

ГЛАВА 3

ДОСТУП ДО БАНКІВСЬКОЇ ІНФОРМАЦІЇ

3.1. Порядок доступу до банківської інформації

Право банків на комерційну таємницю діє згідно з ст. 30 Закону України "Про підприємства в Україні", оскільки банки відносяться до суб'єктів підприємницької діяльності. Під комерційною таємницею розуміють відомості, пов'язані з банківським виробництвом та технологією, управлінням, фінансами та іншою діяльністю банку, які не є державною таємницею, розголошення (передача, витік) яких може завдати шкоди його інтересам.

Юридичне закріплення права на комерційну таємницю, організацію її захисту мають для банку виняткове значення, бо дають можливість відшкодування збитків у разі втрати інформації конфіденційного характеру.

Згідно з існуючою практикою, першим кроком на цьому шляху є закріплення у статуті банку права на:

- комерційну таємницю;
- визначення складу і обсягу відомостей, що становлять комерційну таємницю та конфіденційну інформацію;
- захист комерційної таємниці.

Такі положення, зафіксовані у статуті, дають банку право:

- організувати захист своїх таємниць;
- включати вимоги щодо захисту комерційної таємниці в усі угоди комерційного характеру;
- домагатися відшкодування збитків, понесених від злочинних посягань на інформацію;
- видавати нормативні та інші документи з питань захисту таємниць банку;
- створювати підрозділи захисту таємниць банку.

До комерційної таємниці необхідно відносити інформацію, яка характеризує нові банківські технології, роботу в галузі надання нових послуг, плани розвитку банку та його мережі, іншу інформацію, яка використовується для отримання прибутку.

Склад і обсяг відомостей, що становлять комерційну таємницю, порядок їх захисту визначаються керівником банку самостійно з урахуванням вимог

Постанови Кабінету Міністрів України № 611 від 09.08.93р. "Про перелік відомостей, що не складають комерційну таємницю".

Виділення відомостей, що складають комерційну таємницю, є важливим елементом у системі заходів банку по захисту своєї економічної безпеки. І треба враховувати наступні ознаки інформації, яку відносять до комерційної таємниці:

- не становить державної таємниці;
- не підпадає під положення постанови Кабінету Міністрів України №611 від 09.08.93р.;
- не включає загальновідомої інформації;
- є власністю банку і має відношення до банківського виробництва;
- має певну або потенційну важливість для розвитку банку;
- має систему розподілу повноважень доступу;
- включає відомості про технологію, виробництво, управління та комерційну діяльність банку.

Методика віднесення тих або інших відомостей до комерційної таємниці у нашій країні ще не розроблена, тому запропонуємо рекомендації, враховуючи практику інших країн:

1. Насамперед, необхідно визначити, яка саме інформація потребує захисту, для кого вона має цінність, який "період життя" цих секретів та скільки буде коштувати їх охорона.

2. Необхідно враховувати принцип економічної доцільності та ефективності інформації. І використовувати правило "золотої середини" при віднесенні інформації до комерційної таємниці. Згідно з існуючою практикою, комерційна таємниця банку не повинна становити більше 10% від усієї його інформації. Занадто таємна діяльність банку може стати причиною втрати прибутків через те, що умови ринку вимагають реклами. Зневажливе ставлення до комерційної таємниці також може призвести до негативних наслідків. Згідно з практикою втрата 20% інформації може призвести до банкрутства у 60 випадках із 100.

3. Необхідно враховувати принцип новизни інформації, наявність її аналогів та її конкурентоспроможність. Інформація типу "ноу-хау" обов'язково повинна бути віