостей, фабрикування та поширення неправдивих відомостей про конкурента; тощо.

Сьогодні втратам комерційної таємниці в Україні сприяє безсистемність її захисту, роз'єднаність зусиль держави та приватних підприємців у забезпеченні цілісності інформації, відсутність у власників комерційної таємниці організаційного досвіду щодо її захисту, брак правової

підготовки та інформаційної культури.

Аналіз практики застосування організаційно-правового механізму захисту комерційної таємниці являє цілу низку проблем, серед яких: відсутність чіткого визначення поняття «комерційна таємниця» з урахуванням інтересів як юридичних, так і фізичних осіб; не розробленість механізму реалізації права власності на інформацію, віднесену до комерційної таємниці; методики визначення її вартості; відсутність органу державної виконавчої влади, котрий формував би й реалізовував державну політику щодо охорони прав на комерційну таємницю тощо.

ГК України також частково визначає особливості комерційної таємниці, включаючи останню до об'єктів права інтелектуальної власності (ст.155). Ст. 162 цього кодексу визначає повноваження та права суб'єктів господарювання щодо комерційної таємниці, зокрема: «суб'єкт господарювання, що є володільцем технічної, організаційної або іншої комерційної інформації, має право на захист від незаконного використання цієї інформації третіми особами, за умов, що ця інформація має комерційну цінність у зв'язку з тим, що вона невідома третім особам і до неї немає вільного доступу інших осіб на законних підставах, а володілець інформації вживає належних заходів до охорони її конфіденційності».

Акцентуємо увагу на тому, що строк правової охорони комерційної таємниці обмежується часом дії сукупності зазначених вище умов.

Відповідно до постанови Кабінету Міністрів України від 09.08.93 р. №611 комерційну таємницю не становлять:

- установчі документи, документи, що дозволяють займатися підприємницькою чи господарською діяльністю та її окремими видами;
- інформація за всіма встановленими формами державної звітності;
- дані, необхідні для перевірки обчислення і сплати податків та інших обов'язкових платежів;
- відомості про чисельність і склад працюючих, їхню заробітну плату в цілому та за професіями й посадами, а також наявність вільних робочих

місць;

- документи про сплату податків і обов'язкових платежів;
- інформація про забруднення навколишнього природного середовища, недотримання безпечних умов праці, реалізацію продукції, що завдає шкоди здоров'ю, а також інші порушення законодавства України та розміри заподіяних при цьому збитків;
- документи про платоспроможність;
- відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, спілках, об'єднаннях та інших організаціях, які займаються підприємницькою діяльністю;
- відомості, що відповідно до чинного законодавства підлягають оголошенню.

Підприємства зобов'язані подавати перелічені у зазначеній постанові відомості органам державної виконавчої влади, контролюючим і правоохоронним органам, іншим юридичним особам відповідно до чинного законодавства, за їх вимогою.

Зважаючи на зазначені вище положення, можна виокремити такі правові ознаки комерційної таємниці:

- секретність інформації, яка є комерційною таємницею, полягає в тому, що вона не є відомою та легкодоступною для осіб, які зазвичай мають справу з видом інформації, до якого вона належить,
- інформація, яка визнається комерційною таємницею, має комерційну цінність, тобто певну цінову визначеність (вартість);
- комерційна таємниця - склад і обсяг відомостей, визначені суб'єктом господарювання або уповноваженим на це органом;
- при визначенні складу та обсягу комерційної таємниці має враховуватись постанова Кабінету Міністрів України від 09.08.93 р. №611 «Про перелік відомостей, що не становлять комерційної таємниці»;
- володілець інформації повинен вживати належних заходів до охорони інформації, яка є комерційною таємницею;

– строк правової охорони комерційної таємниці обмежується часом дії сукупності факторів, коли така інформація має комерційну цінність, невідома третім особам і до неї немає вільного доступу інших осіб на законних підставах, а володілець інформації вживає належних заходів до її схоронності.

Комерційна таємниця відповідно до ст.30 Закону України «Про інформацію» належить до інформації з обмеженим доступом.

Для того, щоб економічно важливі відомості мали статус саме комерційної таємниці, їх необхідно оформити відповідним чином.

Існування комерційної таємниці бажано передбачити в установчих документах підприємця, включивши, наприклад, в установчий договір та/або статут підприємства розділ, що регламентує її захист.

При формуванні переліку відомостей, що становлять комерційну таємницю підприємця, доцільно діяти в такий спосіб.

Для безпосереднього визначення переліку відомостей, що становлять комерційну таємницю, на підприємстві створюється спеціальна комісія, яка систематизує й уточнює інформацію для цього переліку.

Чисельність такої комісії не повинна, як правило, перевищувати чотирьох - п'яти осіб. Створюється вона з найбільш кваліфікованих і компетентних фахівців основних підрозділів і представників служби безпеки підприємства, ознайомлених як з діяльністю підприємства в цілому, так і з роботою окремих підрозділів. До її складу бажано включити:

- фахівця, який володіє фінансовими питаннями, кон'юнктурою ринку та інформацією щодо діяльності конкурентів (зазвичай, це фінансовий менеджер);

- фахівця, котрий досконало знає систему організації роботи підприємства, її особливості; фахівця з питань зв’язків з іншими підприємствами, а також з укладення контрактів і договорів;

- фахівця, котрий володіє певними даними щодо продукції, яка випускається, її технологічного циклу й виробництва, циркуляцію усіх видів

інформації (усної, документальної, у вигляді зразків, вузлів, блоків, готової продукції).

Якщо підприємство досить велике або його продукція має різнорідний характер, можна створити кілька таких груп: одну, головну, - з метою координації та узагальнення результатів роботи, інші - залежно від потреби по кожній окремій ділянці.

З іншого боку, не виключено, що підприємство може складатися лише з кількох осіб, особливо на початкових етапах розвитку. Тоді, вказане завдання здатен самостійно виконати один керівник за умови, що він володітиме всією необхідною інформацією. Однак, щоб уникнути суб'єктивних помилок,доцільно розглядати ці питання щонайменше удвох.

Те, що, групу мають складати провідні фахівці, які володіють повним обсягом даних, не означає, що варто обов'язково ознайомлювати всіх залучених експертів з конкретною інформацією, яка може становити комерційну таємницю, якщо раніше вони її не знали. У більшості випадків досить, якщо хоча б один з них детально обізнаний з окремим питанням, що розглядається, а інші мали про нього загальне уявлення. Такий підхід оптимізує роботу групи і вже на першому етапі виключить можливі передумови необґрунтованого поширення комерційної таємниці.

Із усього переліку інформації, з якою працює підприємець і яка циркулює на підприємстві, насамперед необхідно виключити відомості, що становлять державну таємницю (якщо суб'єкт господарювання з такою працює), а також ту інформацію, що не є комерційною таємницею відповідно постанови КМУ від 09.08.93 р. № 611.

До комерційної таємниці обов’язково слід віднести різні види ноу-хау, відомості про не захищені авторським або патентним правом винаходи й рацпропозиції; інформацію про факти укладання договорів та їх зміст.

Отже, перед групою експертів необхідно поставити комплекс питань у такій послідовності:

а) виділити всі види діяльності підприємства, що приносять прибуток

на даний момент;

б) на основі наявних відомостей про ринок збуту зіставити рівень прибутку для даного виду діяльності з аналогічними показниками на інших підприємствах;

в) видати прогноз на перспективу щодо рентабельності цієї діяльності.

Якщо з економічної точки зору зазначений вид діяльності відповідає поточним і перспективним цілям підприємства, а прибуток вищий, ніж у конкурентів, то експерти мають визначити те головне, завдяки чому цей вид діяльності дозволяє отримувати прибуток. Відповідь на це питання і буде комерційною таємницею підприємства.

Особливу увагу слід приділити розробці положення про комерційну таємницю на підприємстві. Такий документ є основним у системі правового захисту інформації від несанкціонованого доступу. У ньому розкриваються загальні положення у сфері захисту інформації, принципи й процедури розмежування доступу до такої інформації, порядок прийому, реєстрації, інвентаризації й обліку носіїв інформації, що містить комерційну таємницю. У положенні прописується також механізм забезпечення схоронності інформації, що є комерційною таємницею, зокрема деталізуються процедури забезпечення доступу до комерційної таємниці сторонніх осіб (включаючи контролюючи органи). Рекомендується встановити правило, згідно з яким сторонні особи допускаються до ознайомлення з документами, що містять комерційну таємницю, з дозволу керівника за обов'язкової наявності письмового запиту. При цьому такі особи повинні дати розписку про нерозголошення комерційної таємниці або укласти відповідну угоду з підприємством. У положенні доцільно регламентувати порядок поширення комерційної таємниці, а також процедуру виключення інформації з переліку комерційної таємниці.

Аналіз чинного законодавства дає підстави стверджувати, що законодавець, визначаючи засоби захисту комерційної таємниці, застосовує два підходи:

- абсолютного захисту, що захищає комерційну таємницю як об'єкт інтелектуальної власності від посягань будь-яких третіх осіб,

- відносного захисту, що передбачає захист нелегко важкодоступної та не загальновідомої комерційної інформації, щодо якої вжито заходів збереження її таємності, від актів недобросовісної конкуренції.

Саме такою концепцією слід керуватись для побудови системи інформаційної безпеки на підприємстві. Звісно, об'єкт захисту доволі незвичний - інтелектуальна власність з обмеженим доступом. Проте очевидним є й переваги, які зумовлені дуалістичною природою комерційної таємниці, а саме: комплексність і всебічність її захисту, що випливає з такого:

захист комерційної таємниці як інформації з обмеженим доступом забезпечується за допомогою встановлення і реалізації режиму таємності (ст. 30 Закону України «Про інформацію»);

захист комерційної таємниці як об'єкта інтелектуальної власності здійснюється судом з використанням спеціальних правових засобів, в тому числі й оприлюдненням у засобах масової інформації факту посягання на неї та публікування в друкованому офіційному видані відповідного судового рішення (ст. 432 ЦК України).

Умови, за яких працівник вважатиметься таким, якому комерційна таємниця відома на законних підставах:

а) він є керівником підприємства або виконує його обов'язки. В такому разі йому за статутом належить бути обізнаним в інформації з обмеженим доступом,

б) працівник створив на підставі трудового договору інформацію, яка є комерційною таємницею підприємства;

в) виконання трудових обов'язків працівника потребує його обізнаності в інформації з обмеженим доступом (з певного питання, в частині або в цілому), виходячи з чого його допущено до комерційної таємниці, про що є розпорядження керівника підприємства, а від працівника отримано

зобов'язання про нерозголошення комерційної таємниці. Поряд з цим не слід забувати, що працівник може стати потенційним конкурентом або вже бути таким в силу володіння корпоративними правами іншого підприємства. Не виключена і ситуація, коли працівник не має допуску до комерційної таємниці, але зацікавлений у тому, щоб отримати в будь-який спосіб відповідну інформацію.

У будь-якому випадку система захисту комерційної таємниці в трудових правовідносинах має бути спрямована на таке:

- працівники, яким довірено комерційну таємницю, не повинні розголошували її третім особам;
- працівники, яким не довірено комерційну таємницю, але відомо про її існування, не повинні збирати відповідну інформацію з метою її неправомірною використання.

З огляду на зазначене рекомендується включати норму про нерозголошення комерційної таємниці в трудовий договір (контракт) як керівника підприємства, так і інших співробітників.

На керівника має покладатися обов'язок із забезпечення збереження комерційної таємниці підприємства. У його контракт із власником підприємства доцільно включити відповідні положення. Зокрема, необхідно зобов'язати керівника зберігати комерційну таємницю організації й не використовувати її для заняття будь-якою іншою діяльністю на шкоду підприємству. Варто також зазначити, що керівник організації несе персональну відповідальність за створення необхідних умов для забезпечення схоронності комерційної таємниці підприємства. Зрозуміло, що керівник підприємства, як і члени трудового колективу, має бути попереджений про відповідальність за порушення режиму комерційної таємниці, зокрема про передбачену законом юридичну відповідальність та розірвання контракту.

Зобов'язання про нерозголошення інформації може бути оформлене як записом безпосередньо в тексті трудового договору (контракту), так і у

вигляді окремого документа - додатку до трудового договору (контракту). Форма та зміст відповідного розділу трудового договору (контракту) або додатка до нього в частині, що стосується збереження інформації, яка становить комерційну таємницю, мають велике значення. У разі розголошення працівником інформації, що становить комерційну таємницю, ці документи становитимуть юридичну основу для до відповідальності та відшкодування заподіяного збитку.

У договір (контракт) працівника, що допускається до комерційної таємниці, або в додаток до нього можуть бути включені такі зобов'язання:

- не розголошувати інформацію, що становить комерційну таємницю, яка буде йому довірена або стане відома по роботі;
- виконувати вимоги наказів, інструкцій і положень по забезпеченню схоронності комерційної таємниці;
- не розголошувати інформацію, що становить комерційну таємницю тих підприємців, з якими є ділові стосунки;
- не передавати третім особам і не оприлюднювати інформацію, яка становить комерційну таємницю, без згоди керівництва підприємства;
- у разі спроби сторонніх осіб одержати від працівника інформацію, що становить комерційну таємницю підприємства, негайно сповістити про це відповідну посадову особу;
- не використовувати інформацію, що становить комерційну таємницю підприємства, для заняття іншою діяльністю, котра як конкурентна дія може завдати шкоди підприємству;
- негайно повідомляти відповідну посадову особу підприємства про втрату або не достачу носіїв інформації, що становить комерційну таємницю, ключів від режимних приміщень, сховищ, сейфів, особистих печаток і про інші факти, які можуть призвести до розголошення комерційної таємниці, а також про причини й умови можливого витоку інформації, що становить комерційну таємницю підприємства;
- у випадку звільнення всі носії інформації, що становить комерційну

таємницю, які перебували в розпорядженні працівника у зв’язку з виконанням ним службових обов'язків під час роботи на підприємстві, передати відповідній посадовій особі.

Сьогоднішня практика підприємницької діяльності дає чимало прикладів, коли працівників поряд із підписанням додатків до договору (контракту) про нерозголошення й недопущення неправомірного використання комерційної таємниці змушують підписувати зобов'язання про відмову працювати після звільнення з підприємства на підприємствах-конкурентах протягом певного періоду. З цього приводу слід зазначити, що чинне законодавство України гарантує особі право на працю (ст. 43 Конституції України), зокрема можливість заробляти собі на життя працею, яку він вільно обирає або на яку вільно погоджується. Тому додатковий превентивний захист комерційної таємниці за допомогою обмеження права працівника на працю вважаємо є не лише недоцільним, а й неправомірним. Якщо працівник неправомірно використає відомості, що становлять комерційну таємницю підприємства, то навіть після звільнення з нього він нестиме відповідальність, у тому числі передбачену кримінальним законодавством.

Працівника під розписку слід попередити про відповідальність за невиконання взятих на себе зобов'язань. У трудовому договорі (контракті) або його невід'ємної частини (зобов'язанні про нерозголошення інформації, що становить комерційну таємницю) варто передбачити порядок ознайомлення працівника з діючими на підприємстві положеннями й інструкціями із забезпечення схоронності комерційної таємниці.

Якщо зібрати усі доступні способи запобігання порушенням, виходить цілком ефективний комплекс заходів, продумана реалізація якого може стати надійним захистом від розголошення конфіденційної інформації працівниками підприємства.

Американський психолог Абрахам Маслоу (Abraham Maslow) виокремив п’ять груп основних потреб індивіда: фізіологічні, безпекові,

комунікативні, соціальні та у самореалізації. Відтак, можна передбачити, що, створивши на підприємстві умови для задоволення працівниками потреб у реалізації їхніх здібностей і потенціалу, у суспільному визнанні значущості їхніх успіхів, можна створити сприятливий соціально-психологічний клімат, знизити плинність кадрів, сформувати «корпоративний патріотизм».

Домогтися цього в колективі й таким чином мінімізувати витік конфіденційної інформації найлегше на підприємстві, де:

- створено дієву систему матеріальних стимулів;
- кожен працівник забезпечений тривалою роботою;
- до підлеглих ставляться як до самостійних індивідів;
- є перспектива участі в прибутку підприємства;
- створено можливості для службового зростання;
- забезпечена участь усього персоналу у виробленні рішень.

Причинами розголошування працівниками комерційних секретів більшість науковців і практиків називають:

- балакучість, особливо пов'язану з уживанням алкоголю і спілкуванням у дружніх компаніях, — 32%;
- прагнення заробити гроші у будь-який спосіб за принципом «гроші не пахнуть» — 24%;
- відсутність служби безпеки підприємства — 14%;
- «Совкова» звичка ділитися досвідом, давати поради — 12%;
- безконтрольне використання інформаційних і копіювальних засобів на підприємстві — 10%;
- психологічні конфлікти між працівниками, між працівниками й керівництвом — 8%.

У теперішній час теорія та практика менеджменту не знають таких методів роботи з персоналом, які цілковито виключали б можливість розголошування комерційної таємниці та конфіденційної інформації. Найефективніший превентивний захід, на думку фахівців, — формувати відданий підприємству колектив, оскільки збереження корпоративних

таємниць визначальною мірою ґрунтується на високій лояльності працівників.

Тому необхідно створити і впровадити прозору та зрозумілу персоналові програму мотивації, так званий соціальний пакет та систему заохочень. Як показує досвід, чинниками, які сприяють формуванню відданості працівників, можуть бути: залежність заробітної плати від стажу роботи на підприємстві, можливість підвищення своєї кваліфікації, кредитування купівлі автомобіля чи нерухомості, медичне страхування та інші соціальні й матеріальні блага. Це ж стосується і планування кар'єри працівників. Кожен має чітко розуміти перспективу свого кар’єрного зростання: пропрацювавши в компанії певний час і досягши високих результатів, він може розраховувати на просування службовими сходами.

На сьогодні не існує чіткого нормативного регламентування процесу організації та реалізації режиму комерційної таємниці. /Законодавство містить лише імперативну вказівку на те, що комерційна таємниця має бути «предметом адекватних існуючим обставинам заходів збереження її секретності».

Порядок поширення інформації випливає із режиму, встановленого для, і визначається її власником. Відповідно до ч. 4 ст. 14 Закону України «Про інформацію» поширення інформації - це розповсюдження, обнародування, реалізація у встановленому законом порядку документованої або публічно оголошуваної інформації. Керівник підприємства вирішує всі питання щодо розповсюдження власними силами, оприлюднення через ЗМІ та реалізації права на розпорядження комерційною таємницею.

Способи розголошення відомостей, що становлять комерційну таємницю, можуть бути різними: повідомлення відповідної інформації іншим особам, зокрема конкурентам; надання іншим особам для ознайомлення документів, що містять комерційну таємницю; оприлюднення інформації, що є комерційною таємницею, в засобах масової інформації тощо.

Правові засади захисту комерційної таємниці від актів недобросовісної

конкуренції передбачені ст. 36 ГК України та деталізуються у ст. 16-19 Закону України «Про захист від недобросовісної конкуренції». У вказаних статтях дається кваліфікація:

- неправомірного збирання комерційної таємниці (ст. 16);
- розголошення комерційної таємниці (ст. 17);
- схилення до розголошення комерційної таємниці (ст. 18);
- неправомірного використанням комерційної таємниці (ст. 19).

У даних нормативно-правових актах встановлюється підстава для юридичної відповідальності особи, яка посягає на комерційну таємницю. Юридична відповідальність є засобом захисту комерційної таємниці, й має каральний (адміністративна) чи компенсаційний характер (цивільно-правова). Але практика засвідчила, неефективність такого підходу, оскільки засоби захисту комерційної таємниці підприємства мають виконувати превентивну функцію.

Юридичні особи, винні у скоєнні вищевказаних діянь недобросовісної конкуренції несуть відповідальність, передбачену у ст. 21 та 24 ЗУ «Про недобросовісну конкуренцію». Громадяни, вину яких у вчиненні названих правопорушень доведено і які займаються підприємницькою діяльністю без створення юридичної особи, несуть також адміністративну відповідальність. Стягнення за вказані правопорушення визначені ст. 164-3 КУАП - штраф від дев’яти до вісімнадцяти неоподатковуваних мінімумів доходів громадян.

Крім того, Кримінальний кодекс України (далі - КК України) містить дві статті, які передбачають кримінальну відповідальність за посягання на комерційну таємницю: ст. 231 «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю» і ст. 232 «Розголошення комерційної або банківської таємниці».

Так, умисні дії, спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської

діяльності, - караються штрафом від трьох тисяч до восьми тисяч неоподаткованих мінімумів доходів громадян, або обмеженням волі на строк до п'яти років, або позбавленням волі на строк до трьох років (ст. 231 КК України). Злочин, передбачений цією статтею вважається закінченим з моменту вчинення дій, спрямованих на незаконне збирання відомостей, що містять комерційну таємницю. Тобто, дії особи, вважаються злочинними ще задовго до того моменту, коли вона отримала відомості, що містять комерційну таємницю, оскільки склад злочину утворює вже збирання такої інформації.

Питання для самоконтролю до розділу 5

1. Поняття та ознаки підприємницької діяльності.
2. Принципи підприємницької діяльності
3. Види підприємницької діяльності.
4. Поняття підприємницького права.
5. Підприємства як суб'єкти підприємницької діяльності.
6. Поняття та зміст безпеки підприємницької діяльності.
7. Загрози безпеці підприємницької діяльності.
8. Складові безпеки підприємницької діяльності.
9. Поняття системи забезпечення безпеки підприємницької діяльності.
10. Складові системи забезпечення безпеки підприємницької діяльності.
11. Суб'єкти забезпечення безпеки підприємницької діяльності.
12. Політика безпеки підприємства.
13. Концепція безпеки підприємства.
14. Поняття та види інформації, що циркулює на підприємстві.
15. Поняття та зміст системи захисту інформації на підприємстві.
16. Поняття комерційної таємниці.
17. Правові ознаки комерційної таємниці.
18. Механізм визначення переліку інформації, яка становить комерційну таємницю.

Література

1. Конституція України // Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 14.
2. Кримінальний кодекс України // Офіційний Вісник України 2001. - № 21, Ст. 920.

3. Цивільний кодекс України // Офіційний Вісник України 2003. - № 11, Ст. 461.

4. Кодекс України про адміністративні правопорушення // Відомості Верховної Ради Української РСР (ВВР) 1984, додаток до № 51, Ст.1122.

5. Закон України від 19 вересня 1991 року № 1576-XII «Про господарські товариства» // Відомості Верховної Ради, 1991, № 49, ст.682.

6. Закон України від 23 березня 1996 року № 98/96-ВР «Про патентування деяких видів підприємницької діяльності» // Відомості Верховної Ради, 1996, № 20, ст.82.

7. Закон України «Про ліцензування певних видів господарської діяльності» від 01.06.2000 № 1775-III. // Відомості Верховної Ради України (ВВР), 2000, N 36, ст.299.

8. Закон України від 15 травня 2003 року № 755-IV «Про державну реєстрацію юридичних осіб та фізичних осіб - підприємців» // Відомості Верховної Ради, 2003, № 31-32, ст.263.

9. Закон України від 11 вересня 2003 року № 1160-IV «Про засади державної регуляторної політики у сфері господарської діяльності» // Відомості Верховної Ради, 2004, № 9, ст.79.

10. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» // Відомості Верховної Ради, 1994.-№31.-ст.286

11. Закон України «Про оперативно-розшукову діяльність»: наук.-практ. коментар. - К.: РВВ МВС України, 1993. - 120 с.

12. Закон України «Про інформацію» від 2 жовтня 1992 року №2657-XII // Відомості Верховної Ради, 1992, № 48, ст.650.

13. Закон України «Про основи національної безпеки України» від 19 червня 2003 р. // Офіц. Вісн. України. - 2003. - № 29. - Ст. 1433.

14. Постанова Кабінету Міністрів України «Про затвердження переліку органів ліцензування» від 14 листопада 2000 р. № 1698.

15. Указ Президента України від 23 липня 1998 року № 817/98 «Про деякі заходи з дерегулювання підприємницької діяльності».

16. Указ Президента України від 12 травня 1998 року № 456/98 «Про державну підтримку малого підприємництва».

17. Постанова Кабінету Міністрів України «Про затвердження переліку органів ліцензування» від 14 листопада 2000 р. № 1698.

18. Положення про технічний захист інформації в Україні, затверджене постановою Кабінету Міністрів України від 9 вересня 1994 р. № 632 // ЗП України. - 1994. - №12.

19. Про перелік відомостей, що не становлять комерційної таємниці: Постанова Кабінету Міністрів України від 09.08.1993 р. № 611 // Збірник постанов Уряду України. – 1993. – № 12. – Ст. 269.

20. Саніахметова Н.О. Підприємницьке право: Навч. посібник. − К.: А.С.К., 2001. − 704 с.

21. Бандурка О.М., Духов В. Є., Петрова К.Я., Червяков І.М.. Основи

економічної безпеки: Підручник для вищих навч. закл. / МВС України; Національний ун-т внутрішніх справ. - Х.: Видавництво НУВС, 2003. - 236с.

22. Бондарчук Ю.В., Марущак А.І. Безпека бізнесу: організаційно-правові основи // Науково-практичний посібник. – К.: Видавничий дім «Скіф», 2008. - 369 с.

23. Економічна безпека підприємств, організацій, установ (навчальний посібник) // В.Л. Ортинський, І.С. Керницький, З.Б. Живко та ін. - К.: Правова єдність, 2009. - 544 с.

24. Когут Ю.И. Безпека фірми – інформаційна безпека. - М., 1996.- 519 с.

25. Низенко З.И. Обеспечение безопасности предпринимательской деятельности: Учеб. Пособие. - К.: МАУП, 2003.- 124 с.

26. Одинцов А.А. Защита предпринимательства (экономическая и информационная безопасность). Учебное пособие. - М.: Междунар. отношения, 2003. - 328с.

27. Соснин А.С., Пригунов П.Я. Менеджмент безопасности предпринимательства: Уч.пособие. - К.:Изд-во Европ. ун-та, 2004.-357 с.

28. Шевчук Т.Ф. Безпека бізнесмена і підприємництва в Україні: Монографія. - К.: УСПП, 2002. - 424 с.

29. Чернявский А.А. Безопасность предпринимательской деятельности: Конспект лекций // Межрегион. акад. упр. персоналом. - К., 1998. - 121с.

30. Основи безпеки комерційної діяльності підприємств та банків: навч.-метод. Посібник / К.: КНТЕУ, 2005. – 200 с.

31. Серпєнко Н.П. Економічна безпека підприємництва // Світ бухгалтерського обліку. − 2006 − №4. − С. 75-80.

Практика защиты коммерческой тайны и интеллектуальной собственности в США. − К.: − Хрещатик, 2000.− с. 4

РОЗДІЛ 6.
ОСНОВИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

6.1. Класи завдань з технічного захисту інформації в інформаційних системах

Технічний захист інформації є одним з напрямків захисту інформації в інформаційних системах.

При цьому під інформаційною системою визначається сукупність організаційних і технічних засобів для збереження і обробки інформації з метою забезпечення інформаційних потреб користувачів.

З урахуванням широти наведеного поняття під інформаційну систему потрапляє як будь-яка класична бібліотека, сучасна електронна база даних, розміщена в мережі Інтернет або локальній комп'ютерній мережі.

В залежності від ступеня автоматизації процесів зберігання та обробки інформації інформаційна система може бути ручною (де задіяні лише люди), автоматизованою (в ній частково задіяні люди, а частково – автомати, наприклад ЕОМ) або автоматичною (задіяні лише автомати).

Більшість сучасних інформаційних систем в епоху розвитку інформаційних технологій як мінімум частково автоматизовані або навіть є повністю автоматичними. З урахуванням зазначеного при розгляді питань технічного захисту інформації акцент робиться саме на автоматизованих інформаційних системах.

Досить часто у літературі серед інформаційних систем за функціональними особливостями окремо виділяють інформаційно-телекомунікаційні системи та обчислювальні (комп'ютерні) системи.

Згідно із Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» під інформаційно-телекомунікаційною системою слід розуміти сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле. В свою чергу, згідно із положеннями цього законодавчого акту телекомунікаційна система

– це сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб. Отже, характерна риса телекомунікаційної системи – функціональна спрямованість на обмін інформацією між її елементами.

Під обчислювальною системою слід розуміти сукупність програмно-апаратних засобів, призначених для обробки інформації. Обчислювальна система поєднує технічні засоби обробки та передавання інформації, а також числові методи і алгоритми обробки даних, реалізовані у вигляді відповідного програмного забезпечення, як правило, змінного. Обчислювальна система може бути базою для побудови як телекомунікаційної, так і автоматизованої інформаційної системи.

Нарешті автоматизована (інформаційна) система – це організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

Наразі в Україні існує така класифікація автоматизованих систем (АС):

АС класу 1 (АС-1) – одномашинний багатокористувацький комплекс, який обробляє інформацію однієї або кількох категорій конфіденційності. Приклад – автономний (ізольований) персональний комп'ютер, доступ до якого здійснюється з використанням організаційних засобів безпеки.

АС класу 2 (АС-2) – локалізований багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності. Приклад – локальна обчислювальна мережа. Істотна відмінність від попередньої категорії – наявність категорій користувачів з різними повноваженнями доступу та наявність апаратного-програмного забезпечення, яке може одночасно обробляти інформацію різних категорій конфіденційності.

АС класу 3 (АС-3) – розподілений багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності. Приклад – глобальна мережа. Істотна відмінність від

попередньої категорії – необхідність передавання інформації через незахищене середовище.

Таким чином, питання технічного захисту інформації можуть бути актуальними для будь-якої інформаційної системи в найбільш широкому визначенні цього поняття. Утім, з урахуванням розвитку на сьогоднішній день інформаційних технологій, на практиці вони стосуються, як правило, саме автоматизованих (інформаційних) систем різного класу: АС-1, АС-2 або АС-3.

У широкому розумінні захист інформації в будь-якій системі – це діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в цій системі.

Технічний захист інформації – це вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів або апаратно-програмних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Таким чином, виходячи із наведеного визначення загальним об’єктом технічного захисту є інформація, що обробляється в інформаційній системі, та програмне забезпечення, яке призначено для обробки цієї інформації.

Безпосередніми об’єктами технічного захисту інформації є матеріальні об’єкти (будівлі, приміщення, окремі основні або допоміжні технічні засоби або їх групи), об’єднані загальним призначенням і пов’язані з обробкою інформації, що повинна бути захищеною.

Згідно із положеннями державних стандартів України об’єкт захисту, мету і завдання технічного захисту інформації визначають і встановлюють особи, які володіють, користуються, розпоряджаються інформацією, що захищається, у межах прав і повноважень, наданих законами України, підзаконними актами та нормативними документами з технічного захисту інформації.

Зазначений державний стандарт визначає, що фізичними носіями інформації можуть бути фізичні поля, сигнали, хімічні речовини, що

утворюються в процесі інформаційної діяльності, виробництва й експлуатації продукції різного призначення, тобто в процесі інформаційної діяльності. Середовищем поширення носіїв інформації можуть бути лінії зв'язку, сигналізації, керування, енергетичні мережі, прикінцеве мережеве обладнання, інженерні комунікації і споруди, огороджувальні будівельні конструкції, а також світлопроникні елементи будинків і споруд (отвори), повітряне, водне та інше середовища, ґрунт, рослинність тощо.

Метою технічного захисту інформації є запобігання витоку, блокуванню, викривленню або знищенню або порушенню цілісності інформації. Зазначена мета може бути досягнута шляхом побудови системи захисту інформації, що є організованою сукупністю методів і засобів забезпечення технічного захисту інформації.

Систему технічного захисту інформації складають сукупність суб'єктів, об'єднаних цілями та завданнями захисту інформації інженерно-технічними заходами або апаратно-програмними засобами, нормативно-правова та матеріально-технічна база.

Правову основу забезпечення технічного захисту інформації в Україні становлять: Конституція України, «Концепція (основи державної політики) національної безпеки України», Закони України «Про інформацію», «Про захист інформації в автоматизованих системах», «Про державну таємницю», «Про науково-технічну інформацію», державні стандарти України (ДСТУ 3396.0-96, ДСТУ 3396.1-96, ДСТУ 3396.2-97 тощо), інші нормативно-правові акти, а також міжнародні договори України, що стосуються сфери інформаційних відносин.

Побудова системи технічного захисту інформації здійснюється поетапно, в загальному вигляді у наступному порядку:

1 етап – визначення й аналіз загроз;

2 етап – розроблення системи захисту інформації;

3 етап – реалізація плану захисту інформації;

4 етап – контроль функціонування та керування системою захисту інформації.

Водночас, за своїми видами питання технічного захисту інформації охоплюють два великих класи завдань:

– захист інформації від витоку технічними каналами (акустичними, радіотехнічними, оптичними тощо);

– захист інформації від несанкціонованого доступу (НСД).

Розглянемо зміст заходів з технічного захисту інформації у цих двох класах завдань.

6.2. Захист інформації від витоку технічними каналами

Канал зв'язку – це частина комунікаційної системи, яка зв'язує між собою джерело повідомлень та його приймача.

Класична схема обробки та розповсюдження інформації, відома з теорії інформації, містить передавач інформації, канал зв'язку (або канал зберігання інформації, чи обидва канали разом) та приймач інформації (який може мати систему вторинної обробки). З позиції класичної теорії інформації канал зв'язку є найбільш уразливою ділянкою для дії завади.

Технічний канал витоку інформації – це сукупність небезпечних фізичних сигналів, середовища їх розповсюдження та зберігання, пов'язаних з об'єктом технічного захисту інформації, а також способів і засобів, що можуть бути застосовані для зняття інформації з об'єкту, що охороняється, на основі інтерпретації фізичних сигналів у пов'язаному з ним середовищі.

Нагадаємо з фізики, що фізичний сигнал – це зміна певної фізичної величини (наприклад, температури, тиску повітря, світлового потоку, сили струму тощо), що використовується для пересилання даних. Саме завдяки цій зміні сигнал може нести в собі якусь інформацію.

В цьому аспекті небезпечний фізичний сигнал – це фізичний сигнал, що містить інформацію, яку необхідно захищати.

Технічні канали витоку інформації можна класифікувати за наступними критеріями:

а) за фізичною природою:

– акустичні канали (розповсюдження звукових коливань);

– радіотехнічні канали (відкриті канали радіозв'язку та канали, що утворюються за рахунок паразитного випромінення та наводу);

– електричні канали (засоби провідникового зв'язку та різні струмопровідні комунікації);

– оптичні канали (електромагнітне випромінювання від інфрачервоної до ультрафіолетової частини спектру).

За своєю фізичною природою часто технічні канали витоку можуть бути комбінованими.

б) за походженням:

– природні канали (утворюються на базі фізичних властивостей джерел виникнення небезпечних сигналів, самих небезпечних сигналів та середовища їх розповсюдження);

– штучні канали, в тому числі створеними навмисно (використовуються зміни фізичних властивостей джерел та середовищ розповсюдження небезпечних сигналів, а також подання спеціальних сигналів на окремі елементи приміщення).

Штучні канали витоку, як правило, створюються шляхом конструктивних змін джерел та конструкції об'єкту, де розповсюджуються небезпечні сигнали. Крім того, сама апаратура технічної розвідки, розміщена на об'єкті, що охороняється, утворює навмисний штучний канал витоку інформації.

Для того, щоб захищати інформацію від витоку необхідно знати потенційні канали витоку та методи їх блокування.

Розглянемо спочатку потенційні канали витоку, зокрема, фізичні основи утворення технічних каналів витоку інформації.

1. Акустичний канал.

Фізична природа цього каналу пов’язана з акустичними сигналами. Акустичний сигнал – це механічні коливання часток пружного середовища. Виходячи з цього визначення, акустичні сигнали можуть розповсюджуватися у будь-якому пружному середовищі. Єдине середовище, в якому розповсюдження акустичного сигналу неможливо – повний вакуум (оскільки відсутні частинки повітря, тобто немає пружної середи).

Всі інші середовища придатні для розповсюдження акустичних сигналів. Саме цим пояснюється можливість проходження акустичних сигналів через елементи будівельних конструкцій (стіни, стелі, підлоги, двері, скло вікон, труби і тощо).

Акустичний сигнал може безпосередньо прийматися слуховими органами людини та інших живих істот. Зокрема, людина сприймає акустичні коливання у діапазоні частот від 20 до 20000 Гц. Цей діапазон є звуковим діапазоном частот. Крім звукового, розділяють інфразвуковий (від 0 до 20 Гц) та ультразвуковий (вище 20000 Гц) діапазони частот. Ці частоти можуть сприймати окремі види тварин, але люди їх не чують.

Для того, щоб передати звук по каналах зв’язку або запам’ятати у приладах звукозапису, акустичний сигнал необхідно перетворити у адекватний йому електричний сигнал. Для такого перетворення використовується спеціальний перетворювач – мікрофон. Для зворотного перетворення використовується гучномовці.

Принцип перетворення акустичного сигналу в електричний можна показати на прикладі вугільного мікрофону. Мікрофон цього типу побудований на ефекті зміни електричного опору вугільного порошку під дією механічного тиску акустичних коливань на мембрану мікрофону. За своїми характеристиками такі мікрофони поступаються іншим сучасним типам мікрофонів: динамічним, конденсаторним та електретним. Однак принципи дії усіх типів мікрофонів однакові: перетворення під дією

зовнішніх механічних коливань внутрішніх властивостей матеріалів, та в результаті – зміна їх електричних характеристик.

Мікрофони є обов'язковою складовою всіх засобів зняття акустичної інформації. Але багато інших елементів різних електричних та електронних приладів можуть бути використані для зняття акустичної інформації за рахунок акустично-електричних перетворень, що виникають за рахунок так званого «мікрофонного ефекту».

Принцип виникнення цього ефекту можна пояснити на прикладі звичайного телефону. Відомо, що на телефон від лінії подається постійний струм з напругою 45 В. Також відомо, що у вхідному каскаді телефону завжди є трансформатор, що підключається до цієї лінії. Сам телефон знаходиться у середовищі повітря, отже на трансформатор діють акустичні сигнали розмов, що ведуться у приміщенні, де цей телефон знаходиться (при цьому по телефону у цей час розмови можуть не вестись). Акустичні хвилі тиснуть на феритовий сердечник трансформатора, що викликає у ньому появу змінного магнітного поля внаслідок ефекту Віларі. Ефект Віларі пов'язаний з явищем зворотної магнітострикції. Магнітострикція – це зміна форми або розмірів тіл (наприклад, нікелю, легованого залізонікелевого, залізокобальтового або залізоалюмінієвого сплавів, нікелевого фериту тощо) при намагнічуванні й розмагнічуванні їх, що викликана зміною взаємозв'язків між атомами в кристалічній ґратці (саме внаслідок явища магнітострикції гудуть трансформатори). Існує також і зворотний ефект (ефект Віларі) – поява змінного магнітного поля при зміні форми або розмірів таких тіл.

Поява змінного магнітного поля призводить до виникнення змінного струму в обмотках трансформатора за рахунок явища самоіндукції у відповідності до законів Фарадея та Ленца. А цей струм можна зняти безпосередньо з телефонної лінії, підключеної до телефонного апарату.

Крім того, акустичні хвилі тиснуть на обмотки трансформатора, що викликає у них зміну величини паразитної міжвиткової ємності. Це, у свою

чергу, призводять до зміни власної резонансної частоти обмоток трансформатора. Такі ж ефекти виникають при дії акустичного сигналу на будь-які котушки індуктивності. Слід додати, що уникнути наявності паразитної міжвиткової ємності та власної резонансної частоти у індуктивностях неможливо, оскільки вони є фізичними властивостями таких елементів.

Всі ці зміни відбуваються з частотою акустичного сигналу, що діє на згадані елементи, та пропорційно рівню його тиску. Отже, всі розмови у кімнаті можна зняти користуючись «мікрофонним ефектом» та ефектом зміни власної резонансної частоти, що виникають на трансформаторах або котушках індуктивності будь-якого технічного засобу, де вони використовуються.

Зрозуміло, що для зняття інформації з використанням цих ефектів необхідно користуватися спеціальною апаратурою технічної розвідки.

2. Радіотехнічний канал.

Головною особливістю радіозв'язку є використання процесу модуляції для передавання інформаційних (корисних) сигналів. Його сутність полягає у тому, що для переносу на відстань корисного сигналу використовується сигнал-переносник, в якому формуються інформаційний сигнал. У результаті цього процесу (модуляції) утворюються модульовані сигнали, які й випромінюються у ефір. Процес модуляції застосовується для забезпечення передавання низькочастотних інформаційних сигналів з найменшими енергетичними втратами, оскільки високочастотні сигнали-переносники для свого випромінювання та розповсюдження вимагають набагато менших енергетичних витрат, ніж низькочастотні.

Зрозуміло, що частота несучого коливання завжди значно більша, ніж частота інформаційного сигналу.

Існують основні три види модуляції: амплітудна, частотна та фазова. При амплітудній модуляції інформаційний сигнал у модульованому

коливанні проявляється у зміні амплітуди несучого коливання, при частотній – у змінах частоти, при фазовій – у змінах фази.

З переходом на цифрові методи зв'язку використовується також амплітудноімпульсна модуляція, але вона застосовується лише при перетвореннях безперервних сигналів у цифрові та не використовується при випромінюванні радіосигналів у ефір.

Таким чином, у модульованому коливанні присутні всі компоненти інформаційного сигналу, які можна виділити у процесі демодуляції (детектування).

Зазначені властивості утворюють радіотехнічний канал витоку інформації за рахунок паразитних випромінювань та наводок.

Будь-який електронний прилад генерує паразитне випромінювання на суто індивідуальній власній частоті. Це явище викликається численними паразитними ємнісними зв'язками, що обов'язково утворюються між дротами, друкованими струмопроводами, ніжками електрорадіоелементів тощо. При цьому виникають нові паразитні ланцюги, появу яких передбачити неможливо при проектуванні приладів та у процесі їх виробництва. Ці паразитні ланцюги призводять до появи паразитних позитивних зворотних зв'язків, що й перетворює будь-який (навіть низькочастотний) електронний прилад (наприклад, підсилювач) у передавач, що випромінює в ефір паразитні коливання на високих та надвисоких частотах.

При проектуванні та виробництві більшості побутових приладів на ці випромінювання не звертають уваги, оскільки вони не впливають на виконання апаратурою своїх функцій. Лише при проектуванні та виробництві спеціальної та захищеної апаратури цим параметрам приділяється значна увага.

Оскільки такі коливання високочастотні, то вони, не зважаючи на їх малу потужність, можуть розповсюджуватися на сотні метрів. А у зв'язку з тим, що у будь-якій сучасній апаратурі присутні нелінійні елементи

(транзистори та транзисторні мікросхеми), на них відбувається модуляція високочастотного сигналу паразитного випромінювання інформаційними сигналами, що обробляються у приладі.

Крім того, що такі сигнали можуть бути перехоплені з ефіру, вони ще гарантують утворення наводок. Наводка – це сигнал, що утворюється у будь-якій струмопровідній конструкції (наприклад, на трубах центрального опалення) через явище самоіндукції. Тобто, змінне електромагнітне поле (електромагнітна хвиля), падаючи на будь-який нерухомий провідник, викликає в останньому появу змінного струму. А оскільки паразитне випромінювання несе на собі небезпечні сигнали, то їх можна зняти з будь-яких струмопровідних конструкцій та мереж.

Акустичний та радіотехнічний канал у своєї комбінації використовуються при знятті акустичної інформації методом високочастотного нав'язування. Можливість використання цього методу заснована на явищі резонансу у резонансному контурі. Отже, цей метод може використовуватися для зняття інформації з будь-якого елемента, що має власну резонансну частоту. Таким елементом може бути спеціальна порожнина у елементі конструкції або предметі інтер'єру, яка виконує роль пасивного акустичного резонатора. Цей резонатор опромінюється зовнішнім радіосигналом стабільної високої частоти, що відповідає власній резонансній частоті резонатора. Під дією акустичних хвилі резонансна частота резонатора змінюється і відбитий високочастотний сигнал стає модульованим акустичним сигналом.

3. Оптичний канал

Оптичний канал витоку інформації утворюється безпосереднім сприйняттям оком людини навколишнього оточення шляхом застосування спеціальних технічних засобів, що розширюють можливості органа зору в умовах недостатньої освітленості, великій відстані до об'єктів спостереження й недостатності кутового огляду. Це й звичайне підглядання із сусіднього

будинку через бінокль, і реєстрація випромінювання різних оптичних датчиків у видимому або інфрачервоному діапазоні, яке може бути модульоване корисною інформацією.

Одержання видових характеристик об'єкта є результатом розв'язання трьох завдань:

а) виявлення – це стадія зорового сприйняття, коли спостерігач виділяє з навколишнього тла об'єкт, характер якого залишається для нього неясним;

б) розрізнення – коли спостерігач здатний визначити великі деталі об'єкта, роздільно сприймати два об'єкти, розташовані поруч;

в) розпізнання (ідентифікація) – коли спостерігач, розрізняючи окремі дрібні деталі, виділяє істотні ознаки об'єкта й може відрізнити цей об'єкт від інших, наявних у його поле зору.

Видові характеристики об'єктів спостереження можуть бути отримані або безпосереднє у світловому діапазоні, або шляхом візуалізації зображень в інфрачервоному діапазоні, радіолокаційному діапазоні, за рахунок теплового випромінювання об'єктів.

Можливість утворення оптичного каналу витоку інформації залежить від певних психофізіологічних особливостей сприйняття спостерігачем об'єкта, таких, як: 1) кутові розміри об'єкта; 2) рівні адаптаційної яскравості; 3) контраст між об'єктом та фоном; 4) час сприйняття; 5) зашумленність зображення.

Будь-яке зображення характеризується контрастом – прямим або зворотним. При прямому контрасті яскравість фона більше яскравості об'єкта, при зворотному – навпаки. Контраст може виражатися у відносних одиницях або відсотках. Контраст до 20% розглядається як малий, до 50% – як середній і більш 50% – як високий.

Оптимальним при тривалому спостереженні є контраст зображення 85-90%. Мінімальне значення, при якому око розрізняє об'єкт (поріг контрастної чутливості), рівний 2-3% у випадку, коли точно відомий напрямок на об'єкт, і 7-9% при нефіксованому спостереженні.

Визначальними при візуальних характеристиках є також кутові розміри об’єкта спостереження. Абсолютний поріг візуального виявлення об’єктів у більшості людей становить 0,5" (тонка чорна лінія на світлому фоні).

Істотний вплив на одержання візуальної інформації виявляє стан середовища спостереження – від чистого повітря до дуже сильного туману, що відповідає по метеорологічному коду від 10 до 0, що визначає метеорологічну дальність можливого виявлення й спостереження об’єктів.

Використовуючи особливості різних технічних каналів витоку інформації на сьогодні розроблені та використовуються на практиці різноманітні способи та засоби зняття інформації з цих каналів. В залежності від особливостей розташування та облаштування об’єкту, що охороняється, можливо використання різних каналів витоку. При цьому можуть використовуватися різні види перетворення та способи і засоби перенесення інформації. Наприклад, акустичну інформацію можна зняти в приміщенні за допомогою радіомікрофону, який живиться від струму електромережі, а можна виконати цю операцію за допомогою дротового мікрофону, який також підключено до електромережі. В цьому випадку інформація буде передаватися електромережею і її можна зняти навіть на трансформаторній підстанції.

Для зняття акустичної інформації з закритого приміщення дедалі частіше використовується метод високочастотного нав’язування, коли для зняття інформації використовується спеціальне обладнання та заздалегідь підготовлені резонансні елементи в приміщенні, які мають вигляд звичайних побутових речей (картини, естампи, елементи декору, меблі тощо). Крім того, в закритих приміщеннях акустичну інформацію можна знімати за рахунок того, що будівельні конструкції (стіни, підлоги, стелі, вікна, труби, зачинені двері) є по суті акустичними мембранами та чудово передають звукові коливання. Таким чином, за допомогою віброперетворювача та підсилювача можна знімати акустичний сигнал з будь-якого приміщення через стіну, підлогу або стелю.

На відстані акустичний сигнал можна зняти з зачинених вікон, спрямувавши випромінювання лазеру на скло чи скористувавшись спрямованим мікрофоном.

Акустичну інформацію можна знімати також з побутових приладів та апаратури зв'язку. В цьому контексті особливо небезпечним приладом є телефон. Наявність незахищеного телефонного апарату в режимному приміщенні дає змогу прослухувати в ньому всю акустичну інформацію навіть без використання ніякої спецтехніки. Завдяки мікрофонному ефекту електричний сигнал, модульований акустичними сигналами з приміщення, можна зняти з дротів телефонної мережі за допомогою простого пристрою.

Мають свої резонансні контури та мембранні елементи інші побутові прилади: кондиціонери, оргтехніка. В цьому випадку акустичну інформацію можна зняти з електричної мережі, до якої вони підключені.

До того ж, незахищена оргтехніка надає можливість знімати електронну чи електромагнітну інформацію з неї (тобто фактично викрадати будь-які документи, що створюються, передаються та зберігаються у незахищених засобах електронної обробки інформації), використовуючи радіотехнічні канали витоку, наприклад, паразитні електромагнітні випромінювання та наведення.

Не дивлячись на незначний рівень цих паразитних сигналів, сучасна чутлива апаратура дозволяє їх перехоплювати на відносно значних відстанях (кількасот метрів) від їх джерела. Наприклад, таку апаратуру може бути розміщено в легковому автомобілі, який знаходиться на стоянці поряд з об'єктом, де обробляється інформація. При перехопленні за допомогою стаціонарних потужних засобів, які розміщаються, як правило, у дипломатичних представництвах або інших стаціонарних об'єктах розвідки та контррозвідки, перехопленням може бути охоплено великий регіон.

Для перехоплення інформації з радіоефіру використовуються так звані панорамні радіоприймачі (в разі роботи на стаціонарному розвідувальному об'єкті) та малогабаритні сканери (для роботи на рухомому об'єкті). Ці

прилади мають багато різних функцій та здатні приймати сигнали з різними видами модуляції, слідкувати за частотою станції, працювати під керуванням комп'ютера тощо.

Для зняття інформації, яка наводиться на струмопровідні конструкції приміщення, використовуються спеціальні приймачі наводок, що побудовані за принципом частотно-селективного підсилювача з великим коефіцієнтом підсилення та, відповідно, значним динамічним діапазоном. При обробці отриманої таким чином інформації для підвищення співвідношення сигнал/завада використовують апаратуру спектральної обробки сигналів.

Письмова інформація з документів, які знаходяться в приміщенні, може бути отримана у двох видах: як оптична і як електронна.

Електронна інформація може бути отримана шляхом зняття з ліній зв'язку (факсимільний зв'язок чи електронна пошта), або перехопленням каналами паразитних випромінювань та наводок (наприклад, дисплей комп'ютера, який, до речі, має найбільший рівень паразитного випромінювання). В електронному вигляді письмову інформацію можна також отримати шляхом копіювання магнітних чи оптичних носіїв, або копіювання шляхом зняття з паперового документа електронної копії на сканері. Оптична інформація може бути отримана шляхом використання прихованих телекамер, які можуть працювати або у інфрачервоному, або у діапазоні видимих хвиль.

Крім того, можуть бути використані фотоапарати, копіювання шляхом зняття ксерокопій.

Для зняття оптичної інформації використовуються оптичні та електронно-оптичні пристрої. Серед оптичних пристроїв слід відзначити біноклі, фотоапарати, підзорні труби, кінокамери, тобто засоби прямого оптичного спостереження та фіксації оптичної інформації без застосування електронних приладів. Серед оптично-електронних приладів слід відзначити відео- та телекамери, цифрові фотоапарати, прилади нічного бачення, інфрачервоні приціли, лазерні прилади спостереження та лазерні приціли.

Сучасні можливості несанкціонованого одержання інформації з оптичного каналу винятково важливі. Так, наприклад, довгофокусні фотоапарати дозволяють здійснювати зйомку документів, розташованих на стіні офісу або столі, на відстані до 5 км. Телескоп РК 6500, виконаний за схемою Шмидта, дозволяє пізнавати автомобіль на відстані 10 км.

Мініатюрні фотоапарати у звичайному виконанні або закамуфльовані під різні побутові предмети (наручний годинник, запальнички й т.п.), у тому числі з дистанційним керуванням, дозволяють знімати копії з документів формату А4 - А6 у кількостях до 1000 документів.

Поява й широке використання світловодів дозволили отримати принципово нові прилади візуального спостереження. З'явилася можливість одержання інформації із замкнених приміщень, коли зонд пропускається в замкову щілину або отвір у стіні, і його поворот забезпечує візуальний огляд усередині приміщення.

Для захисту інформації від витоку технічними каналами вживають низку заходів, зміст яких залежить від того які, по-перше, види інформації необхідно захистити та, по-друге, у яких приміщеннях об'єкту циркулює ця інформація.

Якщо це лише один вид інформації, що може циркулювати в одному або групі приміщень будівлі, виконують лише заходи з захисту цього виду інформації та певних приміщень. Якщо треба захищати велику кількість приміщень (велику група, яка, наприклад, складається з підгруп), об'єкт захисту може складатися зі всієї будівлі. Якщо необхідно захистити декілька видів інформації, що циркулює у приміщеннях об'єкту, то використовується комплексний захист інформації. Також необхідно враховувати ступінь таємності інформації, що підлягає захисту.

Крім того, обов'язково необхідно враховувати загрози для інформації з боку потенційного супротивника.

Загроза для інформації – це виток, можливість блокування або порушення цілісності інформації, які можуть здійснюватися під час

використання технічних засобів, недосконалих з точки зору захисту інформації, або через інші канали витоку інформації.

Також слід пам'ятати, що для кожного виду інформації та кожного виду загроз існують цілком конкретні засоби захисту та способи їх застосування. Отже, треба користуватися тими системами та засобами захисту, що найбільш повно відповідають потенційним загрозам для кожного з видів інформації, яку слід захищати на конкретному об'єкті.

У разі комплексного захисту інформації необхідно розробляти підсистеми захисту для кожного окремого виду інформації, обов'язково пов'язавши їх у комплексну систему.

На загальному рівні технічний захист інформації реалізується двома основними методами: пасивним та активним.

Активний захист пов'язаний із постановкою перешкод для зняття інформації шляхом випромінювання завад у канал витоку, при чому рівень таких завад повинен перевищувати рівень небезпечних сигналів, які можна зняти з каналів витоку. До активного захисту також відносяться методи протидії, що засновані на постійному контролі середовища розповсюдження небезпечних сигналів за допомогою відповідних технічних пристроїв, які дозволяють виявляти спроби зняття інформації, здійснювати їх пошук та знешкодження.

Пасивний захист побудовано на зниженні спроможності певного технічного джерела витоку або середи розповсюдження небезпечних сигналів до передачі інформації шляхом технічних змін його властивостей, наприклад, шляхом екранування електромагнітного випромінювання.

Слід відзначити, що пасивні методи захисту не використовують фізичних процесів, які шкідливі для здоров'я оточуючих та заважають повсякденній діяльності людей. Однак у більшості випадків застосування активних методів захисту є необхідним, які разом з пасивними методами захисту забезпечують потрібний ступень рівня технічного захисту інформації.

Розглянемо основні способи та засоби захисту від витоку інформації на різних технічних каналах.

1. Акустичний канал

Захиститися від витоку акустичної інформації через зачинені вікна та через стіни, стелю й підлогу можна при застосуванні спеціальних генераторів випадкових або псевдовипадкових електричних коливань. Такі генератори створюють випадковий або псевдовипадковий електричний сигнал і перетворює його в механічні та акустичні коливання. Механічні перетворювачі генераторів розміщують на склі, стінах, підлозі й стелях. Перед цим з'ясовують можливість зняття інформації з суміжних приміщень (тобто можливість проникнення в суміжні приміщення сторонніх осіб). Захищати вікна в приміщеннях необхідно у тих випадках, коли вони виходять на незахищений простір, якщо охоронна зона (відстань від вікна до периметру охорони) не перевищує 200 м. Серед пристроїв подібного типу можна відзначити генератори «ANG-2000» (США), «РІАС-2ГС» (Україна). Акустичні перетворювачі забезпечують випромінювання у повітря приміщення акустичного шуму, що є акустичною завадою для небезпечних акустичних сигналів.

При роботі подібних генераторів вести розмову дуже неприємно, бо шум, що випромінюється, заважає розмовляти. Тому існують також комбіновані генератори, які побудовані на принципі: завада не повинна заважати тому, хто її використовує. Прикладом такого генератора є «Базальт-4ГА» (Україна, НДІ «Квант»). Цей пристрій в процесі своєї роботи використовує змішану заваду, яка складається з тихої музики, шуму та голосових сигналів декількох учасників розмови, які зсунуті у часі та інвертовані по спектру.

Для захисту від витоку акустичної інформації через мікрофони, що негласно встановлені в приміщення, може бути використаний метод «завантаження» їх мембран. Він передбачає випромінювання у повітря

акустичної завади у вигляді модульованих ультразвукових сигналів високого рівня, які діють на мембрану мікрофону з таким тиском, що інші акустичні коливання меншого рівня мікрофонами не сприймаються. До недоліків такого методу захисту слід віднести шкідливий вплив на людину та зовнішнє середовище ультразвукових коливань високого рівня та дуже швидке затухання таких коливань у повітрі.

Для захисту телефонного каналу використовуються декілька типів пристроїв. По-перше, для убезпечення витоку інформації через «мікрофонний ефект» при покладеній телефонній слухавці використовують спеціальні фільтри, що вмикаються у розрив ланцюга між телефонним апаратом та телефонною розеткою. Вони не дають змогу не перепускати через прилад електричні сигнали малої амплітуди, які виникають у дзвінковому ланцюзі за рахунок «мікрофонного ефекту». Крім того, окрема складова такого фільтру захищає телефон від зняття інформації методом високочастотного нав'язування на дзвінковий ланцюг. Прикладом подібного пристрою є вітчизняний фільтр «Базальт-31» (Україна).

Значно складніше захиститися від зняття інформації під час розмови по телефону. Для цього використовують другий тип приладів, що реагують на дуже незначні падіння напруги у мережі, що виникають при підключенні додаткових споживачів електричного струму. Прикладом подібного пристрою є вітчизняна розробка «Рікас-16».

Але ніякі прилади, що використовуються з боку одного абонента, не можуть виявити наявність засобів зняття інформації на протилежному кінці лінії, тобто у абонента, з яким ведеться розмова. Тому для надійного захисту телефонних розмов використовується третій тип пристроїв, що створюють телефонні канали, захищені криптографічними методами (скремблери). Найбільш надійними з них є прилади, що використовують вокодери і ліпідери з подальшим шифруванням. Принцип їх роботи полягає у цифровій обробці аналогових сигналів, виявленні та розкладенні слів і звуків на окремі форманти та передачі мови у вигляді попередньо зашифрованому набору

формант. При цьому, ключове слово до шифру може сягати довжини 512 знаків і більше. На розшифрування такої перехопленої розмови, за правило, потрібно багато часу і коштів.

Прикладом таких пристроїв можуть бути прилади «Voice Coder-2400», «Voice Coder-GSM», система захисту телефонних розмов «SEC-STEALTH» та інші.

Зрозуміло, що нормальної роботи апарати криптографічного захисту телефонних розмов повинні бути встановлені з обох кінців лінії зв'язку.

2. Радіотехнічний канал

Одним із напрямів захисту інформації від витоку радіотехнічним каналом є виявлення, пошук та знешкодження радіозакладних пристроїв, тобто, радіомікрофонів, що негласно встановлені в приміщенні для передачі акустичної інформації через радіосигнали.

Основними методами виявлення радіозакладних пристроїв є:

– постійний моніторинг радіоефіру (найбільш ефективний метод);

– періодична перевірка ефіру спеціальними сканерами.

Перший метод полягає у постійній перевірці радіовипромінювань та виявленні нових складових у малюнку спектра шляхом порівняння з попереднім його малюнком. Прикладом такого пристрою є автоматизований комплекс радіомоніторингу і пошуку закладних пристроїв «Акор-3» (Україна).

Другий метод забезпечується відповідними сканерами, які випромінюють в повітря декілька складних акустичних сигналів і контролюють їх відсутність у радіоефірі на різних частотах.

У разі, якщо встановлено наявність у приміщенні радіозакладки, для її пошуку використовують спеціальні індикатори поля, які сигналізують про наявність джерела випромінювання на близьких відстанях (до 25 см від антени) і, таким чином, дають можливість встановити місце розташування

радіозакладки. Прикладом такого пристрою є виріб «РТ-025» фірми «Optoelectronics».

Іншим напрямом захисту інформації від витоку радіотехнічним каналом є використання спеціальних генераторів шуму з метою постановки радіотехнічної завади. Подібні пристрої також застосовують для блокування радіовибухових мін під час розмінування. Прикладом подібних генераторів може бути серія виробів фірми «РІАС» (Україна).

Для захисту від паразитного електромагнітного випромінення та наводу (ПЕМВН) використовуються наступні методи:

– екранування ПЕМВН;
– маскування сигналів від ПЕМВН (генератори шуму);
– застосування спеціальних ланцюгів заземлення;
– використання спеціальних джерел електроживлення;
– використання спеціальних фільтрів у джерелах електроживлення.

Подібні методи вимагають складного технологічного обладнання. Наприклад, екранування комп'ютерної техніки здійснюється через напилення тонких захисних шарів металу шляхом осадження у вакуумі. Для маскування використовуються генератори широкосмугового шуму. У приміщенні встановлюється спеціальний генератор випадкових електромагнітних коливань для протидії ПЕМВН. Прикладом подібного генератору може бути прилад типу «Базальт» (Україна).

3. Оптичний канал

Основними засобами захисту від витоку інформації оптичним каналом є захист від зняття через вікна за допомогою фотоапаратів та відеокамер із спеціальними довгофокусними об'єктивами, а також від зняття інформації за допомогою відеокамер, розміщених у приміщенні.

Захист від оптичного зняття інформації через вікна досягається або використанням спеціального скла (матового чи з нерівностями, що робить

неможливим перегляд приміщення), або застосуванням штор та спеціальних плівок, які наклеюють на скло.

Захист від відеокамер, які негласно встановлені всередині приміщення, досягається використанням приладів, що ставлять активну заваду роботі електронних приладів (що не завжди можливо), або пошуком, виявленням та знешкодженням таких пристроїв. При цьому, пошук відеокамер здійснюється тими самими приладами та за тією ж самою методикою, що і пошук радіозакладних пристроїв.

6.3 Захист інформації від несанкціонованого доступу

Несанкціонований доступ до інформації – це такий доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу.

При цьому, в залежності від типу носія інформації (документ, файл, людина тощо) йдеться як про фізичний доступ до носіїв інформації, так і опосередкований доступ до інформації через технічні засоби – елементи інформаційної системи, за допомогою яких інформація зберігається або оброблюється. Головна ознака несанкціонованого доступу – порушення політики розмежування доступу, що встановлена в інформаційній системі.

Несанкціонований доступ може здійснюватися на різних рівнях інформаційної системи:

– на рівні периметру інформаційної системи;

– на рівні комунікаційного обладнання;

– на рівні апаратної частини серверів і робочих станцій;

– на рівні системного й прикладного програмного забезпечення.

Розглянемо основні заходи і засоби для захисту від несанкціонованого доступу на вказаних рівнях інформаційної системи.

1. Захист на рівні периметра інформаційної системи.

Для захисту від несанкціонованого доступу на рівні периметра інформаційної системи використовуються:

– системи охоронної й пожежної сигналізації;

– системи цифрового відеоспостереження;

– системи контролю й керування доступом.

Основою сучасних систем охоронної сигналізації є різні типи датчиків: 1) акустичні – що спрацьовують при різких характерних звуках в приміщенні; 2) інфрачервоні – що реагують на рух; 3) вібраційні – що фіксують пересування, механічний вплив на предмети та інше; 4) геркони – що аналізують зміни магнітного поля і попереджають про розгерметизацію сейфа, злам об'єкта, відкриття дверей, вікон та тощо.

В залежності від інформації, що надається датчиками, виділяють три підвиди охоронної сигналізації:

1) Індивідуальна GSM-охоронна сигналізація.

Відправляє сигнал датчиків на номер мобільного телефону за допомогою СМС, ММС або телефонного дзвінка, а також включає звукове та світлове сповіщення. Недоліки: потенційні порушники за допомогою спеціального обладнання можуть заглушити GSM-сигналізацію. Переваги: гнучкість налаштування і бюджетна вартість.

2) Автономна охоронна сигналізація.

Сигнал тривоги нікуди не передає, проте запускає світлові і звукові сповіщувачі для привертання уваги до проблемного об'єкту. Недоліки: можливість пошкодження сигнальних проводів, необхідність перебування на об'єкті охорони для реагування, необхідність періодичного моніторингу стану датчиків. Переваги: невелика ціна.

3) Пультова охоронна сигналізація.

Включає звукове та світлове сповіщення, а також відправлення через зашифрований канал сигналів від датчиків на центральний пульт охорони. Недоліки: порівняно висока вартість. Переваги: своєчасне реагування на тривожний сигнал групою тренованих охоронців, постійний моніторинг стану датчиків.

Конструктивно до складу охоронної сигналізації, як правило, входять: 1) набір різних датчиків (датчики руху, розбиття, вібрації, відкриття (геркони), температури, комбіновані, кнопки тривоги тощо); 2) набір інфрачервоних бар'єрів для охорони периметру (встановлюються на відстані від 5 до 100 м у зоні прямої видимості, працюють як приймач і передавач, як правило, багатопроменеві); 3) пристрої світлового та звукового сповіщення (сирени, світлові табло тощо); 4) GSM-комплекти (для сповіщення та керування засобами мобільного зв'язку); 5) централі та пульти (прибори приймально-контрольні) для об'єднання периферійних пристроїв в єдину систему.

Системи пожежної сигналізації за своєю побудовою подібні до систем охоронної сигналізації. Вони складаються також із різних датчиків, пристроїв світлового та звукового сповіщення, централей та пультів.

Різниця між двома типами систем (охоронної та пожежної сигналізації) полягає у датчиках. В системах пожежної сигналізації використовуються датчику газу (напівпровідникові на принципі іонізації або інфрачервоні на принципі аналізу спектру), датчики диму (оптико-електронні або радіоізотопні), датчики полум'я (інфрачервоні або ультрафіолетові), теплові датчики (максимальні, що спрацьовують при збільшенні максимального обмеження температури, або диференціальні, що спрацьовують при збільшенні швидкості зростання температури) та ручні сповіщувачі.

Система відеоспостереження – це система передавання інформації з відеокамер, телевізійних камер на обмежену кількість моніторів та / або пристроїв запису. Бувають цифрові та аналогові, дротові та бездротові, безперервні та ті, що спрацьовують на подію. Стандартна система відеоспостереження складається з наступних елементів: 1) набору відеокамер; 2) відеореєстратора (центральний блок системи, який з'єднує периферійні пристрої; 3) монітора; 4) додаткових датчиків.

Відеокамери, що використовуються у системах відеоспостереження, характеризуються типом корпусу (модульна, пальчикова, купольна, типу

«відеооко», пін-хол, антивандальна, вулична, роботизовано тощо), технологією передачі даних камер до відеореєстратора (потокова або пакетна), роздільною здатністю (540-600 телевізійних ліній для аналогових, 288-1080 для цифрових), чутливістю до світла, кутом огляду (фокусом об'єктива), кольором, наявністю інфрачервоного підсвітлення, функціями день-ніч, фільтрації шумів, стабілізації зображення тощо.

Відеореєстратори характеризуються типом (комп'ютерні – на базі персонального комп'ютера та операційної системи або одноплатні DVR), кількістю відеоканалів (4, 8, 16, 24, 32), швидкістю запису (від 4-6 кадрів за секунду до 25 і більше), кількістю одночасних операцій (дуплексні, триплесні, пентаплексні), обсягом пам'яті на жорсткому диску тощо.

Система контролю і керування доступом – це комплекс технічних та програмних засобів безпеки, що здійснює регулювання входу / виходу та переміщень людей чи транспортних об'єктів на територіях, які знаходяться під охороною, для адміністративного моніторингу та попереджень несанкціонованого проникнення на територію, що охороняється.

За допомогою подібних систем також досягається: 1) ідентифікація осіб, що мають право доступу в зону, що охороняється; 2) розмежування доступу до різних приміщень; 3) керування автоматичними режимами доступу; 4) реєстрація часу перебування особи на об'єкті; 5) обробка інформації та ведення статистики.

Система контролю і керування доступом, як правило, складається з ідентифікаторів (ключовий елемент, що встановлює право доступу особи на контрольну територію), зчитувальних пристроїв (залежать від типу ідентифікатора), контролера із власним джерелом резервного живлення (може працювати автономно або разом з іншими контролерами під керуванням головного комп'ютера), додаткового обладнання (датчики, кнопки виходу, турнікети, електронні замки, механізми доведення дверей, пристрої світлового та звукового сповіщення, відповідне програмне забезпечення тощо).

Ключовим елементом системи є ідентифікатор, що встановлює право доступу особи на контрольну територію. В якості такого ідентифікатора можуть використовуватися карти з магнітною смужкою, безконтактні карти, спеціальні брелоки, цифрові коди для введення з клавіатури, унікальні особисті ознаки людини (відбитки пальця, відбитки долоні, малюнок сітківки ока тощо).

Розрізняють централізовані та автономні системи контролю й керування доступом. В централізованих системах контролери об'єднано в єдину мережу та підключено до головного комп'ютера, що здійснює загальне керування. Як правило, подібні системи входять до складу вже наявних систем: відеоспостереження, пожежної та охоронної сигналізації. Встановлюються переважно у великих організаціях. Автономні системи самостійно керують роботою периферійних елементів та контролюють точки доступу. Як правило, вони встановлюються на окремі невеликі приміщення (наприклад, доступ до банкомату), в малих організаціях, в приватних будинках тощо.

2. Захист на рівні комунікаційного обладнання.

На рівні комунікаційного обладнання від несанкціонованого доступу використовуються наступні засоби мережевого захисту інформації:

– міжмережеві екрани (Firewall) – для блокування атак із зовнішнього середовища;

– системи виявлення вторгнень (IDS – Intrusion Detection System) – для виявлення спроб несанкціонованого доступу як ззовні, так і усередині мережі, захисту від атак типу «відмова в обслуговуванні»;

– засоби створення віртуальних приватних мереж (VPN – Virtual Private Network) – для організації захищених каналів передачі даних через незахищене середовище;

– засоби аналізу захищеності – для аналізу захищеності локальної мережі й виявлення можливих каналів несанкціонованого доступу до інформації.

Міжмережевий екран або фаєрвол (Firewall – вогняна стіна) – пристрій або набір пристроїв, які налаштовані для керування комп'ютерним мережевим трафіком між областями різного рівня безпеки згідно з набором правил та інших встановлених критеріїв. Як правило, міжмережеві екрани встановлюються на вході мережі й розділяють внутрішню її частку і зовнішню. Прикладами подібних пристроїв можуть бути продукти Cisco PIX Firewall, Symantec Enterprise FirewallTM, Contivity Secure Gateway, Alteon Switched Firewall тощо).

В залежності від виконання фаєрвол може бути у вигляді окремого приладу (так званий маршрутизатор або роутер), або у вигляді окремої програми, що встановлюється на персональний комп'ютер чи на серверну станцію. Простий та дешевий фаєрвол може не мати такої гнучкої системи налаштувань правил фільтрації пакетів та трансляції адрес вхідного та вихідного трафіку.

В залежності від активних з'єднань, що відслідковуються, фаєрволи розділяють на пристрої:

– з простою фільтрацією (stateless), які не відслідковують поточні з'єднання (наприклад, TCP), а фільтрують потік даних виключно на основі статичних правил;

– з фільтрацією з урахуванням контексту (stateful), які відслідковують поточні з'єднання та пропускають лише такі мережеві пакети, що задовольняють логіці й алгоритмам роботи відповідних протоколів та програм. Такі типи міжмережевих екранів дозволяють ефективніше боротися з різноманітними DDoS-атаками та вразливістю деяких мережевих протоколів.

В залежності від рівня роботи у стеку мережевих протоколів фаєрволи можуть бути мережевого рівня, прикладного рівня або рівня з'єднання.

Кожен з цих трьох типів використовує свій, відмінний від інших, підхід до захисту комп'ютерної мережі.

Фаєрвол мережевого рівня представлений екрануючим маршрутизатором. Він контролює лише дані мережевого і транспортного рівнів моделі OSI. Мінусом таких маршрутизаторів є те, що інші п'ять рівнів залишаються неконтрольованими. У більшості таких приладів відсутні механізми аудиту та подачі сигналу тривоги. Іншими словами, маршрутизатори можуть піддаватися атакам і відбивати велику їх кількість, а адміністратори навіть не будуть про це проінформовані.

Фаєрвол прикладного рівня відомий як проксі-сервер (сервер-посередник). Такі фаєрволи встановлюють певний фізичний поділ між локальною мережею і зовнішньою мережею, тому вони відповідають найвищим вимогам безпеки. Однак, оскільки програма повинна аналізувати пакети і приймати рішення щодо контролю доступу до них, фаєрволи прикладного рівня неминуче зменшують продуктивність (пропускну здатність) комп'ютерної мережі, тому в якості проксі-сервера необхідно використовувати достатньо швидкі й недешеві комп'ютери.

Фаєрвол рівня з'єднання схожий на фаєрвол прикладного рівня тим, що обидва вони є серверами-посередниками. Відмінність полягає в тому, що фаєрволи прикладного рівня вимагають спеціального програмного забезпечення для кожної мережевої служби на зразок FTP або HTTP. Натомість, фаєрволи рівня з'єднання обслуговують велику кількість різноманітних протоколів.

Маршрутизатор, або роутер (англ. router) – електронний пристрій, що використовується для поєднання двох або більше різних мереж і керування процесом маршрутизації між ними. Тобто, на підставі інформації про топологію мережі та певних правил маршрутизатор приймає рішення про пересилання пакетів мережевого рівня (рівень 3 в моделі OSI) між різними сегментами мережі. Для того, щоб надсилати пакети в потрібному напрямку, маршрутизатор використовує таблицю маршрутизації, яка зберігається у його

пам’яті. Таблиця маршрутизації може складатися засобами статичної або динамічної маршрутизації. Часто маршрутизатор не обмежується простим пересиланням даних між різними мережами, а також виконує й інші функції: захищає локальну мережу від зовнішніх загроз, обмежує доступ користувачів локальної мережі до ресурсів Інтернет, роздає IP-адреси, шифрує трафік тощо.

Маршрутизатором може бути як спеціалізований апаратний пристрій (наприклад – продукція компанії Cisco), так і звичайний комп’ютер, що виконує функції маршрутизатора. Існує кілька пакетів програмного забезпечення (в основному на основі ядра ОС Linux), за допомогою якого можна перетворити персональний комп’ютер на високопродуктивний і багатофункціональний маршрутизатор (наприклад, програмний пакет GNU Zebra).

Серед додаткових функцій маршрутизатора можна навести такі можливості, як контроль доступу, фільтрація портів, фільтрація змісту, перенаправлення портів, підтримка віртуальних серверів, блокування протоколів, створення віртуальних приватних мереж, підтримка серверу автоматичного налаштування мережі DHCP, підтримка серверу системи доменних імен DNS, підтримка серверу друку, функції віддаленого керування мережею, ведення журналу мережевих подій, підтримки IP-телефонії тощо.

Проксі-сервер (від англ. proxy – «представник, уповноважений») – сервер (комп’ютерна система або програма) в комп’ютерних мережах, що дозволяє клієнтам виконувати непрямі (через посередництво проксі-сервера) запити до мережевих сервісів. Спочатку клієнт з’єднується з проксі-сервером і запитує який-небудь ресурс (наприклад, поштовий e-mail), розташований на іншому сервері. Потім проксі-сервер або підключається до вказаного сервера і отримує ресурс у нього, або повертає ресурс з власного кешу (у випадках, якщо проксі має свій кеш). У деяких випадках запит клієнта або відповідь сервера може бути змінена проксі-сервером з певною метою. Також проксі-

сервер дозволяє захищати клієнтський комп'ютер від деяких мережевих атак і допомагає зберігати анонімність клієнта.

Найчастіше проксі-сервери застосовуються для:

– забезпечення доступу з комп'ютерів локальної мережі в Інтернет;

– кешування даних, тобто у випадках, якщо часто відбуваються звернення до одних і тих же зовнішніх ресурсів, то можна тримати їх копію на проксі-сервері та видавати за запитом, знижуючи тим самим навантаження на канал у зовнішню мережу і прискорюючи отримання клієнтом потрібної інформації;

– стиснення даних;

– захист локальної мережі від зовнішнього доступу (наприклад, можна налаштувати проксі-сервер так, що локальні комп'ютери будуть звертатися до зовнішніх ресурсів тільки через нього, а зовнішні комп'ютери не зможуть звертатися до локальних взагалі, оскільки будуть бачити лише проксі-сервер);

– обмеження доступу з локальної мережі до зовнішньої (наприклад, можна заборонити доступ до певних веб-сайтів, обмежити використання Інтернет якимось локальним користувачам, встановлювати квоти на трафік або смугу пропускання, фільтрувати рекламу і віруси);

– анонімізації доступу до різних ресурсів тощо.

В залежності від способу організації роботи розрізняють наступні види проксі-серверів:

– відкритий проксі-сервер, до якого може отримати доступ будь-який користувач мережі Інтернет;

– прозорий проксі-сервер, до якого увесь трафік або певна його частина перенаправляється неявно;

– зворотній проксі-сервер, який на відміну від прямого, ретранслює запити клієнтів із зовнішньої мережі на один або декілька серверів, логічно розташованих у внутрішній мережі (часто використовується для балансування мережевого навантаження між декількома веб-серверами і

підвищення їх безпеки, граючи при цьому роль міжмережевого екрану на прикладному рівні).

Прикладами проксі-серверів є програмні пакети 3proxy (BSD, багатоплатформений), CoolProxy (Windows, платний), HandyCache (Windows, безкоштовний для домашнього використання), Kerio Control (Windows, Linux, платний), Squid (багатоплатформений, безкоштовний), TOR (багатоплатформений, платний) та інші.

Система виявлення вторгнень (Intrusion Detection System – IDS) – програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу до комп'ютерної системи або мережі, в тому числі несанкціонованого керування ними. Системи виявлення вторгнень забезпечують додатковий рівень захисту комп'ютерних систем разом з системою запобігання вторгненням (IPS — англ. Intrusion Prevention System).

Використовуючи спеціальні механізми, системи виявлення вторгнень здатні запобігати шкідливим діям, що дозволяє значно знизити час простою в результаті атаки й витрати на підтримку працездатності мережі. Подібні системи можуть сповістити про початок атаки на мережу, причому деякі з них здатні виявляти атаки, що були раніше невідомими. Вони не обмежуються лише оповіщенням, але й здійснюють певні заходи, спрямовані на блокування атаки (наприклад, розрив з'єднання або виконання програми, заданої адміністратором). На практиці досить часто програмно-апаратні рішення поєднують у собі функціональність двох типів систем (їх об'єднання тоді називають IDPS).

За своїми видами IDS можуть бути:

1) статичними і динамічними;
2) мережевими та системними.

Статичні системи роблять «знімки» (snapshot) середовища та здійснюють їх аналіз, розшукуючи вразливе програмне забезпечення, помилки в конфігураціях, відомі уразливості, слабкі паролі, перевіряючи вміст

спеціальних файлів в каталогах користувачів або конфігурацію відкритих мережевих сервісів. Статичні IDS виявляють сліди вторгнення.

Динамічні IDS здійснюють моніторинг у реальному часі всіх дій, що відбуваються в системі, переглядаючи файли аудиту або мережеві пакети, що передаються за певний проміжок часу. Динамічні IDS дозволяють постійно стежити за безпекою системи.

Мережеві (Network-based IDS, NIDS) контролюють пакети в мережевому середовищі і виявляють спроби зловмисника проникнути всередину системи або реалізувати атаку «відмова в обслуговуванні». Ці IDS працюють з мережевими потоками даних. Типовий приклад NIDS — система, яка контролює велике число TPC-запитів на з'єднання (SYN) з багатьма портами на обраному комп'ютері, виявляючи, таким чином, що хтось намагається здійснити сканування TCP-портів. Мережева IDS може запускатися або на окремому комп'ютері, який контролює свій власний трафік, або на виділеному комп'ютері, що прозоро переглядає весь трафік у мережі (концентратор, маршрутизатор). Мережеві IDS контролюють багато комп'ютерів, тоді як системні IDS контролюють тільки один. Прикладом мережевої IDS є Snort.

Окремо виділяють IDS для бездротових мереж, які перевіряють активність в бездротових мережах. Зокрема, такі системи виявляють точки бездротового доступу до мережі, що невірно налаштовані, атаки типу «людина посередині» (Man-in-middle), сканування MAC-адрес тощо.

Методи роботи систем виявлення вторгнень:

- аналіз сигнатур і протоколів;
- поведінковий аналіз мережі.

Аналіз сигнатур був першим методом, застосованим для виявлення вторгнень. Він базується на простому понятті збігу послідовності зі зразком. У вхідному пакеті проглядається байт за байтом і порівнюється з сигнатурою (підписом), характерною частиною програми, що вказує на характеристику

шкідливого трафіку. Такий підпис може містити ключову фразу або команду, яка пов'язана з нападом. Якщо збіг знайдено, оголошується тривога.

Аналіз протоколів полягає у вивченні окремих полів мережевих протоколів, що використовуються. В цих полях повинні бути очікувані або нормальні значення. Якщо що-небудь порушує ці стандарти, можна говорити про ймовірну зловмисність. IDS переглядає кожне поле всіх протоколів вхідних пакетів: IP, TCP, UDP. Якщо є порушення протоколу, наприклад, якщо він містить несподівані значення в одному з полів, оголошується тривога.

Поведінковий аналіз мережі (Network Behavior Analysis, NBA) аналізує мережевий трафік і ідентифікує нетипові потоки, наприклад DoS і DDoS атаки.

Засоби створення віртуальних приватних мереж забезпечують прозоре для користувача з'єднання локальних мереж, зберігаючи при цьому конфіденційність і цілісність інформації шляхом її динамічного шифрування. Прикладами таких засобів є вироби Symantec Enterprise VPN, Cisco IOS VPN, Cisco VPN concentrator та інші.

Віртуальні приватні мережі (англ. Virtual Private Networking, VPN) надають можливість використовувати загальнодоступні небезпечні мережі, такі як Інтернет, для захищеної передачі даних, використовуючи для цього можливості шифрування і електронно-цифрового підпису. При такому підключенні користувач може працювати з ресурсами віддаленої мережі точно так, як і з ресурсами локальної мережі.

Багато виробників маршрутизаторів почали випускати моделі з підтримкою VPN, починаючи від простого пропускання тунелів VPN, до повноцінних вбудованих серверів PPTP або IPSec. Для створення VPN використовуються такі мережеві протоколи: IPSec (англ. Internet Protocol Security), PPTP (англ. Point-to-Point Tunneling Protocol), L2TP (англ. Layer 2 Tunneling Protocol), SSL.

Технологія VPN дозволяє об'єднати, наприклад, декілька географічно віддалених мереж організації в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів.

Прикладом створення віртуальної мережі є інкапсуляція протоколу PPP в будь-який інший протокол – IP (ця реалізація називається також PPTP — Point-to-Point Tunneling Protocol) або Ethernet (PPPoE). Деякі інші протоколи так само надають можливість формування захищених каналів (SSH).

VPN складається з двох частин: «внутрішня» (підконтрольна) мережа, яких може бути декілька, і «зовнішня» мережа, через яку проходять інкапсульовані з'єднання (зазвичай використовується Інтернет).

Підключення до VPN віддаленого користувача робиться за допомогою сервера доступу, який підключений одночасно як до внутрішньої, так і до зовнішньої (загальнодоступною) мережі. При підключенні віддаленого користувача (або при установці з'єднання з іншою захищеною мережею) сервер доступу вимагає проходження процесу ідентифікації, а потім процесу аутентифікації. Після успішного проходження обох процесів, віддалений користувач (віддалена мережа) наділяється повноваженнями для роботи в мережі, тобто відбувається процес авторизації.

Зазвичай VPN утворюють на рівнях не вище мережевого, так як застосування криптографії на цих рівнях дозволяє використовувати в незмінному вигляді транспортні протоколи (такі як TCP, UDP).

В Україні технологія VPN останнім часом використовується не тільки для створення приватних мереж, але і деякими провайдерами для надання виходу в Інтернет.

Засоби аналізу захищеності локальної мережі дозволяють запобігти можливим атакам на локальну мережу, оптимізувати витрати на захист інформації й контролювати поточний стан захищеності мережі. Прикладами подібних засобів є програмні пакети Symantec Enterprise Security Manager, Symantec NetRecon та інші.

Постійний контроль за роботою локальної мережі, що становить основу будь-якої корпоративної мережі, необхідний для підтримки її в працездатному стані. Зважаючи на важливість цієї функції, її часто відокремлюють від інших функцій систем управління і реалізують спеціальними засобами. Такий поділ функцій контролю і власне управління корисно для невеликих і середніх мереж, для яких установка інтегрованої системи управління економічно недоцільна. Використання автономних засобів контролю допомагає адміністратору мережі виявити проблемні ділянки і налаштування мережі, а їх відключення або зміну конфігурації він може виконувати у цьому випадку вручну.

Процес контролю роботи мережі зазвичай ділять на два етапи: моніторинг і аналіз.

На етапі моніторингу виконується більш проста процедура – збір первинних даних про роботу мережі: статистики про кількість циркулюючих в мережі кадрів і пакетів різних протоколів, стан портів концентраторів, комутаторів і маршрутизаторів тощо.

На етапі аналізу виконується більш складна і інтелектуальна процедура обробки зібраної на етапі моніторингу інформації, порівняння її з даними, отриманими раніше, і формування припущень про можливі причини сповільненої або ненадійної роботи мережі.

Всі засоби моніторингу та аналізу мереж, можна розділити на кілька великих класів:

– системи управління мережею (Network Management Systems);

– засоби управління системою (System Management);

– вбудовані системи діагностики і управління (Embedded Systems);

– аналізатори протоколів (Protocol analyzers);

– обладнання для діагностики і сертифікації кабельних систем.

Системи управління мережею – централізовані програмні системи, які збирають дані про стан вузлів і комунікаційних пристроїв мережі, а також дані про трафік в мережі. Ці системи не тільки здійснюють моніторинг і аналіз, а й виконують в автоматичному чи напівавтоматичному режимі управління мережею – включення і відключення портів пристроїв, зміна параметрів мостів адресних таблиць мостів, комутаторів і маршрутизаторів тощо. Прикладами систем управління можуть служити популярні системи HPOpenView, SunNetManager, IBMNetView.

Засоби управління системою часто виконують функції, аналогічні функціям систем управління, але щодо інших об'єктів. У першому випадку об'єктом управління є програмне і апаратне забезпечення комп'ютерів мережі, а у другому – комунікаційне обладнання. Разом з тим, деякі функції цих двох видів систем управління можуть дублюватися, наприклад, засоби управління системою можуть виконувати найпростіший аналіз мережевого трафіку. До найбільш відомих систем управління системами відносяться LANDesk, IBM Tivoli, Microsoft Systems Management Server, HP OpenView, Novell ZENworks і CA Unicenter.

Вбудовані системи діагностики і управління виконуються у вигляді програмно-апаратних модулів, які встановлюються у комунікаційне обладнання, а також у вигляді програмних модулів, вбудованих в операційні системи. Вони виконують функції діагностики і управління тільки одним пристроєм, і в цьому їх основна відмінність від централізованих систем управління. Прикладом засобів цього класу може служити модуль управління концентратором Distrebuted 5000, який реалізує функції автоматичної сегментації портів при виявленні несправностей, приписування портів внутрішнім сегментам концентратора і деякі інші. Як правило, вбудовані модулі управління також виконують роль SNMP-агентів, які постачають дані про стан пристрою системам управління.

Аналізатори протоколів становлять собою програмні або апаратно-програмні системи, які обмежуються на відміну від систем управління лише

функціями моніторингу і аналізу трафіку в мережах. Сучасний аналізатор протоколів може перехоплювати і декодувати пакети великої кількості протоколів, що використовуються в мережах – зазвичай їх кілька десятків. Аналізатори протоколів дозволяють встановити деякі логічні умови для перехоплення окремих пакетів і виконують повне декодування перехоплених пакетів, тобто показувати в зручній для користувача формі вкладеність пакетів протоколів різних рівнів один в одного з розшифруванням змісту окремих полів кожного пакета.

Обладнання для діагностики і сертифікації кабельних систем умовно можна поділити на чотири основні групи: мережеві монітори, прилади для сертифікації кабельних систем, кабельні сканери і тестери (мультіметри). Мережеві монітори (мережеві аналізатори) призначені для тестування кабелів різних категорій. Вони збирають дані лише про статистичні показники трафіку – середньої інтенсивності загального трафіку мережі, середньої інтенсивності потоку пакетів з певним типом помилки тощо. Призначення пристроїв для сертифікації кабельних систем безпосередньо випливає з їх назви. Сертифікація виконується відповідно до вимог одного з міжнародних стандартів на кабельні системи. Кабельні сканери використовуються для діагностики мідних кабельних систем, а тестери призначені для перевірки кабелів на відсутність фізичного розриву.

3. Захист на рівні апаратного забезпечення.

Для захисту інформації на рівні апаратного забезпечення використовуються апаратні ключі, системи сигналізації та засоби блокування пристроїв і інтерфейсів введення-виведення інформації.

Апаратний ключ (електронний ключ, донгл від англ. dongle) – апаратний засіб, призначений для захисту програмного забезпечення і даних від копіювання, нелегального використання й несанкціонованого поширення.

Основою даної технології є спеціалізована мікросхема, або захищений від зчитування мікроконтролер, що мають унікальні для кожного ключа

алгоритми роботи. Апаратні ключі також мають захищену енергонезалежну пам'ять (як правило, невеликого обсягу), більш складні пристрої можуть мати вбудований криптопроцесор (для апаратної реалізації криптографічних алгоритмів), годинник реального часу. Як правило, вони підключаються до комп'ютера через USB. Прикладом подібного пристрою може бути вітчизняна розробка «Кристал» (Україна, м. Харків).

Алгоритм шифрування може бути секретним або публічним. Секретні алгоритми розробляються самим виробником засобів захисту, у тому числі й індивідуально для кожного замовника. Головним недоліком використання таких алгоритмів є неможливість оцінки криптографічної стійкості. Публічний алгоритм має криптостійкість незрівнянно більшу. Такі алгоритми перевіряються не випадковими людьми, а групою експертів, що спеціалізуються на криптографії і криптоаналізі. Прикладами таких алгоритмів можуть служити широко використовувані алгоритми AES, RSA, Elgamal та інші.

Системи сигналізації для комп'ютера призначені для контролю розкриття його корпуса і можуть використовуватися як додатковий засіб захисту від несанкціонованого доступу.

Робота і принцип дії систем сигналізації аналогічні до звичайної охоронної сигналізації. Як правило, сигналізація складається із плати сигналізації, яка встановлюється в комп'ютер, одного або декількох датчиків розкриття, а також спеціального обладнання постановки на охорону (пульт). Живлення сигналізації здійснюється від автономного джерела. Сигналізація контролює спрацьовування датчиків розкриття й зняття елемента живлення.

В якості елементів сповіщення можуть використовуватися сирена, світлодіоди, GSM-модуль, програмна реалізація через комп'ютерну мережу тощо.

Засоби блокування пристроїв і інтерфейсів вводу-виводу інформації можуть бути використані як додатковий елемент захисту комп'ютерної системи, оскільки не є достатньо надійними. Серед існуючих варіантів

знайшли певне розповсюдження корпуси для персональних комп'ютерів с дверцятами на замках і окремі замки для портів USB.

Наприклад, пристрій USB Security Lock за зовнішнім виглядом нагадує звичайний флеш-накопичувач. З його допомогою можна встановити в USB-порт заглушку, для зняття якої необхідний той же USB Security Lock. Доки заглушка перебуває в порту, підключення в нього інших пристроїв або кабелів фізично неможливе.

4. Захист на рівні системного і прикладного програмного забезпечення.

Для захисту інформації на рівні системного й прикладного програмного забезпечення використовуються:

– системи ідентифікації й аутентифікації;

– системи розмежування доступу до інформації;

– системи аудита й моніторингу;

– системи антивірусного захисту.

Системи ідентифікації й аутентифікації дозволяють розмежувати доступ до інформаційної системи різних категорій користувачів на підставі їх персональної ідентифікації, перевірки достовірності ідентифікатора і подальшого наділення необхідними повноваженнями.

Ідентифікація користувачів полягає у встановленні і закріпленні за кожним із них унікального ідентифікатора у вигляді номера, шифру, коду тощо (персональний ідентифікаційний номер (PIN), соціальний безпечний номер (SSN), особистий номер, код безпеки тощо).

Аутентифікація користувачів полягає в перевірці достовірності користувача за пред'явленим ним ідентифікатором, наприклад, при вході в систему. Така перевірка повинна виключати фальсифікацію користувачів в системі та їх компрометацію. Без перевірки достовірності втрачається сенс в самій ідентифікації користувачів і застосуванні засобів розмежування доступу, побудованих на базі особистих ідентифікаторів.

Авторизація користувачів полягає у наділенні авторизованих користувачів певними повноваженнями в системі в залежності від їх ролі.

Аутентифікація може здійснюватися різними методами і засобами. Нині в автоматизованих системах використовуються три основні способи аутентифікації за наступними ознаками: 1) паролю або особистому ідентифікуючому номеру (користувач «знає»); 2) деякому предметі, який є у користувача (користувач «має»); 3) певними фізіологічним ознакам, властивими конкретній особі (користувач «є»).

Перший спосіб реалізують програмні засоби аутентифікації, що використовуються в більшості операційних систем, систем управління базами даних, мережевих пакетів тощо. Суть цього способу полягає в тому, що кожному зареєстрованому користувачеві видається персональний пароль, який він повинен тримати в таємниці і вводити в автоматизовану систему при кожному зверненні до неї. Спеціальна програма порівнює введений пароль з еталоном, що зберігається в пам'яті, і при збігу паролів запит користувача приймається до виконання.

Простота цього способу очевидна, але очевидні також і його явні недоліки: пароль може бути підібраний перебором можливих комбінацій, а майстерний зловмисник може проникнути в ту область пам'яті, де зберігаються еталонні паролі.

Тому більш безпечніші системи здійснюють зберігання списків паролів в зашифрованому виді, у вигляді хеш-функції, у вигляді хеш-функцій від перетворених паролів. До того ж, необхідно забезпечити додаткові засоби захисту: мінімальну складність паролю, скорочення термінів використання паролів, двохфакторну авторизацію, додаткові питання-відповіді зі списку тощо.

Другий спосіб аутентифікації застосовує так звані карти ідентифікації, на які наносяться дані, що персоніфікують користувача: персональний ідентифікаційний номер, спеціальний шифр або код тощо. Ці дані заносяться на картку в зашифрованому виді, причому ключ шифрування може бути

додатковим ідентифікуючим параметром, оскільки він може бути відомий тільки користувачеві, вводиться ним кожного разу при зверненні до системи і знищується відразу ж після використання.

Інформація, що знаходиться на карті, може бути записана і зчитана різними способами або комбінацією декількох способів. Однак найбільше поширення серед пристроїв аутентифікації за типом «користувач має» отримали індивідуальні магнітні карти. Для захисту карт від несанкціонованого зчитування і підробки застосовуються спеціальні фізичні і криптографічні методи.

Третій спосіб аутентифікації розрізняє користувачів за фізіологічними ознаками. Тільки при такому підході дійсно встановлюється, що користувач, що претендує на доступ до терміналу, саме той, за кого себе видає. При використанні цього класу засобів аутентифікації виникає проблема «соціальної прийнятності»: процедура аутентифікації не повинна принижувати людську гідність, створювати дискомфорт, просто бути занадто морочливою і займати багато часу. Існує досить фізіологічних ознак, що однозначно вказують на конкретну людину. До них відносяться: відбитки ніг і рук, зуби, ферменти, динаміка дихання, риси обличчя і так далі. Для аутентифікації термінальних користувачів автоматизованих систем найбільш прийнятними вважаються відбитки пальців, геометрія руки, голос, особистий підпис, сітчатка ока.

Системи розмежування доступу до інформації становлять собою сукупність процедур, що реалізують перевірку запитів на доступ і оцінку на підставі правил розмежування доступу можливості надання доступу.

Правила розмежування доступу – частина політики безпеки, що регламентує правила доступу користувачів і процесів до пасивних об’єктів.

При розгляді взаємодії двох об’єктів комп’ютерної системи, що виступають як приймальники або джерела інформації, слід виділити пасивний об’єкт, над яким виконується операція, і активний об’єкт, який виконує або ініціює цю операцію.

Коли користувачі або процеси намагаються одержати доступ до пасивних об’єктів, механізми, що реалізують керування доступом, на підставі політики безпеки і перевірки атрибутів доступу можуть «прийняти рішення» про легальність запиту. Прийнято розрізняти 3 типи моделі системи розмежування доступу: 1) дискреційну (DAC – Discretionary Access Control); 2) мандатну (MAC – Mandatory Access Control); 3) рольову (RBAC – Role Based Access Control).

Дискреційна модель заснована на керуванні доступом суб’єктів до об’єктів на основі списків керування доступом (або матриці доступу). Матриця доступу – це таблиця, в якій містяться ідентифікатори об’єктів комп’ютерної системи і дозволені або заборонені режими доступу. Матриця доступу може бути двомірною (наприклад, користувачі/пасивні об’єкти або процеси/пасивні об’єкти) або тримірною (користувачі/процеси/пасивні об’єкти).

Мандатна модель базується на розмежуванні доступу суб’єктів до об’єктів, заснованому на призначенні мітки конфіденційності для інформації, що міститься в об’єктах, і видачі офіційних дозволів (допуску) суб’єктам на звертання до інформації такого рівня конфіденційності.

Рольова модель заснована на дискреційній моделі, що більш розвинена, при цьому права доступу суб’єктів системи до об’єктів групуються з урахуванням специфіки їх застосування, утворюючи ролі користувачів.

Системи розмежування доступу виконуються наступні функції: 1) реалізація правил розмежування доступу суб’єктів та їх процесів до даних; 2) реалізація правил розмежування доступу суб’єктів та їх процесів до обладнання; 3) ізоляція програм процесу, що виконується в інтересах суб’єкта, від інших суб’єктів; 4) керування потоками даних з метою запобігання запису даних на носії невідповідного грифа; 5) реалізація правил обміну даними між суб’єктами для систем, побудованих на мережевих принципах.

В операційних системах Microsoft Windows і Unix/Linux, як правило, використовується дискреційне керування доступом до об'єктів. Об'єкти розмежування доступу у Microsoft Windows мають дескриптор безпеки, що містить інформацію про власника об'єкта, і дискреційний список керування доступом до об'єкта, право редагування якого мають власник об'єкта й адміністратор.

Об'єкти в Unix/Linux містять інформацію про власника файлу, його первинну групу і вектор доступу до файлу. На відміну від Windows вектор доступу в Linux складається завжди із трьох елементів, що визначають права доступу до об'єкта трьох категорій суб'єктів (власника, членів його групи й усіх інших).

Системи аудита й моніторингу призначені для своєчасного виявлення відхилень від реалізації політики управління доступом до інформаційних ресурсів з метою фіксації неавторизованих дій, контролю за інцидентами, виявлення правопорушників, пошуку слабких місць в системі захисту тощо.

Як правило, моніторингу й аудиту підлягають:

– авторизований доступ, включаючи фіксацію ідентифікатора користувача, дату й час головних подій, типи подій, файли, до яких був здійснений доступ, програми / утиліти, що використовувалися при цьому;

– всі привілейовані дії, такі як використання облікового запису супервізора, запуск й зупинка системи, приєднання/від'єднання пристрою введення/виведення тощо;

– спроби неавторизованого доступу, такі як невдалі спроби, порушення політики доступу й повідомлення мережевих шлюзів і між мережевих екранів, попередження від власних систем виявлення вторгнення;

– попередження або помилки системи, такі як консольні (термінальні) попередження або повідомлення, виключення, записані в системні журнали реєстрації, попереджувальні сигнали, пов'язані з керуванням мережею.

Як правило, системи аудиту й моніторингу інтегровані в комплексні програмні рішення із захисту інформації, такі як системи розмежування доступу, антивірусного захисту тощо.

Системи антивірусного захисту – спеціалізовані програмні засоби для знаходження й знешкодження в автоматизованій системі шкідливого програмного забезпечення, в першу чергу комп'ютерних вірусів, а також для запобігання зараження програмного середовища шкідливим програмним кодом.

На сьогодні існує біля півсотні відомих антивірусних засобів. Основні завдання, що виконуються антивірусною програмою: 1) сканування файлів і програм в режимі реального часу; 2) сканування комп'ютера за потребою; 3) сканування мережевого трафіку; 4) сканування електронної пошти; 5) захист від атак ворожих веб-вузлів; 6) відновлення пошкоджених файлів.

Питання для самоконтролю до розділу 6

1. Охарактеризуйте поняття інформаційної системи, обчислювальної системи, автоматизованої системи, інформаційно-телекомунікаційної системи.
2. Назвіть основні класи завдань з технічного захисту інформації в інформаційних системах.
3. Розкрийте зміст основних етапів побудови системи технічного захисту інформації.
4. Дайте визначення та охарактеризуйте поняття витоку інформації технічними каналами.
5. Класифікуйте технічні канали витоку інформації.
6. Визначте фізичні передумови для витоку інформації акустичними каналами, радіотехнічними та оптичними каналами.
7. Охарактеризуйте основні способи і засоби зняття інформації з технічних каналів.
8. Назвіть основні види технічних засобів для захисту інформації від витоку з технічних каналів.
9. Розкрийте сутність заходів для захисту інформації від витоку технічними каналами.
10. Дайте визначення та класифікацію несанкціонованого доступу до інформації.
11. Назвіть основні засоби для захисту інформації від несанкціонованого доступу на рівні периметра інформаційної системи.

12. Охарактеризуйте засоби для захисту інформації від несанкціонованого доступу на рівні комунікаційного обладнання.

13. Визначте основні типи засобів для захисту інформації від несанкціонованого доступу на рівні апаратного забезпечення.

14. Дайте характеристику засобам для захисту інформації від несанкціонованого доступу на рівні системного і прикладного програмного забезпечення.

Література

1. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.96 р. № 423.

2. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р. № 200.

3. ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. Затверджено наказом Держстандарту України від 19.12.96 р. № 511.

4. Закон України "Про електронні документи та електронний документообіг" // Відомості Верховної Ради (ВВР), 2003. — № 36. — ст. 275.

5. Закон України "Про електронний цифровий підпис" // Відомості Верховної Ради (ВВР), 2003. — № 36. — ст. 276.

6. Закон України "Про захист інформації в автоматизованих системах" від 05.07.94, № 80/94-ВР. — К., 1994.

7. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.94, № 80/94-ВР.

8. Закон України "Про інформацію" // Відомості Верховної Ради (ВВР), 1992. — № 48. — ст. 650.

9. Інструкція про порядок забезпечення режиму безпеки, що повинен бути створений на підприємствах, установах та організаціях, які здійснюють підприємницьку діяльність у галузі криптографічного захисту конфіденційної інформації, що є власністю держави, затверджена наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 22.10.99 № 46 і зареєстрована в Міністерстві юстиції України 29.11.99 за № 817/4110.

10. Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави, затверджена постановою Кабінету Міністрів України від 27.11.98 № 1893.

11. Концепція технічного захисту інформації в Україні. Затверджено постановою Кабінету Міністрів України від 08.10.97 р. № 1126.

12. НД ТЗІ 1.1-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. Затверджено наказом ДСТСЗІ СБ України від 28.05.99 р. № 26.

13. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99 р. 1" 22.

14. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СВ України від 28.04.99 р. № 22.

15. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000 № 63.

16. НД ТЗІ 1.5-001-2000 Радіовиявлювачі. Класифікація. Загальні технічні вимоги. Затверджено наказом ДСТСЗІ СБ України від 13.06.2000. № 29.

17. НД ТЗІ 1.6-001-96 Правила побудови, викладення, оформлення та позначення нормативних документів системи ТЗІ. Затверджено наказом ДСТЗІ від 26.07.96 р. № 51.

18. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення. Затверджено наказом ДСТЗІ від 09.02.2001 р. № 2.

19. НД ТЗІ 2.3-001-2001 Радіовиявлювачі вимірювальні. Методи та засоби випробувань. Затверджено наказом ДСТЗІ від 27.02.2001 р. № 5.

20. НД ТЗІ 2.3-002-2001 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Нелінійні атенюатори та загороджувальні фільтри. Методика випробувань. Затверджено наказом ДСТСЗІ СБ України від 06.04.2001 р. № 11.

21. НД ТЗІ 2.3-003-2001 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби активного приховування мовної інформації. Генератори спеціальних сигналів. Методика випробувань. Затверджено наказом ДСТСЗІСБУкраїни від 06.04.2001 р. № 11.

22. НД ТЗІ 2.3-004-2001 Радіовиявлювачі індикаторні. Методи та засоби випробувань. Затверджено наказом ДСТСЗІСВ України від 09.04.2001 р. № 12.

23. НД ТЗІ 2.5-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту. Затверджено наказом ДСТСЗІ СБ України від 28.05.99 р. № 26.

24. НД ТЗІ 2.5-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту. Затверджено наказом ДСТСЗІ СБ України від 28.05.99 р. № 26.

25. НД ТЗІ 2.5-003-99 Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту. Затверджено наказом ДСТСЗІ СБ України від 28.05.99 р. № 26.

26. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99 р. № 22.

27. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99 р. № 22.

28. НД ТЗІ 2.7-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт. Затверджено наказом ДСТСЗІ СБ України від 28.05.99 р. № 26.

29. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 20.12.2000 р. № 60.

30. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 28.04.99 р. №22.

31. НД ТЗІ 3.7-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова). Затверджено наказом ДСТСЗІ СБ України від 28.05.99 р. № 26.

32. НД ТЗІ 4.7-001-2001 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби визначення наявності та віддаленості місця контактного підключення засобів технічної розвідки. Рекомендації щодо розроблення методів випробувань. Затверджено наказом ДСТСЗІ СБ України від 06.04.2001 р. № 11.

33. НД ТЗІ Р-001-2000. Засоби активного захисту мовної інформації з акустичними та віброакустичними джерелами випромінювання. Класифікація та загальні технічні вимоги. Рекомендації. Затверджено наказом ДСТСЗІ СБ України від 04.09.2000. № 41.

34. Положення про державну експертизу в сфері технічного захисту інформації. Затверджено наказом ДСТСЗІ СБ України від 29.12.99 р. №62.

35. Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах. Затверджено постановою Кабінету Міністрів України від 16.02.98 р. № 180.

36. Положення про контроль за функціонуванням системи технічного захисту інформації. Затверджено наказом ДСТСЗІ СБ України від 22.12.99 р. № 61.

37. Положення про порядок здійснення криптографічного захисту інформації в Україні, затверджене Указом Президента України від 22.05.98 р. № 505.

38. Положення про технічний захист інформації в Україні. Затверджено Указом Президента України від 27.09.99 р. № 1229.

39. Бузов Г. А., Калинин С. В., Кондратьев А. В. Защита от утечки информации по техническим каналам. —М.: Горячая линия —Телеком, 2005. — 416 с.

40. Барсуков В. С. Современные технологии безопасности: Интегральный подход. — М.: Нолидж, 2000. — 496 с.

41. Гатчин Ю. А. Основы информационной безопасности: учебное пособие/ Ю. А. Гатчин, Е. В. Климова. — СПб.: СПбГУ ИТМО, 2009. — 84с.

42. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. — М.: Энергоатомиздат, 1994. — 400 с.

43. Грушо А. Л., Тимонина Е. Е. Теоретические основы защиты информации. — М.: Изд-во агентства "Яхтсмен", 1996. — 192 с.

44. Девяткин П. М., Михальский О. О., Правиков Д.Л., Щербаков А. О. Теоретические основы компьютерной безопасности. — М.: Радио и связь, 2000. — 192 с.

45. Захист інформації в автоматизованих системах управління [Текст]: навч. посібник/ Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. — Житомир: Вид-во ЖДУ ім. І. Франка, 2015. — 226 с.

46. Конеев И. Р. Информационная безопасность предприятия. — СПб.: БХВ-Петербург, 2003. — 752 с.

47. Конахович Г. Ф., Климчук В. П., Паук С. М., Потапов В. Г. Защита информации в телекоммуникационных системах. — К.: «МК-Пресс», 2005. — 288 с.

48. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. — Х. : Вид. ХНЕУ, 2013. — 476 с.

49. Рибальський О. В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. — К.: Вид. Національної академії внутріш. справ, 2012. — 104 с.

50. Рибальський О. В. Інформаційна безпека правоохоронних органів. Курс лекцій / О. В. Рибальський, В. Г. Хахановський, В. В. Шорошев, О. І. Грищенко, С. В. Сторожев, М. В. Кобець. — К.: НАВСУ, 2003. — 160 с.

51. Хорошко В. А., Чекетков А. А. Методы и средства защиты иформации. — К.: Изд. Юниор, 2003. — 504 с.

52. Хорошко В. О. Основи інформаційної безпеки / В. О. Хорошко, В. С. Чередниченко, М. Є. Шелест / За ред. проф. В. О. Хорошка. – К.: ДУІКТ, 2008. – 186 с.

РОЗДІЛ 7

ЮРИДИЧНА ВІДПОВІДАЛЬНІСТЬ У СФЕРІ ОБІГУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

7.1 Теоретичні засади юридичної відповідальності у сфері обігу інформації з обмеженим доступом

В системі забезпечення режиму інформації з обмеженим доступом важливе місце посідає інститут юридичної відповідальності, існування якого покликано створити додаткові гарантії охорони та захисту суспільних відносин у сфері інформаційної безпеки особи, держави і суспільства.

В теорії права юридична відповідальність розглядається як вид соціальної відповідальності, що реалізується через специфічні охоронні правовідносини, спрямовані на покладення на правопорушника обов'язку перетерпіти негативні наслідки особистого, організаційного, майнового характеру за вчинене правопорушення, визначені санкціями правових норм.

Поняття юридичної відповідальності традиційно розкривається через її основні риси (ознаки), мету, функції, принципи та підстави.

Основні риси (ознаки) юридичної відповідальності відображають її найбільш узагальнені властивості, зокрема те, що вона:

а) визначається виключно нормами права;

б) є зовнішньою реакцією суспільства на правопорушення, що тягне для особи, яка його вчинила негативні наслідки, які виражаються в обмеженнях особистого, майнового або організаційного характеру;

в) спирається на державний примус, який реалізується через діяльність спеціально уповноважених державних органів в межах їх компетенції, визначеної законом;

г) реалізується за чітко визначеною законом процедурою (процесуальною формою).

Метою юридичної відповідальності є утвердження законності, упорядкування і відновлення порушених суспільних відносин, забезпечення прав, свобод і законних інтересів людини та громадянина, безпеки держави і

суспільства в цілому.

У сфері обігу інформації з обмеженим доступом мета юридичної відповідальності знаходить свій вираз у забезпеченні нормального функціонування законодавчо визначеного порядку обігу інформації, захист інформаційних прав і свобод громадян від незаконних порушень, попередження вчинення правопорушень у сфері доступу до інформації в майбутньому.

Мета юридичної відповідальності є результатом здійснення *функцій юридичної відповідальності* – основних напрямів впливу на суспільство, які розкривають мету і відображають призначення юридичної відповідальності в системі правового регулювання та суспільному житті.

Основними функціями юридичної відповідальності є:

1) репресивно-каральна (штрафна) – полягає у негативному впливі з боку суспільства на правопорушника у вигляді безпосереднього акту засудження особи від імені держави;

2) правовідновлювальна (компенсаційна) – полягає у відновленні порушеного права та необхідності відшкодувати завдану правопорушенням матеріальну і моральну шкоду;

3) виховна (превентивна) – полягає в попередженні вчинення нових правопорушень, обмеженні можливостей вчиняти нові протиправні діяння, формуванні стереотипів, стимулів правомірної поведінки (превенція) конкретного правопорушника (спеціальна превенція) та утриманні від правопорушень інших осіб (загальна превенція).

Поряд із традиційними функціями юридичної відповідальності в інформаційному контексті необхідно виділити також *сигналізаційну (інформативну) функцію*. Вона полягає в тому, що юридична відповідальність несе у собі інформацію щодо моделей протиправної поведінки, можливих засобів впливу на правопорушників, змісту і особливостей конкретних видів відповідальності.

Регулювання та охорона суспільних відносин у сфері обігу інформації з обмеженим доступом відбувається через здійснення всіх функцій юридичної відповідальності. Утім, сучасна правова доктрина орієнтує на виконання інститутом юридичної відповідальності передусім правозахисних, виховних та інформативних функцій. Надання пріоритету каральним функціям свідчить про порушення принципу гуманізму в правовому житті, підміну права насильством, що не припустимо ні з яких міркувань. Тож у розвиненому в правовому суспільстві сама можливість застосування примусових заходів юридичної відповідальності створює значно більший організаційний ефект ніж безпосереднє їх здійснення.

Принципи юридичної відповідальності – це вихідні керівні ідеї, які відображають природу юридичної відповідальності, забезпечують високу якість і ефективність реалізації відповідних заходів впливу особистого, майнового, організаційного та іншого характеру. До основних принципів юридичної відповідальності належать:

1) *принцип законності* – означає, що настання юридичної відповідальності стає можливим виключно в соціально-правових ситуаціях, передбачених законом, а сама відповідальність повинна реалізовуватися компетентними на те суб'єктами, в межах відповідної процесуальної форми;

2) *принцип невідворотності юридичної відповідальності* – означає, що несприятливі наслідки для правопорушника є наслідком вчинення протиправного діяння і відсутні законні підстави для її звільнення;

3) *принцип справедливості юридичної відповідальності* знаходить свій вираз: по-перше, у встановленні формальної рівності всіх перед законом і судом, а по-друге, у застосуванні еквівалентних заходів впливу скоєному правопорушенню;

4) *принцип гуманізму* гарантує, що будь-які заходи впливу, які застосовуються до правопорушника, не повинні мати на меті приниження його людської гідності;

5) *принцип індивідуалізації відповідальності* знаходить вираз в тому,

що заходи впливу до конкретного правопорушника повинні застосовуватися з урахуванням характеру і тяжкості вчиненого протиправного діяння, форми і ступеню його вини, обставин, що пом'якшують і обтяжують відповідальність;

6) *принцип неприпустимості подвоєння відповідальності* означає, що ніхто не повинен двічі притягуватись до юридичної відповідальності за одне і те саме правопорушення;

7) *принцип обґрунтованості юридичної відповідальності* передбачає об'єктивне дослідження всіх обставин справи, що мають юридичне значення для встановлення наявності або відсутності конкретного правопорушення, з метою визначення відповідних заходів впливу;

8) *принцип доцільності* виявляється у визначені таких заходів впливу, які є необхідними і достатніми для виправлення правопорушника і попередження вчинення нових протиправних діянь;

9) *принцип своєчасності (оперативності)* юридичної відповідальності – з одного боку вимагає притягнення винного до відповідальності у найкоротші строки, а з іншого – встановлює терміни давності, після спливу яких відповідальність не застосовується.

Реалізація юридичної відповідальності стає можливою тільки тоді, коли існують підстави для її виникнення (настання) і відсутні підстави, що її виключають.

Під підставами юридичної відповідальності розуміється певна сукупність обставин, за наявністю яких вона є можливою і необхідною. В теорії права розрізняють фактичну, нормативну і процесуальну підстави юридичної відповідальності.

Фактична підстава – це наявність факту правопорушення (фактично зробленого діяння), з яким пов’язується виникнення охоронних правовідносин, в межах якого реалізується юридична відповідальність.

Висновок про факт вчинення особою суспільно-небезпечного, протиправного діяння формулюється через визначення *складу правопорушення* – сукупності закріплених в законі об’єктивних і

суб’єктивних ознак, за наявності яких суспільно небезпечне діяння визнається конкретним правопорушенням.

Елементами складу правопорушення є: об’єкт, об’єктивна сторона, суб'єкт, суб'єктивна сторона. Відсутність в діянні особи хоча б одного з елементів складу правопорушення виключає можливість реалізації юридичної відповідальності за будь-яке вчинене правопорушення, у тому числі у сфері обігу інформації з обмеженим доступом.

Об'єктом правопорушення є суспільні відносини, які охороняються нормами права і на які посягає конкретне правопорушення. *Об’єктом правопорушень сфері обігу інформації з обмеженим доступом* є суспільні відносини правового режиму відкритої публічної інформації та інформації з обмеженим доступом (зокрема державної, комерційної, банківської, професійної таємниці, таємниці листування і телефонних розмов, службової інформації, інформації про особисте життя, персональних даних тощо).

Від об'єкта правопорушення необхідно відрізняти *предмет правопорушення* – цінності, з приводу яких та шляхом безпосереднього впливу на які вчиняється протиправне діяння. *Предметом правопорушення у сфері обігу інформації з обмеженим доступом* є відомості, що становлять зміст інформації, яка становить державну таємницю, або іншу інформацію з обмеженим доступом, спрямовану на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави.

Об’єктивна сторона правопорушення представляє собою зовнішній вираз протиправного діяння і полягає в діях або бездіяльності суб’єкта правопорушення. *У сфері інформації з обмеженим доступом об’єктивна сторона* знаходить свій вираз у формі порушення встановленого законом порядку обігу таких відомостей, зокрема, розголошенні інформації, негласних способах отримання інформації, втраті документів, що містить інформацію з обмеженим доступом тощо.

Суб’єктом будь-якого правопорушення є деліктоздатна особа, яка вчинила протиправне діяння. *Суб’єктами правопорушень у сфері обігу*

інформації з обмеженим доступом можуть бути фізичні та юридичні особи. Загальним суб'єктом інформаційних правопорушень є осудні фізичні особи віком від 16-ти років. Спеціальним суб'єктом можуть бути особи, які володіють професійною таємницею, посадові особи, уповноважені на здійснення організаційно-розпорядчих та адміністративно-господарчих функцій в органах державної влади та органах місцевого самоврядування в інформаційній сфері. Спеціальним суб'єктом також є військовослужбовці та інші особи, на яких поширюється дія дисциплінарних статутів або спеціальних положень про службу, у випадках вчинення правопорушення, пов'язаного з дотриманням та збереженням державної таємниці. Юридичні особи можуть бути суб'єктом адміністративної чи цивільно-правової відповідальності.

Суб'єктивна сторона правопорушення відображає психічне ставлення особи до свого діяння та представляє собою вину у формі умислу або необережності. *Умисел* має місце в протиправних діяннях тоді, коли суб'єкт усвідомлює суспільну небезпечність (шкідливість) свого діяння, передбачає настання шкідливих наслідків, при прямому умислі бажає настання шкідливих наслідків, а при непрямому – байдуже до них ставиться, не бажаючи їх настання, але свідомо допускаючи це. *Необережність* знаходить свій вираз у: 1) протиправній самовпевненості - суб'єкт усвідомлює суспільну небезпечність (шкідливість) свого діяння, передбачає настання шкідливих наслідків та легковажно сподівається їм запобігти; 2) протиправній недбалості: суб'єкт усвідомлює суспільну небезпечність (шкідливість) свого діяння, не передбачає настання шкідливих наслідків, але повинен був і міг їх передбачати.

Правопорушення у сфері обігу інформації з обмеженим доступом можуть характеризуватися будь-якою формою вини. Проте досить часто правовий режим інформації з обмеженим доступом порушується через необережну форму вини працівників, що його забезпечують. Тому невипадково серед загроз інформаційній безпеці при створенні системи

управління інформаційною безпекою організації окреме місце займає необережне, недбале поводження персоналу з інформацією з обмеженим доступом та плануються відповідні системні попереджувальні заходи.

*Нормативна підстава юридичної від*повідальності передбачає наявність норми права, яка забороняє протиправну поведінку і встановлює за її вчинення відповідні санкції. Вимога правової визначеності передбачає чітку регламентацію нормами права правопорушення та його складу, форм, засобів та меж державно-правового примусу, що може бути застосований до правопорушника за вчинене ним діяння. Процес встановлення кореляційної відповідності між фактичною і нормативною підставою є юридичною кваліфікацією конкретного правопорушення.

Процесуальна підстава юридичної відповідальності передбачає наявність правозастосовчого акта – рішення компетентного органу (наказ адміністрації, постанова уповноваженого органу, вирок суду тощо), яким визначаються вид юридичної відповідальності та примусові заходи впливу на правопорушника.

Якщо фактична і нормативна підстави є достатніми умовами для вирішення питання про виникнення юридичної відповідальності, наявність процесуальної підстави є необхідною передумовою її настання. Правозастосовчий акт дозволяє розпочати процес притягнення (настання) юридичної відповідальності, конкретизує факт протиправного діяння й індивідуалізує заходи впливу щодо особи, яка його вчинила, з урахуванням всіх суб'єктивних і об'єктивних обставин.

При вирішенні питання щодо притягнення особи до юридичної відповідальності також необхідно враховувати наявність або відсутність *підстав виключення та/або звільнення від юридичної відповідальності*. Різниця між зазначеними поняттями полягає в тому, що підстави виключення правової відповідальності вказують на неприпустимість правової відповідальності через відсутність суспільної небезпеки правопорушення (неосудність, необхідна оборона, крайня необхідність, казус, фізичний або

психічний примус, виконання наказу або розпорядження заподіяння шкоди при затриманні особи, що скоїла злочин; обґрунтований ризик тощо); підстави звільнення від правової відповідальності є умовою зняття обов'язку зазнавати заходи державно-примусового впливу за вчинене правопорушення (малозначність діяння, діяльне каяття правопорушника завершення строку давності притягнення до юридичної відповідальності, акти про амністію або помилування тощо). У сері обігу інформації з обмеженим доступом кожен вид юридичної відповідальності має підстави для виключення або звільнення від неї, що закріплені у приписах відповідних законодавчих актів.

Різноманітність відносин у сфері обігу інформації з обмеженим доступом, а також норм, що визначають різний ступінь суспільної небезпеки протиправного діяння, надають можливість класифікувати юридичну відповідальність на кримінальну, адміністративну, цивільно-правову та дисциплінарну (матеріальну).

У сфері обігу інформації з обмеженим доступом *кримінальна відповідальність* є найбільш суворим видом юридичної відповідальності і характеризується низкою специфічних ознак, зокрема:

– настає за вчинення протиправних діянь (злочинів), що характеризуються найвищим ступенем суспільної небезпеки;

– вид і міра обмежень особистого, майнового або організаційного характеру, визначені виключно в кримінальному законі, перш за все у санкції статті Кримінального кодексу України (надалі – КК України), що передбачає відповідальність за вчинений злочин;

– офіційна оцінка суспільно-небезпечної і протиправної поведінки особи як злочинної здійснюється спеціально уповноваженими органами держави – судами і процесуально закріплюється у вироку суду, який проголошується ім’ям України;

– кримінальна відповідальність породжує особливий правовий стан засудженої особи – судимість, і, як наслідок, погіршення її правового становища, чого не породжують інші види юридичної відповідальності.

Адміністративна відповідальність є самостійним видом юридичної відповідальності, що настає за адміністративні правопорушення в різних сферах державного управління та життєдіяльності суспільства, тобто норми щодо застосування адміністративної відповідальності спрямовані на охорону нормативних приписів різних галузей права і зокрема інформаційного права. Характерними ознаками адміністративної відповідальності є наступні ознаки:

– за допомогою інституту адміністративної відповідальності здійснюється захист не тільки адміністративно-правових відносин, а й відносин врегульованих нормами інших галузей права, зокрема інформаційного, банківського, фінансового, медіа-права тощо;

– підставою адміністративної відповідальності є вчинення правопорушення (проступку), передбаченого нормами Кодексу України про адміністративні правопорушення (надалі – КУпАП) та іншим законами, що регулюють порядок створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації;

– перелік заходів адміністративної відповідальності, що застосовується до особи, яка вчинила адміністративне правопорушення в інформаційній сфері, є дещо ширшим і не завжди знаходить своє закріплення в нормах КУпАП, проте, за своєю юридичною природою, такі заходи є адміністративним стягненням і не виключають можливості настання адміністративної відповідальності;

– повноваження органів, які в межах своєї компетенції наділені правом застосовувати адміністративні стягнення за адміністративні правопорушення в інформаційній сфері, визначаються у нормативних приписах КУпАП та інших нормативно-правових актах, якими врегульовано порядок створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації в Україні.

Цивільно-правова відповідальність – самостійний вид юридичної відповідальності, яка передусім спрямована на виконання обов’язку по відновленню порушеного становища (права) потерпілого або компенсації

нанесених правопорушенням шкоди, збитків, упущеної вигоди, що забезпечується відповідними заходами державного примусу, передбаченими нормами цивільного права. Характерними ознаками цивільно-правової відповідальності є наступні риси:

– цивільна відповідальність спрямована на охорону приватних правовідносин – належне здійснення суб'єктивних цивільних прав та виконання цивільних обов'язків, а у разі нанесення шкоди – максимально ефективне відновлення становища потерпілого;

– підставою цивільної відповідальності є вчинення цивільного правопорушення (делікту) – протиправного діяння, яке виражається в порушенні суб'єктивних цивільних прав та невиконанні чи неналежному виконанні цивільних обов'язків, передбачених договором або актом цивільного законодавства, що призводить до збитків, майнової або моральної шкоди та інших втрат;

– в цивільному праві ініціатива щодо притягнення до відповідальності, а також обґрунтування її обсягів покладається на постраждалу сторону, а не на державу;

– заходи цивільно-правової відповідальності мають переважно майновий характер і спрямовані на відшкодування потерпілому нанесених збитків передусім майновими засобами, серед яких: відшкодування в натурі; вилучення належного порушнику майна; відшкодування завданих збитків у грошовому еквіваленті; сплата неустойки, пені; майнова компенсація за нанесену моральну шкоду тощо.

– відновлення порушеного права внаслідок вчинення цивільного правопорушення (делікту) в багатьох випадках стає можливим завдяки добровільному відшкодуванню, компенсації без звернення до суду; регулятивний ефект тоді забезпечує сама можливість примусових заходів з боку держави, а їх безпосереднє здійснення відбувається у разі відмови від виконання обов'язків відповідальності.

Самостійним видом юридичної відповідальності *є дисциплінарна відповідальність*, яка виступає особливим засобом охорони встановленого нормами трудового законодавства і суміжних галузей права порядку. Характерними особливостями дисциплінарної відповідальності є наступні ознаки:

– метою дисциплінарної відповідальності є забезпечення трудової або службової дисципліни;

– фактичною підставою дисциплінарної відповідальності є дисциплінарний проступок – суспільно небезпечне, протиправне, винне діяння (дія або бездіяльність), яке полягає у невиконанні або у неналежному виконанні працівником покладених на нього трудових або службових обов'язків, визначених нормами локальних актів та Кодексу законів про працю України (надалі – КЗпП України);

– дисциплінарна відповідальність має односторонній характер, оскільки суб'єктом такої відповідальності є працівник, який набуває певних прав і обов'язків у процесі здійснення трудової діяльності;

– в основі реалізації дисциплінарної відповідальності лежать відносини субординації між працівником і суб'єктом дисциплінарної влади;

– заходи дисциплінарного впливу застосовуються виключно у порядку передбаченому локальними нормативними актами і КЗпП України, та вимагають наявності акта їх застосування з боку уповноважених органів.

Чинне трудове законодавство поряд з дисциплінарною виділяє матеріальну відповідальність, у зв'язку з чим постає питання щодо визначення співвідношення між зазначеними видами юридичної відповідальності.

Матеріальна відповідальність у правовій літературі визначається як обов'язок кожної із сторін трудових правовідносин (працівника та роботодавця) відшкодувати шкоду, заподіяну іншій стороні внаслідок невиконання чи неналежного виконання трудових обов'язків у встановленому законом розмірі та порядку. В основі матеріальної відповідальності лежить обов'язок працівника дбайливо ставитися до майна роботодавця та вжити заходів щодо запобігання шкоди, а також обов'язок

власника або уповноваженого ним органу створити працівникам умови, необхідні для нормальної роботи і забезпечення повного збереження дорученого їм майна.

За правовою сутністю матеріальна відповідальність працівника має багато спільних рис з дисциплінарною відповідальністю, а саме:

1) і матеріальна, і дисциплінарна відповідальність наступає за невиконання або неналежне виконання обов'язків, що становлять зміст трудової дисципліни;

2) притягнення і до матеріальної, і до дисциплінарної відповідальності відбувається за умови доведення в діях особи складу правопорушення.

Разом з тим матеріальна та дисциплінарна відповідальність працівників є самостійними видами юридичної відповідальності, а тому між ними є принципові відмінності:

– метою дисциплінарної відповідальності є забезпечення трудової дисципліни, матеріальної – відшкодування (компенсація) завданої шкоди;

– підставою виникнення дисциплінарної відповідальності є будь-яке винне протиправне недотримання трудової дисципліни, матеріальної – винне протиправне недотримання трудової дисципліни, внаслідок якого була завдана майнова шкода роботодавцю;

– характер заходів дисциплінарної відповідальності виховний і каральний, матеріальної – правовідновлювальний;

– суб'єктами дисциплінарної відповідальності є працівник,матеріальної і працівник, і роботодавець;

– реалізація дисциплінарної відповідальності вимагає наявності акта застосування дисциплінарного стягнення з боку уповноважених органів, у випадку матеріальної відповідальності обов'язок працівника чи роботодавця щодо відшкодування майнової шкоди може бути реалізований добровільно і без наявності такого акта.

7.2 Характеристика правопорушень у сфері обігу інформації з обмеженим доступом

7.2.1 Кримінальні правопорушення у сері обігу інформації з обмеженим доступом

Залежно від ступеню суспільної небезпеки, групи однорідних відносин, яким завдається шкода протиправним діянням, кримінальні правопорушення у сфері обігу інформації з обмеженим доступом доцільно класифікувати на:

1) злочини, що посягають на встановлений законом порядок обігу таємної інформації;
2) злочини, що посягають на порядок обігу службової інформації;
3) злочини, що посягають на порядок обігу конфіденційної інформації.

Злочини у сфері обігу таємної інформації охоплюють кримінальні правопорушення у сфері встановленого законом порядку обігу державної, професійної таємниці, таємниці особистого життя, банківської та комерційної таємниці, таємниці слідства та інших таємниць, що охороняються законом.

Злочини у сфері обігу інформації, що становлять державну таємницю, містяться у різних розділах Особливої частини КК України, проте спільним для них є предмет злочинного посягання – відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою (ст. 1 Закону України «Про державну таємницю»).

Кримінальна відповідальність за злочини, предметом яких є відомості, що становлять державну таємницю, насамперед, передбачена у Розділі I КК України – «Злочини проти основ національної безпеки України». Два склади злочинів цього розділу мають безпосереднє відношення до встановленого законом порядку охорони та захисту

відомостей, що становить державну таємницю: ст.111 КК України – «Державна зрада» і ст.114 КК України – «Шпигунство».

Як і інші злочини проти основ національної безпеки, дії, передбачені ст.ст.111,114 КК України, є найбільш суспільно-небезпечними посяганнями, оскільки їх родовим об'єктом виступають відносини, які забезпечують державну безпеку, конституційний лад, суверенітет, територіальну цілісність і недоторканність, обороноздатність України.

З об'єктивної сторони злочини, передбачені ст.ст.111, 114 КК України можуть виражатися у двох формах:

1) *передача* іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю;

2) *збирання* таких відомостей *з метою передачі* іноземній державі, іноземній організації або їх представникам.

Передача зазначених відомостей матиме місце у випадках, коли особа володіє ними і повідомляє їх іноземній державі, організації або їх представнику шляхом усного повідомлення, пересилання тощо. Збирання зазначених відомостей полягає в їх пошуку і добуванні, придбанні будь-яким способом з наступним зосередженням їх в одному чи кількох місцях.

Для кваліфікації злочину не має значення кому саме належить ініціатива збирання чи передачі відповідних відомостей – виконавцю чи адресату шпигунства. Не матиме значення для відповідальності і оригінальність самого документа, що містить відповідні відомості, оскільки протиправною визнаватиметься першоджерел інформації тощо.

Висока суспільна небезпечність цих злочинів відбивається в їх суб'єктивній стороні: дії, передбачені ст.ст. 111, 114 КК України є умисними і вчиняються тільки з прямим умислом. Характерною ознакою зазначених злочинів є наявність спеціального суб'єкту – іноземець або особа без громадянства, які є осудними та досягли 16-річного віку (ст.114 КК України) та громадянин України (осудний, 16-річного вік – ст.111 КК України).

Слід зауважити, що чинний КК України містить заохочувальні норми щодо звільнення від кримінальної відповідальності осіб, які вчинили протиправні дії, передбачені ст.ст.111, 114, а саме:

1) ч.1 ст.111 КК України – звільняється від кримінальної відповідальності громадянин України, якщо він на виконання злочинного завдання іноземної держави, іноземної організації або їх представників ніяких дій не вчинив і добровільно заявив органам державної влади про свій зв'язок з ними та про отримане завдання;

2) ч.1 ст.114 КК України – звільняється від кримінальної відповідальності особа, яка припинила протиправну діяльність та добровільно повідомила органи державної влади про вчинене, якщо внаслідок цього і вжитих заходів було відвернене заподіяння шкоди інтересам України.

Підстави кримінальної відповідальності за вчинення злочинів у сфері обігу державної таємниці також закріплені у Розділі XIV КК України – «Злочини у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову на мобілізацію»

Ст. 328 КК України («Розголошення державної таємниці») передбачає відповідальність за розголошення відомостей, що становлять державну таємницю, особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків, за відсутності ознак державної зради або шпигунства.

Ст. 329 КК України («Втрата документів, що містить державну таємницю») встановлює відповідальність за втрату документів або інших матеріальних носіїв секретної інформації, що містять державну таємницю, а також предметів, відомості про які становлять державну таємницю, особою, якій вони були довірені, якщо втрата стала результатом порушення встановленого законом порядку поводження із зазначеними документами та іншими матеріальними носіями секретної інформації або предметами

Для злочинів, закріплених ст.ст. 328, 329 КК України, є спільним безпосередній об'єкт – суспільні відносини з охорони державної таємниці у різних сферах діяльності держави (економіки, науки і техніки, зовнішніх відносин, державної безпеки). Проте, предмет цих злочинів не є тотожнім. Предметом злочину, передбаченого ст. 328 КК України, є відомості, що становлять зміст державної таємниці (ст. 1 Закону України «Про державну таємницю»), предметом злочину, передбаченого ст. 329 КК України, є документи, що містять державну таємницю, інші матеріальні носії секретної інформації, що містять державну таємницю, а також предмети, відомості про які становлять державну таємницю.

Відмінність між злочинами, передбаченими ст.ст. 328, 329 КК України, полягає і в їх об'єктивній стороні. Об'єктивна сторона складу злочину, передбаченого ст. 328 КК України, виражається у розголошенні відомостей, що становить державну таємницю, тобто протиправному доведенні їх до відома сторонніх осіб, яким ці відомості не повинні бути відомі. Об'єктивна сторона складу злочину, передбаченого ст.329 КК України, характеризується сукупністю двох взаємопов'язаних ознак, одна з яких є причиною, а інша - наслідком: 1) *порушення* особою, якій було довірено матеріальні носії секретної інформації, що містить державну таємницю, або предмети, відомості про які становлять державну таємницю, *встановленого* законом порядку поводження із ними; 2) втрата зазначених матеріальних носіїв інформації або предметів.

Суб'єктивна сторона злочину, передбаченого ст.328 КК України, може виражатися як у формі умислу, так і у формі необережності. Утім обов'язковою умовою при розголошенні є відсутність ознак державної зради або шпигунства. Суб'єктивна сторона злочину, передбаченого ст.329 КК України, характеризується складною формою вини: умисел або необережність до діяння (порушення встановленого законом порядку поводження з відповідними носіями секретної інформації або предметами) і необережністю до наслідків у вигляді втрати вказаних носіїв інформації

(предметів), а також до тяжких наслідків, які є кваліфікуючими ознаками як злочину, визначеному ст. 329 КК України, так і злочину, визначеному ст. 328 КК України.

Кримінальне законодавство України також містить норми, що встановлюють відповідальність за порушення встановленого законом порядку зберігання відомостей військового характеру, що становить державну таємницю. Розділ XIX КК України – «Злочини проти встановленого порядку несення військової служби (військові злочини)» містить ст.422 КК України – «Розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості».

Безпосереднім об'єктом зазначеного злочину є режим охорони відомостей військового характеру, що становлять державну таємницю, тобто інформація, що належить до державної таємниці у сфері оборони.

З об'єктивної сторони злочин, передбачений ст. 422 КК України, може виражатися у двох формах:

1) *розголошення* відомостей військового характеру, що становлять державну таємницю, за відсутності ознак державної зради (ч. 1 ст. 422 КК України);

2) *порушення встановлених правил поводження* з документами або матеріалами, що містять відомості військового характеру, які становлять державну таємницю, а також із предметами, відомості про які становлять державну таємницю, що спричинило їхню втрату (ч. 2 ст. 422 КК України).

Суб'єктивна сторона злочину у першій його формі характеризується як умисною, так і необережною формою вини до діяння , а у другій - умислом або необережністю до діяння і необережністю до наслідків.

Суб'єктом злочину, передбаченого ч.1 ст.422 ККУкраїни, можуть бути військовослужбовці або військовозобов'язаний під час проходження зборів, незалежно від того, яким чином відповідні відомості стали йому відомі.

Суб'єкт злочину, передбаченого ч. 2 ст. 422 КК України, спеціальний: ним є особа, якій відповідні документи, матеріали чи предмети були довірені.

Кваліфікуючою ознакою злочину, передбаченого ч.3 ст.422 КК України, є тяжкі наслідки. Психічне ставлення винного до тяжких наслідків характеризуватися виною у формі необережності.

В системі кримінальних правопорушень, що посягають на встановлений законом порядок обігу інформації з обмеженим доступом, слід виокремлювати злочини, предметом яких є відомості, що становлять зміст професійної таємниці. Обов'язком зберігати таки відомості наділені представники певних професій (медичні працівники, адвокати, журналісти тощо). Як слушно підкреслюється у навчальній літературі, важливим у відношенні збереження професійної таємниці є питання довіри – особа, яка потребує певної професійної допомоги, погоджується надати чутливу для себе інформацію, очікуючи збереження її в таємниці. Вона також очікує, що надана нею інформація може бути розголошена лише за її згоди. При цьому така інформація надається під час реалізації (захисту) особою своїх прав і свобод (наприклад, право на здоров'я, на правову допомогу, на свободу віросповідання). Тому розголошення довіреної інформації матиме наслідком обмеження прав осіб, які не зможуть вільно користуватися послугами відповідних професій, якщо не матимуть впевненості у захищеності інформації, яку вони передають.

Серед кримінальних правопорушень у сфері охорони професійної таємниці законодавець, насамперед, виділяє злочин, передбачений ст.145 КК України – «Незаконне розголошення лікарської таємниці».

Безпосереднім об'єктом зазначеного злочину є встановлений законом порядок збереження лікарської таємниці, який забезпечує належний стан здоров'я громадян, предметом є відомості, що становлять зміст лікарської таємниці.

Об’єктивна сторона зазначеного злочину характеризується діянням у формі розголошення лікарської таємниці, тяжкими наслідками, а також причинним зв’язком між діянням і його наслідками.

Злочин, передбачений ст. 145 КК України, характеризується спеціальним суб’єктом – медичні працівники та інші особи, яким відповідна інформація стала відома у зв’язку з виконанням професійних чи службових обов’язків. З суб’єктивної сторони цей злочин характеризується змішаною формою вини: прямим або непрямим умислом до діяння і необережністю до його наслідків.

Спеціальною нормою стосовно ст. 145 КК України є дії, передбачені ст. 132 КК України («Розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби»), що виражаються у розголошенні службовою особою лікувального закладу, допоміжним працівником, який самочинно здобув інформацію, або медичним працівником відомостей про проведення медичного огляду особи на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби, що є небезпечною для життя людини, або захворювання на синдром набутого імунодефіциту (СНІД) та його результатів, що стали їм відомі у зв’язку з виконанням службових або професійних обов’язків.

Злочин характеризується наявністю спеціального суб’єкту, а саме: службова особа лікувального закладу (директори, головні лікарі, керівники структурних підрозділів поліклінік, лікарень, диспансерів та інших акредитованих закладів охорони здоров’я), медичні та інші працівники. Суб’єктивна сторона злочину характеризується умислом або необережністю.

До кримінальних правопорушень у сфері охорони професійної таємниці також належить злочин, передбачений ст. 397 КК України – «Втручання в діяльність захисника чи представника особи».

Суспільна небезпечність цього злочину полягає в тому, що він порушує нормальну діяльність осіб, які надають необхідну правову допомогу

юридичним і фізичним особам у захисті їхніх законних інтересів в цивільному, адміністративному і кримінальному судочинстві.

Об'єктивна сторона злочину може характеризуватися діями або бездіяльністю і проявляється у формі:

1) вчинення будь-яких перешкод до здійснення правомірної діяльності захисника чи представника особи з надання правової допомоги;

2) порушенні встановлених законом гарантій їх діяльності та професійної таємниці. Таке порушення може виражатися у проханні, вимозі, примушуванні надати відомості, що становлять зміст адвокатської таємниці, примусовому вилученні, огляді документів, пов'язаних з виконанням захисником його обов'язків, а також розголошенні змісту таких документів.

Суб'єктивна сторона злочину, передбаченого ст.397 КК України, припускає наявність тільки прямого умислу. Суб'єктом злочину за ч.1 ст.397 КК України є фізична, осудна особа, яка досягла 16-річного віку, а за ч.2 ст.397 КК України – тільки службова особа.

Суміжною до професійних таємниць, охорона яких забезпечується нормами чинного КК України, є банківська таємниця. Її основна відмінність від професійних таємниць полягає в тому, що інформація, яка становить зміст банківської таємниці, довіряється не особі, яка належить до певної професії, а конкретній організації – банківській установі.

Чинний КК України містить два склади злочинів у сфері обігу банківської інформації, а саме: ст. 231 КК України – «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю» і ст. 232 КК України – «Розголошення комерційної або банківської таємниці».

Об'єктивна сторона злочину, передбаченого ст. 231 КК України може виражатися у двох формах: 1) вчинення дій, спрямованих на отримання відомостей, що становлять комерційну або банківську таємницю; 2) незаконне використання відомостей, що становлять комерційну або банківську таємницю. Обов'язковою ознакою другої форми об'єктивної сторони є –

наслідок вчинення суспільно небезпечних дій, а саме нанесення істотної шкоди суб'єкту господарської діяльності. При цьому слід враховувати, що істотна шкода – є оціночною категорією, її характер і розмір у кожному випадку вирішується окремо.

Суб'єктивна сторона злочину виражається по-різному: для першої форми вчинення злочину – прямий умисел на вчинення протиправних дій і спеціальна мета – розголошення чи іншого використання цих відомостей, а для другої форми – прямий умисел для вчинення протиправних дій і умисел або необережність щодо заподіяння істотної шкоди суб'єкту господарювання.

Об'єктивна сторона злочину, передбаченого ст. 232 КК України виражається у формі розголошення комерційної або банківської таємниці, тобто доведенні її без згоди власника до відома хоча б однієї особи, яка раніше не була ознайомлена з відповідною інформацією. Як і в ст. 231 КК України, обов'язковим елементом об'єктивної сторони ст. 232 КК України є настання наслідків, що знаходить вираз у нанесенні істотної шкоди суб'єкту господарювання.

Суб'єктом злочину є особа, яка в силу своїх професійних або службових обов'язків мала доступ до банківської або комерційної таємниці.

Суб'єктивна сторона характеризується прямим умислом і корисливим чи іншим особистим мотивом. Таким мотивом може бути бажання отримати матеріальні блага для себе або інших осіб, одержати або зберегти певні майнові права, уникнути матеріальних витрат чи обов'язків або досягти іншої матеріальної вигоди.

Суміжними складами злочинів до правопорушень у сфері обігу банківської або комерційної таємниці є діяння, що посягають на встановлений порядок обігу інсайдерської інформації. Ст. 232^1 КК України встановлює відповідальність за незаконне використання інсайдерської інформації, що відображається у її розголошенні чи іншому використанні і може суттєво вплинути на ринкову вартість цінних паперів компанії. Такі дії

можуть виражатися у доведенні до відома сторонніх осіб інформації про зміну нової стратегії підприємства, підготовку до випуску нового продукту, скуповування контрольного пакета акцій, наданні консультацій іншим особам щодо їх угод чи операцій на основі відповідної інформації тощо.

Суб'єкт злочину спеціальний – це особа, яка одержує інсайдерську інформацію у зв'язку зі своєю професійною чи службовою діяльністю.

Суб'єктивна сторона злочину характеризується прямим умислом винного стосовно злочинного діяння та прямим чи непрямим умислом стосовно наслідків злочину – спричинення істотної шкоди охоронюваним законом правам, свободам та інтересам окремих громадян, державним чи громадським інтересам, або інтересам юридичних осіб.

Ст. 232^2 КК України встановлює відповідальність за приховування інформації про діяльність емітента.

Об'єктивна сторона злочину, передбаченого ст. 232^2 КК України виражається у двох формах: 1) ненаданні службовою особою емітента інвестору в цінні папери (у тому числі акціонеру) на його письмовий запит інформації про діяльність емітента в межах, передбачених законом; 2) наданні йому недостовірної інформації. Обов'язковим елементом об'єктивної сторони є наслідки – заподіяння інвестору в цінні папери (у тому числі акціонеру) матеріальної шкоди в значному розмірі.

Суб'єктивна сторона злочину характеризується прямим умислом стосовно злочинного діяння та прямим чи непрямим умислом стосовно наслідків. Суб'єкт злочину – спеціальний, службова особа емітента.

Суміжною до професійних таємниць, охорона яких забезпечується нормами чинного КК України, є таємниця досудового розслідування. Основна відмінність цієї таємниці полягає в тому, що рішення про обсяг і час її розкриття приймають спеціально уповноваженні органи, що займаються досудовим провадженням. Чинний Кримінальний процесуальний кодекс України у встановлює, що відомості досудового розслідування можна розголошувати лише з дозволу слідчого або прокурора і в тому обсязі, в

якому вони визнають можливим. У необхідних випадках слідчий, прокурор попереджає осіб, яким стали відомі відомості досудового розслідування, у зв'язку з участю в ньому, про їх обов'язок не розголошувати такі відомості без його дозволу. Незаконне розголошення відомостей досудового розслідування тягне за собою кримінальну відповідальність, встановлену законом (ст. 222 КПК України).

Ст. 387 КК України встановлює відповідальність за розголошення даних оперативно-розшукової діяльності, досудового розслідування таємниці досудового розслідування, що виражається у:

– розголошенні без дозволу прокурора, слідчого або особи, яка провадила оперативно-розшукову діяльність, даних оперативно-розшукової діяльності або досудового розслідування особою, попередженою в установленому законом порядку про обов'язок не розголошувати такі дані (ч.1 ст.387 КК України);

– розголошенні даних оперативно-розшукової діяльності, досудового розслідування, вчинене суддею, прокурором, слідчим, працівником оперативно-розшукового органу незалежно від того, чи приймала ця особа безпосередню участь в оперативно-розшуковій діяльності, досудовому розслідуванні, якщо розголошені дані ганьблять людину, принижують її честь і гідність (ч.2 ст.387 КК України).

Характеризуючи склад злочину, передбачений ст. 387 КК України, слід зауважити на тому, що стаття 9 Закону України «Про доступ до публічної інформації» передбачає можливість віднесення даних, зібраних в процесі оперативно-розшукової діяльності, до службової інформації. Остання є схожим видом діяльності до досудового розслідування, але законодавець не відніс дані досудового розслідування до предмету захисту службової інформації. З цього можна зробити висновок, що інформації, отриманої під час досудового розслідування, надано більший захист від розголошення шляхом встановлення її таємниці.

Суб'єктивна сторона злочину характеризується прямим умислом Суб'єкт злочину – спеціальний: за ч. 1 ст. 387 КК України відповідальність можуть нести тільки свідок, потерпілий, цивільний позивач, цивільний відповідач, захисник, експерт, спеціаліст, перекладач, понятий, а також інші особи, які присутні при провадженні слідчих дій і попереджені про обов'язок не розголошувати даних досудового слідства чи дізнання, а за ч.2 ст.387 КК України – суддя, прокурор, слідчий, працівник оперативно-розшукового органу незалежно від того, чи брали вони безпосередню участь у проведенні оперативно-розшукової діяльності, досудовому розслідуванні.

Посяганням на встановлений законом порядок забезпечення таємниці слідства та конфіденційності іншої інформації, пов'язаної з виявленням та розкриттям злочинів і розслідуванням кримінальних справ, слід визнавати злочин, передбачений ст.381 КК України – «Розголошення відомостей про заходи безпеки щодо особи, взятої під захист».

Основним безпосереднім об'єктом злочину є інтереси правосуддя в частині забезпечення безпеки осіб, взятих під захист, та належне здійснення правосуддя, а додатковим – життя і здоров'я особи, майнові чи інші блага.

Предмет злочину становлять відомості про заходи безпеки щодо особи, взятої під захист. Перелік таких заходів встановлюється Законом України «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві». Це може бути інформація про особисту охорону, охорону житла і майна особи, взятої під захист, про зміну її місця роботи або навчання, про переселення в інше місце проживання, про зміну прізвища чи інших конфіденційних відомостей про цю особу тощо.

Об'єктивна сторона злочину характеризується діянням – розголошення відомостей, та наслідками – спричинення шкоди здоров'ю особи, взятої під захист (ч. 1 ст. 381 КК України), її смертю або іншими тяжкими наслідками (ч. 2 ст. 381 КК України).

Суб'єкт злочину спеціальний: 1) службова особа, якою прийнято рішення про заходи безпеки; 2) особа, яка здійснює ці заходи; 3) службова

особа, якій вказані рішення стали відомі у зв'язку з її службовим становищем; 4) особа, взята під захист.

Суб'єктивна сторона характеризується складною формою вини – щодо самого факту розголошення характеризується умисної або необережною формою вини, стосовно наслідків розголошення вина може бути тільки необережною.

Злочини у сфері обігу інформації, що становить зміст таємниці особистого життя, зосереджені у Розділі V Особливої частини КК України «Злочини проти виборчих, трудових та інших особистих прав і свобод людини і громадянина» і передбачають відповідальність за розголошення відомостей, що становлять зміст таємниці кореспонденції (листування, телефонних розмов, телеграфної та іншої кореспонденції), таємниці усиновлення та таємниці голосування.

Таємниця голосування, як вид таємної інформації, поширюється на пряме волевиявлення виборців при обранні органів державної влади та органів місцевого самоврядування. Право на таємницю голосування є невід'ємним правом громадянина і гарантується Конституцією України.

Ст. 159 чинного КК України передбачає відповідальність за порушення таємниці голосування, що виражається у розголошенні змісту волевиявлення громадянина, який взяв участь у виборах або референдумі.

Розголошення змісту волевиявлення громадянина означає, що особа, якій став відомий зміст такого волевиявлення, ознайомлює з ним сторонніх осіб або своєю поведінкою створює умови, які надають стороннім особам можливість ознайомитися зі змістом волевиявлення громадянина. Способи розголошення змісту волевиявлення громадянина можуть бути різними (повідомлення в розмовах з іншими особами, оприлюднення в ЗМІ, демонстрація відеозапису заповнення громадянином бюлетеня тощо).

Суб'єктивна сторона злочину характеризується прямим умислом: винний усвідомлює, що порушує таємницю голосування, і бажає вчинити такі дії. Порушення таємниці голосування, вчинене з необережності,

виключає відповідальність за ст. 159 КК України і за наявності відповідних підстав може розглядатися як службова недбалість (ст. 367 КК України).

Суб'єкт злочину загальний – фізична осудна особа, яка досягла 16-річного віку. Кваліфікуючими ознаками порушення таємниці голосування є вчинення його: 1) членом виборчої комісії або комісії з референдуму; 2) іншою службовою особою з використанням свого службового становища (ч. 2 ст. 159 КК України).

Ст.163 КК України передбачає відповідальність за порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер. Предметом даного злочину є відомості, що передані чи передаються громадянами через листування або телефонні розмови, а також повідомлення громадян, які передаються або були передані телеграфом чи за допомогою інших засобів зв'язку, а також через комп'ютер і становлять таємницю громадянина.

З об'єктивної сторони злочин характеризується активними діями, що можуть проявлятися в ознайомленні з особистою кореспонденцією без згоди адресата, прослуховуванні телефонних переговорів, повідомленні сторонніх осіб про факт листування, телефонної розмови тощо.

Суб'єкт злочину загальний – фізична осудна особа, яка досягла 16-річного віку. Суб'єктивна сторона характеризується прямим умислом. Особа усвідомлює, що незаконно ознайомлюється із відомостями або повідомленнями громадянина, які передаються засобами зв'язку чи через комп'ютер, і бажає вчинити такі дії.

Невід'ємною складовою інституту таємниці особистого життя особи є таємниця усиновлення, зміст якої становлять відомості, що перебувають у власності лише членів сім'ї (як виняток, і у володінні спеціально уповноважених осіб), і розголошення яких може призвести до заподіяння значної шкоди її носіям. Розголошення таємниці усиновлення є кримінально караним діянням, відповідальність за яке передбачена ст. 168 КК України.

З об’єктивної сторони злочин виражається у розголошенні таємниці усиновлення (удочеріння) всупереч волі усиновителя (удочерителя) і може полягати в усному чи письмовому повідомленні будь-якій особі інформації щодо самого факту усиновлення (удочеріння), біологічних батьків, дійсного місця і дати народження, прізвища та ім’я усиновленого, часу прийняття рішення про усиновлення (удочеріння) та реєстрації цього факту.

Суб’єкт злочину загальний – фізична осудна особа, яка досягла 16-річного віку і якій стала відома таємниця усиновлення (удочеріння).

Суб’єктивна сторона злочину характеризується умислом, до тяжких наслідків психічне ставлення виражається у формі необережності.

Прийняття Закону України «Про доступ до публічної інформації» зумовило внесення відповідних змін до кримінального законодавства у частині забезпечення охорони службової інформації1. Як зазначалось раніше, предметом службової інформації є відомості, що 1) міститься в документах суб’єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов’язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень; 2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Важливими для характеристики режиму охорони службової таємниці є положення ст. 9 Закону України «Про доступ до публічної інформації», якими означено, що суб’єкти владних повноважень не зобов’язані автоматично відносити певну інформацію до службової, це відбувається лише за відповідної потреби. Такий законодавчий підхід зумовлює і

1 Попередня редакція КК України передбачала таке поняття як «конфіденційна інформація, що є власністю держави». Такий статус міг довільно надаватися будь-якій інформації «з метою її збереження», що призводило до зловживань і надмірного обмеження доступу до інформації.

встановлення особливого порядку зберігання та обігу службової інформації, але не доступу, порядок якого визначається виключно законом.

Ст. 330 КК України встановлює відповідальність за передачу або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни. Об'єктом даного злочину є суспільні відносини з охорони службової інформації у різних сферах діяльності держави.

Об'єктивна сторона злочину виражається у двох формах: 1) передача відомостей, що становить службову таємницю іноземним підприємствам, установам, організаціям або їх представникам 2) збирання таких відомостей з метою передачі іноземній державі, іноземній організації або їх представникам.

Суб'єкт злочину спеціальний – особа, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових обов'язків.

Суб'єктивна сторона характеризується прямим умислом, проте передача або збирання службової інформації не повинні містити ознак державної зради або шпигунства, тобто умисел не повинен бути спрямованим на нанесення шкоди основам національної безпеки.

Відмова законодавця від уживання терміну «конфіденційна інформація, що є власністю держави» призвела до нового розуміння змісту поняття конфіденційності інформації. Закон України «Про доступ до публічної інформації» розглядає конфіденційну інформацію як об'єкт особистих нематеріальних прав фізичної чи юридичної особи. Такий підхід відповідає Конституції України, яка закріплює права на отримання, зберігання і поширення інформації, а також право на недоторканність особистого і сімейного життя.

Кримінальне законодавство України забезпечує охорону конфіденційної інформації про особу шляхом встановлення відповідальності за порушення недоторканності особистого і сімейного життя. Ст. 182 КК України «Порушення недоторканності приватного життя» визнає

злочинними дії, спрямовані на незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконну зміну такої інформації.

Об'єктивна сторона злочину, передбаченого ст. 182 КК України, проявляється у таких формах:

1) незаконне збирання конфіденційної інформації про особу, тобто отримання відомостей про особу у будь-який спосіб (відкрито або таємно), у тому числі шляхом викрадення, використання прослуховуючих, відео записуючих, інших технічних пристроїв ;

2) незаконне зберігання конфіденційної інформації – накопичення відомостей про особу у певному місці на будь-яких матеріальних носіях;

3) незаконне використання конфіденційної інформації – користування за власним розсудом відомостями, які становлять особисту чи сімейну таємницю особи, для задоволення певної потреби чи одержання певної вигоди (використання інформації про особу з метою її шантажу, залякування, примушування до вчинення певних дій кваліфікується за сукупністю злочинів, передбачених відповідними нормами Особливої частини КК України);

4) незаконне поширення конфіденційної інформації про особу – повідомлення будь-яким способом (усно, письмово, друкованим способом, за допомогою комп'ютерної мережі тощо) такої інформації невизначеному числу осіб (хоча б одній людині);

5) незаконна зміна конфіденційної інформації виражається – умисне перекручення відомостей, що становлять особисту чи сімейну таємницю особи, для задоволення власних потреб.

Суб'єкт злочину загальний – фізична осудна особа, яка досягла 16-річного віку. З суб'єктивної сторони злочин характеризується умислом.

Окрему групу кримінальних правопорушень, відповідальність за які встановлюється чинним КК України, становлять злочини, спрямовані на порушення обігу інформації, що не є обмеженою у доступі, проте її

використання також відбувається у чітко визначеному законодавчому порядку. Об'єктивна сторона таких діянь може виражатися у:

1) наданні завідомо неправдивої інформації (ст.158, ч.1 ст.209^1, ч.1 ст.223^2, ст.238, ст.259, ст.358, ч.1 ст.366, ч.1 ст.383, ч.1 ст.384 КК України);

2) приховуванні або неподанні інформації (ст.136, ч.1 ст.209, ч.1 ст.209^1, ч.1 ст. 238^2, ст.238, ч.3 ст.243, ст.285, ч.1 ст.385, ст.396 КК України).

7.2.2 Адміністративні правопорушення у сері обігу інформації з обмеженим доступом

Чинний КУпАП містить понад п'ятдесят складів правопорушень у сфері створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації. Утім для адміністративного законодавства характерним є відсутність єдиного розділу, який охоплював би зазначені правопорушення. Адміністративно-правове закріплення правопорушень у сфері обігу інформації з обмеженим доступом не є виключенням – конкретні статті КУпАП, що визначають підстави адміністративної відповідальності за вчинення таких проступків міститься в різних главах його Особливої частини. З урахуванням законодавчо визначених видів інформації з обмеженим доступом доцільно розглядати питання адміністративної відповідальності у сфері обігу інформації з обмеженим доступом.

Чинний КУпАП встановлює відповідальність за порушення законодавства про державну таємницю. Нормативні приписи ст. 212^2 КупАП («Порушення законодавства про державну таємницю») закріплюють дев'ять форм об'єктивної сторони зазначеного проступку, зокрема:

1) недодержання встановленого законодавством порядку передачі державної таємниці іншій державі чи міжнародній організації;

2) засекречування інформації:

– про стан довкілля, про якість харчових продуктів і предметів побуту;

– про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися та загрожують безпеці громадян;

– про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти та культури населення;

– про факти порушень прав і свобод людини і громадянина;

– про незаконні дії органів державної влади, органів місцевого самоврядування та їх посадових осіб;

– іншої інформації, яка відповідно до законів та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, не може бути засекречена;

3) безпідставне засекречування інформації;

4) надання грифа секретності матеріальним носіям конфіденційної або іншої таємної інформації, яка не становить державної таємниці, або ненадання грифа секретності матеріальним носіям інформації, що становить державну таємницю, а також безпідставне скасування чи зниження грифа секретності матеріальних носіїв секретної інформації;

5) порушення встановленого законодавством порядку надання допуску та доступу до державної таємниці;

6) невжиття заходів щодо забезпечення охорони державної таємниці та незабезпечення контролю за охороною державної таємниці;

7) провадження діяльності, пов'язаної з державною таємницею, без отримання в установленому порядку спеціального дозволу на провадження такої діяльності, а також розміщення державних замовлень на виконання робіт, доведення мобілізаційних завдань, пов'язаних з державною таємницею, в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах, організаціях, яким не надано спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею;

8) недодержання вимог законодавства щодо забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва, прийому іноземних делегацій, груп, окремих іноземців та осіб без громадянства та проведення роботи з ними;

9) невиконання норм і вимог криптографічного та технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення її конфіденційності, цілісності і доступності.

Суб'єктивна сторона правопорушення характеризується наявністю вини у формі умислу. Суб'єктами цього можуть бути як посадові особи, так і громадяни.

Адміністративним правопорушенням також визнається порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію (ст. 212^5 КУпАП).

Об'єктивна сторона правопорушення, передбаченого ст. 212^5 КУпАП полягає у недодержанні або невиконанні порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, що призвело до розголошення такої інформації. З суб'єктивної сторони зазначене правопорушення характеризується наявністю вини як у формі умислу, так і у формі необережності, а суб'єктами є особи, яким ця інформація була довірена у процесі виконання посадових або службових обов'язків.

Суміжним складом адміністративного правопорушення у сфері обігу службової інформації слід визнавати дії, передбачені ст. 172^8 КУпАП («Незаконне використання інформації, що стала відома особі у зв'язку з виконанням службових повноважень»). Об'єктивна сторона зазначеного правопорушення може виражатися у двох формах: 1) незаконне розголошення інформації, що стала відома особі у зв'язку з виконанням службових повноважень; 2) використання в інший спосіб особою у своїх інтересах інформації, яка стала їй відома у зв'язку з виконанням службових

повноважень. Суб'єкт адміністративного проступку – спеціальний, ним можуть бути особи, уповноважені на виконання функцій держави або місцевого самоврядування. Суб'єктивна сторона правопорушення визначається ставленням до наслідків і характеризується наявністю вини у формі прямого чи непрямого умислу.

Комплексом адміністративно-правових норм охороняються суспільні відносини у сфері обігу цінних паперів та фондового ринку. Так, законодавець передбачає відповідальність за:

– порушення вимог законодавчих та інших нормативних актів з емісії цінних паперів (ст. 163 КУпАП),

– порушення порядку ведення податкового обліку, надання аудиторських висновків (ст. 163^{1} КУпАП),

– приховування інформації про діяльність емітента (ст. 163^{5} КУпАП),

– незаконне використання інсайдерської інформації (ст. 163^{9} КУпАП),

– порушення порядку розкриття інформації на фондовому ринку (ст. 163^{11} КУпАП).

З об’єктивної сторони зазначені склади правопорушень характеризуються як активними діями (порушення встановленого законом порядку ведення податкового обліку, розкриття на фондовому ринку інформації не в повному обсязі або розкриття недостовірної інформації. розголошення, передача або наданні доступу до інсайдерської інформації), так і бездіяльністю (неподання або несвоєчасне подання відповідної інформації). Суб’єктивна сторона означених правопорушень характеризується наявністю вини у формі умислу або необережності. Суб’єктами можуть виступати посадові особи, які мають доступ до відповідної інформації у зв’язку з виконанням ними службових обов’язків або договірних зобов’язань, у тому числі співробітники фондового ринку, аудитори, нотаріуси, експерти, оцінювачі, арбітражні керуючі або інші особи, які виконують надані законом публічні повноваження.

Чинний КУпАП також містить норми, що визначають підстави відповідальності за недобросовісну конкуренцію. Ст. 1 Закону України «Про захист від недобросовісної конкуренції» визначає недобросовісну конкуренцію як будь-які дії у конкуренції, що суперечать торговим та іншим чесним звичаям у господарській діяльності. Також Закон визнає недобросовісною конкуренцією неправомірне збирання комерційної таємниці, розголошення комерційної таємниці, схилення до розголошення комерційної таємниці, неправомірне використання комерційної таємниці.

Нормативні приписи ст. 164^3 КУпАП до недобросовісної конкуренції включає не всі дії, що визначені Законом України «Про захист від недобросовісної конкуренції». Об'єктивну сторону цього правопорушення становлять: 1) незаконне копіювання форми, упаковки, зовнішнього оформлення, а так само імітація, копіювання, пряме відтворення товару іншого підприємця, самовільне використання його імені (ч.1 ст. 164^3 КУпАП); 2) умисне поширення неправдивих або неточних відомостей, які можуть завдати шкоди діловій репутації або майновим інтересам іншого підприємця (ч.2 ст. 164^3 КУпАП); 3) отримання, використання, розголошення комерційної таємниці, а також іншої конфіденційної інформації з метою заподіяння шкоди діловій репутації або майну іншого підприємця (ч.3 ст. 164^3 КУпАП). Втім, вчинення інших протиправних дій, визначених Законом України «Про захист від недобросовісної конкуренції», не виключає можливості настання адміністративної відповідальності та застосування до винної особи відповідних заходів. Суб'єктивна сторона правопорушень, передбачених коментованою статтею, характеризується наявністю прямого умислу. Суб'єктами вчинення протиправних дій можуть бути посадові особи підприємств, установ та організацій усіх форм власності та громадяни, які займаються підприємницькою діяльністю та громадяни, що не є підприємцями і вчинили винні діяння в інтересах третіх осіб.

Ст. 185^{11} КУпАП передбачає настання адміністративної відповідальності за розголошення відомостей про заходи безпеки, щодо особи, взятої під захист. Суб'єктом зазначеного правопорушення може виступати особа, щодо якої застосовуються заходи безпеки, а суб'єктивна сторона характеризується наявністю вини як у формі умислу, так і формі необережності. Для правильної оцінки протиправності зазначених дій також необхідно враховувати, що розголошення відомостей про заходи безпеки тягне за собою адміністративну відповідальність, якщо це не призвело чи могло призвести до тяжких наслідків, у протилежному випадку такі дії є підставою для настання кримінальної відповідальності.

Чинний КУпАП встановлює адміністративну відповідальність за порушення законодавства у сфері захисту персональних даних (ст.188^{39} КУпАП). Об'єктивна сторона зазначеного правопорушення знаходить вираз у:

- неповідомленні або несвоєчасному повідомленні суб'єкта персональних даних про його права у зв'язку із включенням його персональних даних до бази персональних даних, мету збору цих даних та осіб, яким ці дані передаються;

- недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних у базі персональних даних, що призвело до незаконного доступу до них.

Важливість закріплення зазначених форм об'єктивної сторони спрямована на унеможливлення зловживання та незаконного використання персональних даних, уникнення заподіяння шкоди суб'єкту персональних даних.

Адміністративними правопорушеннями у сфері обігу інформації з обмеженим доступом також є неправомірні дії у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Об'єктивна сторона зазначених правопорушень може виражатися у наступних формах:

– здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в інформаційних (автоматизованих) системах (ч.1 ст. 212[6] КУпАП);.

– здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в інформаційних (автоматизованих) системах, призначених для зберігання та обробки інформації з обмеженим доступом, (ч.3 ст. 212[6] КУпАП);.

– незаконне копіювання інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі (ч.4 ст. 212[6] КУпАП);.

– безоплатне незаконне розповсюдження інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі (ч.4 ст. 212[6] КУпАП);.

– незаконний збут інформації, яка зберігається в інформаційних (автоматизованих) системах, у паперовій чи електронній формі (ч.5 ст. 212[6] КУпАП).

Суб'єктивна сторона таких правопорушень характеризується наявністю виключно умисною формою вини, суб'єктом є фізична осудна особа, яка на момент вчинення адміністративного правопорушення досягла 16–річного віку.

7.2.3 Цивільні правопорушення у сері обігу інформації з обмеженим доступом

Цивільний кодекс України (надалі ЦК України) відносить інформацію до нематеріальних об'єктів цивільних прав, що надає передусім немайнового характеру безпосередньому протиправному впливу інформаційного правопорушення. У зв'язку з цим, дослідження цивільно-правової відповідальності у сфері обігу інформації з обмеженим доступом

здійснюється крізь призму особистих немайнових прав, порушення яких становить зміст цивільно-правового правопорушення.

Чинний ЦК України, насамперед, забезпечує захист інформації про особисте життя фізичної особи. Відповідно до ст. 302 ЦК України («Право на інформацію») збирання, зберігання, використання і поширення інформації про особисте життя фізичної особи без її згоди не допускаються, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. При цьому зміст та обсяг інформації, що становить таємницю особисте життя, фізична особа визначає самостійно (ст.301 ЦК України).

Цивільно-правовому захисту підлягає також інформація про особисте життя фізичної особи, що міститься в особистих паперах (ст.303 ЦК України). До особистих паперів, зокрема, належать документи, фотографії, щоденники чи інші записи, особисті архівні матеріали тощо. Право на особисті папери включає в себе можливість надавати згоду чи забороняти ознайомлення з ними, використовувати та розпоряджатися ними за волею власника. Тобто фізична особа самостійно обмежує доступ до інформації, що міститься в особистих паперах, колу осіб, які можуть ознайомлюватись та використовувати, зокрема шляхом опублікування, її особисті папери.

Цивільне законодавство забезпечує захист права особи на таємницю кореспонденції. Відповідно до ст. 306 ЦК України фізична особа має право на таємницю листування, телеграм, телефонних розмов, телеграфних повідомлень та інших видів кореспонденції. Листи, телеграми та інші види кореспонденції можуть використовуватися, зокрема шляхом опублікування, лише за згодою особи, яка направила їх, та адресата. Якщо кореспонденція стосується особистого життя іншої фізичної особи, для її використання, зокрема шляхом опублікування, потрібна згода цієї особи. Кореспонденція, яка стосується фізичної особи, може бути долучена до судової справи лише у разі, якщо в ній містяться докази, що мають значення для вирішення справи.

Інформація, яка міститься в такій кореспонденції, не підлягає розголошенню. Порушення таємниці кореспонденції може бути дозволено судом у випадках, встановлених законом, з метою запобігання злочинові чи під час кримінального провадження, якщо іншими способами одержати інформацію неможливо.

Чинний ЦК України у визначених законом випадках гарантує обмеження доступу до інформації, зміст якої становлять персональні данні особи. Так, відповідно до положень ст. 296 ЦК України («Право на використання імені»), використання імені фізичної особи в літературних та інших творах, крім творів документального характеру, як персонажа (дійової особи) допускається лише за її згодою, а після її смерті - за згодою її дітей, вдови (вдівця), а якщо їх немає, - батьків, братів та сестер. Ім'я фізичної особи, яка затримана, підозрюється чи обвинувачується у вчиненні кримінального правопорушення, або особи, яка вчинила адміністративне правопорушення, може бути використане (обнародуване) лише в разі набрання законної сили обвинувальним вироком суду щодо неї або винесення постанови у справі про адміністративне правопорушення та в інших випадках, передбачених законом. Ім'я потерпілого від правопорушення може бути обнародуване лише за його згодою. Ім'я учасника цивільного спору, який стосується особистого життя сторін, може бути використане іншими особами лише за його згодою.

Також цивільне законодавство захищає інформацію щодо персональних даних донора і реципієнта: особа донора не повинна бути відомою реципієнту, а особа реципієнта - родині донора, крім випадків, коли реципієнт і донор перебувають у шлюбі або є близькими родичами (ст.290 ЦК України)

Цивільно-правове регулювання поширюється і на інформацію, яка має візуальну форму закріплення. Зокрема, фотографія, інші художні твори, на яких зображено фізичну особу, можуть бути публічно показані, відтворені, розповсюджені лише за згодою цієї особи. Фотографія може бути

розповсюджена без дозволу фізичної особи, яка зображена на ній, якщо це викликано необхідністю захисту її інтересів або інтересів інших осіб (ст. 308 ЦК України).

Нормативні приписи чинного цивільного законодавства забезпечують охорону інформації, що становить зміст лікарської таємниці. Відповідно до ст. 286 ЦК України («Право на таємницю про стан здоров'я»), кожна фізична особа має право на таємницю про стан свого здоров'я, факт звернення за медичною допомогою, діагноз, а також про відомості, одержані при її медичному обстеженні. Законом в імперативній формі також встановлено заборону вимагати та подавати за місцем роботи або навчання інформацію про діагноз та методи лікування фізичної особи, а також закріплено зобов'язання фізичної особи утримуватися від поширення зазначеної інформації, якщо вона стала їй відома у зв'язку з виконанням службових обов'язків або з інших джерел.

У сфері цивільного обігу інформації з обмеженим доступом особливе місце посідають банківська і комерційна таємниці.

У науковій літературі поняття банківської таємниці розглядається у вузькому та широкому розумінні. У вузькому розумінні банківська таємниця це обов'язок банку зберігати в таємниці операції клієнтів від сторонніх осіб, насамперед конкурентів того чи іншого клієнта банку, операції, рахунки та вклади (депозити) своїх клієнтів і кореспондентів. У широкому розумінні – це різновид таємної інформації, тобто інформації щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку. У силу своєї специфіки, інформація, яка становить банківську таємницю, не може розглядатися як товар, оскільки зобов'язання банка полягають у збереженні банківської таємниці, а не здійсненні інформаційної діяльності.

Ст. 1076 ЦК України («Банківська таємниця») закріплює обов'язок банку зберігати таємницю банківського рахунка, операцій за рахунком і

відомостей про клієнта, а також визначає, що у разі розголошення банком відомостей, що становлять банківську таємницю, клієнт має право вимагати від банку відшкодування завданих збитків та моральної шкоди.

На відміну від банківської, комерційна таємниця забезпечена майновими правами інтелектуальної власності , якими є:

- право на використання комерційної таємниці;
- виключне право дозволяти використання комерційної таємниці;
- виключне право перешкоджати неправомірному розголошенню, збиранню або використанню комерційної таємниці;
- інші майнові права інтелектуальної власності, встановлені законом.

Майнові права інтелектуальної власності на комерційну таємницю належать особі, яка правомірно визначила інформацію комерційною таємницею, якщо інше не встановлено договором (Ст. 506 ЦК України).

Отже, відновлення порушених особистих немайнових прав на інформацію, у тому числі з обмеженим доступом, реалізовується через можливість суб'єкта відносин у сфері інформації вимагати усунення порушень його права та відшкодування майнової і моральної шкоди, завданої такими правопорушеннями (ст. 200 ЦК України). Водночас немайновий характер інформаційного правопорушення ускладнює вирішення питання про відновлення порушеного становища (права) потерпілого або компенсації нанесених правопорушенням шкоди, збитків, упущеної вигоди, що забезпечується відповідними заходами державного примусу, передбаченими нормами цивільного права.

Виключенням у цій ситуації є комерційна таємниця, яка безпосередньо Цивільним кодексом України визначається як інформація (ст. 505 ЦК України). Особливості цивільно-правового режиму комерційної таємниці полягають у тому, що на відміну від іншої інформації законом встановлені не тільки немайнові, а й майнові права щодо неї, а також спеціальні засоби її охорони і захисту.

7.2.4 Дисциплінарні правопорушення у сері обігу інформації з обмеженим доступом

Чинне трудове законодавство України не містить чіткого визначення поняття дисциплінарного правопорушення (проступку). Утім, в теорії права дисциплінарним проступком визнається винне протиправне діяння (дія або бездіяльність), яке полягає у невиконанні або неналежному виконанні працівником покладених на нього трудових або службових обов'язків. Склад дисциплінарного проступку, як і будь-якого правопорушення, утворюють чотири елементи: об'єкт, об'єктивна сторона, суб'єкт і суб'єктивна сторона. Саме з урахуванням особливостей зазначених складових слід розкривати зміст дисциплінарного проступку в інформаційній сфері.

Об'єктом дисциплінарного правопорушення у сфері обігу інформації з обмеженим доступом є суспільні відносини, що виникають у зв'язку із створенням, збиранням, одержанням, зберіганням, використанням, поширенням, охороною та захистом інформації, яким внаслідок невиконання або неналежного виконання трудових або службових обов'язків завдається шкода.

Об'єктивна сторона таких правопорушень може виражатися як у формі активної дії, так і у формі бездіяльності, і здебільшого проявляється у невиконанні або неналежному виконанні особою своїх трудових або службових обов'язків. Найбільш поширеними з них є: необґрунтована відмова у наданні відповідної інформації, несвоєчасне надання інформації, , використання і поширення конфіденційної інформації в особистих цілях, порушення порядку обліку, зберігання й використання документів та інших носіїв інформації тощо.

Суб'єктом дисциплінарного правопорушення у сфері обігу інформації є фізична деліктоздатна особа, яка перебуває у трудових правовідносинах з роботодавцем і безпосередньо виконує дії, передбачені об'єктивною стороною конкретного проступку. Суб'єкт правопорушення у сфері обігу інформації з обмеженим доступом, переважно, *спеціальний* – працівник, на яких поширюється дія дисциплінарних статутів або спеціальних

законодавчих положень про дисципліну. Такими суб'єктами можуть виступати посадові і службові особи органів державної влади, місцевого самоврядування, особи, які виконують делеговані повноваження суб'єктів владних повноважень, забезпечують реалізацію права на доступ до інформації тощо. Особливий статус спеціальних суб'єктів зумовлює застосування до них дещо інших заходів дисциплінарного впливу (як правило, більш жорстких стягнень), які містяться у спеціальних нормативних актах.

Суб'єктивна сторона дисциплінарного проступку у сфері обігу інформації виражається у психічному ставленні порушника трудової дисципліни до своєї протиправної поведінки. Особливість суб'єктивної сторони дисциплінарних правопорушень у сфері обігу інформації з обмеженим доступом проявляється у формі вини, яка переважно характеризується необережністю і не пов'язується з настанням суспільно-небезпечних наслідків. Виявлення і доведення умисної форми вини опосередковано вказує на більш високий ступінь суспільної небезпеки, внаслідок чого такі дисциплінарні проступки можуть кваліфікуватися як відповідні, суміжні за своїм складом, адміністративні або кримінальні правопорушення в інформаційній сфері.

З урахуванням зазначених елементів складу правопорушення, поняття дисциплінарного проступку у сфері обігу інформації можна визначити як: встановлений нормами трудового законодавства (КЗпП) і суміжних галузей права порядок, якому внаслідок невиконання або неналежного виконання трудових або службових обов'язків, пов'язаних із створенням, збиранням, одержанням, зберіганням, використанням, поширенням, охороною та захистом інформації, завдається реальна шкода або створюється загроза заподіяння такої шкоди.

Більшість службовців за порушення правил дисципліни несуть відповідальність згідно з приписами трудового законодавства, а також трудових договорів або угод. Дисциплінарна відповідальність спеціальних

суб'єктів, що реалізують свої повноваження поза рамками трудового договору чи правил внутрішнього трудового розпорядку, регулюється спеціальними законами, статутами та положеннями, затвердженими повноважними органами.

ДИСЦИПЛІНАРНА ВІДПОВІДАЛЬНІСТЬ СПЕЦІАЛЬНИХ СУБ'ЄКТІВ У СЕРІ ОБІГУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

№ З/П	КАТЕГОРІЯ СПЕЦІАЛЬНОГО СУБ'ЄКТА	НОРМАТИВНИЙ ОБОВЯЗОК ЩОДО ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ	ЗАХОДИ ДИСЦИПЛІНАРНОГО СТЯГНЕННЯ
1	Військовослужбовці Збройних Сил України, Державної прикордонної служби України, Служби безпеки України, Національної гвардії України та інших військових формувань, створених відповідно до законів України, Державної спеціальної службу транспорту, Державної служби спеціального зв'язку та захисту інформації України	Військова дисципліна зобов'язує кожного військовослужбовця бути пильним, зберігати ***державну та військову таємницю*** (ст.3 Дисциплінарний статут Збройних Сил України)	- зауваження; - догана; - сувора догана; - позбавлення чергового звільнення; - призначення поза чергою в наряд ; - попередження про неповну службову відповідність; - пониження в посаді; - пониження військового звання на один ступінь; - звільнення з військової служби через службову невідповідність; - позбавлення військового звання
2	Особи рядового і начальницького складу органів внутрішніх справ України	Берегти ***державну таємницю*** (ст.7 Дисциплінарний статут органів внутрішніх справ)	- усне зауваження; - зауваження; - догана; - сувора догана; - попередження про неповну посадову відповідність; - звільнення з посади;

			- пониження в спеціальному званні на один ступінь; - звільнення з органів внутрішніх справ
3	Особи рядового і начальницького складу органів та підрозділів цивільного захисту, (в тому числі слухачів і курсантів навчальних закладів)	Зберігати ***державну таємницю та іншу охоронювану законом інформацію*** (ст.3 Дисциплінарний статут служби цивільного захисту)	- зауваження; - догана; - сувора догана; - попередження про неповну службову відповідність; - звільнення зі служби у зв'язку з систематичним невиконанням умов контракту чи через службову невідповідність
4	Поліцейські та їх керівники	Зберігати відомості, що становлять ***державну таємницю*** (ст.12 проекту Дисциплінарного статуту Національної поліції України)	- догана; - сувора догана; - попередження про неповну службову відповідність; - пониження у спеціальному званні на один ступінь; - звільнення з посади; - звільнення із служби в поліції
5	Державні службовці	Зберігати ***державну таємницю*** та ***персональні дані осіб***, що стали йому відомі у зв'язку з виконанням посадових обов'язків, а також іншу інформацію, яка відповідно до закону не підлягає розголошенню (ст.8 Закону «Про державну службу»)	- зауваження; - догана; - попередження про неповну службову відповідність; - звільнення з посади державної служби
6	Прокурори	Зберігати ***таємницю, що охороняється законом, яка стала***	- догана; - заборона на строк до одного року на

		відомою прокуророві під час виконання повноважень (ст.43 Закону України «Про прокуратуру»);	переведення до органу прокуратури вищого рівня чи на призначення на вищу посаду в органі прокуратури, в якому прокурор обіймає посаду; - звільнення з посади в органах прокуратури
7	Адвокат, помічник адвоката, стажист адвоката, особа, яка перебуває у трудових відносинах з адвокатом	Заборона без згоди клієнта розголошувати відомості, що становлять ***адвокатську таємницю,*** використовувати їх у своїх інтересах або інтересах третіх осіб (ст.21 Закону України «Про адвокатуру та адвокатську діяльність»)	- попередження; - зупинення права на заняття адвокатською діяльністю на строк від одного місяця до одного року; - для адвокатів України - позбавлення права на заняття адвокатською діяльністю з наступним виключенням з Єдиного реєстру адвокатів України, - для адвокатів іноземних держав - виключення з Єдиного реєстру адвокатів України
8	Нотаріуси	Зберігати в таємниці ***відомості, одержані ним у зв'язку з вчиненням нотаріальних дій*** (ст.5 Закону України «Про нотаріат»)	- зупинення або припинення нотаріальної діяльності приватного нотаріуса; - анулювання свідоцтва про право на заняття нотаріальною діяльністю через неодноразове порушення нотаріусом чинного законодавства при вчиненні нотаріальних дій або грубого порушення закону, яке завдало шкоди інтересам держави, підприємств,

			установ, організацій, громадян
9	Судді	Не розголошувати ***відомості, які становлять таємницю, що охороняється законом, у тому числі таємницю нарадчої кімнати і закритого судового засідання*** (ст.55 Закону України «Про судоустрій і статус суддів»)	- попередження; - догана; - сувора догана; - відсторонення від здійснення правосуддя - переведення судді до суду нижчого рівня; - висновок про направлення рекомендації до Вищої ради юстиції для вирішення питання щодо внесення подання про звільнення судді з посади з підстав порушення присяги.

Дисциплінарним проступкам, що є підставою юридичної відповідальності у сфері обігу інформації з обмеженим доступом властиві усі основні ознаки, що характеризують цей різновид правопорушень. Однак специфіка трудових і службових правовідносин, їхня соціальна спрямованість та інші чинники засвідчують особливий характер цих проступків, що зрештою впливає і на характер самої дисциплінарної відповідальності і визначення заходів дисциплінарних стягнень

Питання для самоконтролю до розділу 7

1. У чому полягає важливість і актуальність юридичної відповідальності у сфері обігу інформації з обмеженим доступом?
2. Що таке юридична відповідальність? Які у неї основні ознаки?
3. Яка мета юридична відповідальності?
4. Які функції має юридична відповідальність?
5. На яких принципах базується юридична відповідальність?
6. У чому полягає сигналізаційна (інформативна) функція юридичної відповідальності?
7. Що є загальними підставами юридичної відповідальності?

8. Які існують види правопорушень у сфері обігу інформації з обмеженим доступом?

9. Що таке юридичний склад правопорушення, які його основні елементи?

10. Назвіть характерні ознаки адміністративної відповідальності в інформаційній сфері.

11. Розкрийте зміст підстав кримінальної відповідальності у сфері обігу інформації з обмеженим доступом.

12. Визначте співвідношення кримінальної, адміністративної і дисциплінарної відповідальності за правопорушення в інформаційній сфері.

13. За якими критеріями будується класифікація злочинів у сфері обігу інформації з обмеженим доступом?

14. Розкрийте зміст підстав адміністративної відповідальності в інформаційній сфері.

15. Охарактеризуйте елементи складу адміністративного правопорушення у сфері обігу інформації з обмеженим доступом.

16. З урахуванням структури Особливої частини чинного КУпАП здійсніть юридичний аналіз відповідних складів правопорушень у сфері обігу інформації з обмеженим доступом.

17. Назвіть основні ознаки цивільно-правової відповідальності.

18. Наведіть приклади інформаційних цивільних прав, порушення яких може спричинити цивільно-правову відповідальність.

19. Які засоби захисту інформаційних правовідносин передбачені цивільним законодавством України?

20. Охарактеризуйте місце дисциплінарної відповідальності в механізмі забезпечення інформаційних правовідносин.

21. Дайте визначення поняття об'єкту дисциплінарного проступку у сфері обігу інформації з обмеженим доступом.

22. У чому проявляються особливості об'єктивної сторони дисциплінарного проступку у сфері обігу інформації з обмеженим доступом?

23. Розкрийте зміст суб'єктивних ознак дисциплінарного проступку в інформаційній сфері.

24. Охарактеризуйте співвідношення загальної і спеціальної дисциплінарної відповідальності у сфері обігу інформації з обмеженим доступом.

Література

1. Адміністративне право: Підручник / Ю. П. Битяк (кер. авт. кол.), Андрусів Г. В. Кримінальне право України. Особлива частина: Посібник для підготовки для іспитів/ Г. В. Андрусів, О. Ф. Бантишев, Б. В. Романюк. – К. : Вид. Паливода А. В., 2002.

2. Андрушко А.В. Дисциплінарний проступок як підстава дисциплінарної відповідальності / Андрушко А.В. // Держава і право: зб. наукових праць. Юридичні і політичні науки / Інститут держави і права ім.Корецького В.М. НАН України. – Київ, 2008. – Вип. 41. – С. 380-387.

3. Андрушко А. В. Основні проблеми загальної дисциплінарної відповідальності у трудовому праві / А. В. Андрушко // Держава і право: зб. наукових праць. Юридичні і політичні науки / Інститут держави і права ім. Корецького В. М. НАН України. – Київ, 2007. – Вип. 37. – С. 371–377.

4. Бантишев О. Кримінальна відповідальність за злочини проти національної безпеки України (проблеми кваліфікації) : Монографія / О. Бантишев, О. Шамара. – 3-те вид., перероб. та доп. – Луганськ : ТОВ «Віртуальна реальність», 2014. – 198 с.

5. Бантишев О. Ф. Кримінальне право України у питаннях і відповідях : посібник / О. Ф. Бантишев, С. А. Кузьмін. – К. : Вид. Паливода А. В., 2009. – 300 с.

6. Бітяк Ю.П. Адміністративне право України в схемах. Загальна частина: Навч. посібник / Ю. П. Бітяк, В. В. Зуй – Харків: Одіссей, 2005. – 317 с.

7. Благодарний А.М. Особливості адміністративної відповідальності за правопорушення в інформаційній сфері / А. Благодарний // Підприємництво, господарство і право. – 2009. – № 11. – С. 123–126.

8. Бородін І. Дисциплінарна відповідальність та дисциплінарне провадження / І. Бородін // Право України. – 2006. – № 12. – С. 93–96.

9. Відповідальність у приватному праві: монографія / [І. Безклубий, Н. Кузнєцова, Р. Майданик та ін.]; за заг. ред. І. Безклубого. – К. : Грамота, 2014. – 416 с.

10. Відповідальність у праві: філософія, історія, теорія : монографія / [І. Безклубий, С. Бобровник, І. Гриценко та ін.]; за заг. ред. І. Безклубого. – К. : Грамота, 2014. – 448 с.

11. Виноградова Г. В. Правове регулювання інформаційних відносин в Україні: Навч. Посібник/ Г. В. Виноградова. – К. : «Юстініан», 2006. – 176 с.

12. Волкова А. М., Бєляков К. І. Особливості юридичної відповідальності за правопорушення в інформаційній сфері / А. М. Волкова, К. І. Бєляков // Правова інформатика. – К. : НДІІП НАПрН України, 2014. – № 1 (14)/2014. – С. 38–46.

13. Гоголь Б. М. Право на інформацію в цивільному праві України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук: 12.00.03 «Цивільне право і цивільний процес; сімейне право; міжнародне приватне право» / Б. М. Гоголь. – К., 2010. – 16 с.

14. Дідук А. Г. Правовий режим конфіденційної інформації: цивільно-правовий аспект : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.03 «Цивільне право і цивільний процес; сімейне право; міжнародне приватне право» / А. Г. Дідук. − Х., 2008. − 23 с.

15. Дрьомов С. Форми та способи протиправного заволодіння комп'ютерною інформацією за Кримінальним кодексом України / С. Дрьомов // Підприємництво, господарство і право. –2005р. – № 2. – С. 42–45.

16. Загальна теорія держави і права / [за ред. В. В. Копєйчікова]. – К. : Юрінком, 1997. – 320 с.

17. Зелена О. Визначення підстав юридичної відповідальності: актуальні питання / О. Зелена // Право України. – 2003. – № 4. – С. 21–26.

18. Зелена О. Поняття юридичної відповідальності: окремі проблеми / О. Зелена // Право України. – 2002. – № 11. – С. 109–112.

19. Канзафарова І. С. Загальні умови цивільно-правової відповідальності за шкоду, завдану порушенням особистих немайнових прав / І. С. Канзафарова // Вісн. Одес. нац. ун-ту ім. І. І. Мечникова. – 2009. – Т. 14, вип. 1 : Правознавство. – С. 24–35.

20. Канзафарова І. С. Принципи цивільно-правової відповідальності / І. С. Канзафарова // Вісн. Одес. ін-ту внутр. справ. – 2005. – № 2. – С. 8–82.

21. Карнаух Б. П. Сутність і явище цивільно-правової відповідальності / Б. П. Карнаух // Вісник Академії правових наук України : зб. наук. пр. / Акад. прав. наук України. – Х. : Право, 2012. – №2(69). – С. 287–299.

22. Кельман М. С. Загальна теорія держави та права : Підручник / М. С. Кельман, О. Г. Мурашин, Н. М. Хома. – Львів : «Новий світ – 2000», 2003. – 584 с.

23. Кримінальне право України: Загальна частина: Підручник / М. І. Бажанов, Ю. В. Баулін, В. І. Борисов та ін.; За ред. професорів М. І. Бажанова, В. В. Сташиса, В. Я. Тація. – 2-е вид., перер. і доп. – К.: Юрінком Інтер, 2005.

24. Кохановська О. В. Правове регулювання у сфері інформаційних відносин / Національна академія внутрішніх справ України. – К., 2001. – 212 с.

25. Кулініч О. О. Інформація як об'єкт цивільних прав / О. О. Кулініч // Університетські наукові записки, 2005. – № 3 (15). – С. 126–128.

26. Лук'янець Д. Про класифікаційні ознаки юридичної відповідальності / Д. Лук'янець // Право України. – 1999. – № 7. – С. 121–123.

27. Макаренко В. Адміністративна відповідальність за порушення законодавства про державну таємницю / В. Макаренко // Право України. – 2001. – №2, – С. 114–118.

28. Максименко Ю. Є., Ліпкан В. А. Засади розвитку інформаційної деліктології / Ю.Є. Максименко, В.А. Ліпкан // Право України. 2013. – № 10. – С. 249–256.

29. Марущак А. І. Визначення поняття «інформаційні права людини» / А. І. Марущак // Інформація і право : наук. журн. – 2011. – № 2. – С. 21–26.

30. Марущак А. І. Цивільні права на інформацію / А. І. Марущак // Юридичний вісник. – 2009. – № 3(12). – С. 33–36.

31. Пилипенко П. Кодифікація вітчизняного трудового законодавства: проблеми та перспективи / П. Пилипенко // Право України. – 2009. – № 3. – С. 7–13.

32. Правдюк С. А. Класифікація інформаційних правопорушень / С. А. Правдюк // Порівняльно-аналітичне право [Електронний ресурс]. − Режим доступу : http://www.pap.in.ua

33. Прокоф'єва Д. Інформація як знаряддя вчинення злочину та злочини проти інформаційної безпеки / Д. Прокоф'єва // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Науково-технічний збірник. НТУУ «КПІ», Міністерство освіти і науки України, Департамент спеціальних телекомунікаційних систем та захисту інформації СБ України. – К., 2000. – С. 31-36.

34. Прокоф'єва Д. Інформація як предмет злочину / Д. Прокоф'єва // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Науково-технічний збірник. НТУУ «КПІ», Міністерство освіти і науки України, Департамент спеціальних телекомунікаційних систем та захисту інформації СБ України. – К., 2001. – С. 11–22.

35. Середюк В. В. Дослідження поняття юридичної відповідальності в правовій науці України і Польщі / В. В. Середюк / Європейське право та порівняльне правознавство : зб. статей. – К. : Шамборі: Логос, 2010. – С. 383–391.

36. Тихомиров О. О. Інформаційні правопорушення: теоретико-правова концепція / О. О. Тихомиров // Інформаційна безпека людини, суспільства, держави. – 2015. – №1(17). – С. 38–47.

37. Тихомиров О. О. «Інформація» у доктрині цивільного права України / О. О. Тихомиров // Держава і право : зб. наук. пр. Юридичні і політичні науки. Випуск 67. – К. : Ін-т держави і права ім. В. М. Корецького НАН України. –2015. – С. 35–43.

38. Тихомиров О. О. Інформаційні права людини як цивільно-правова категорія / О. О. Тихомиров // Юридичний вісник. Повітряне і космічне право. – 2015. – № 1(34). – С. 104–109.

39. Шапченко С. Д. Механізм кримінально-правового регулювання в правовій системі України: поняття та структура // Вісник Київського національного університету імені Тараса Шевченка. Серія: Юридичні науки. – 2002. – Вип. 40. – С. 63–67.

Навчальне видання

ГУЗ Анатолій Михайлович
КАСПЕРСЬКИЙ Ігор Петрович
КНЯЗЄВ Сергій Олександрович
та ін.

ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Навчальний посібник

Друкується в авторській редакції

Технічне редагування та комп'ютерна верстка І В. Єжової

Формат 60х84/16. Ум. друк. арк. 14,65.
Обл.-вид. арк. 12,83. Тираж___ прим. Зам. №___

Реєстр. 29/3-10227 від 5 вересня 2017р.

Видавець і виготовлювач
Національна академія СБ України,
вул. М. Максимовича, 22, м. Київ-22, 03022
Свідоцтво суб'єкта видавничої справи ДК № 99 від 23.06.2000.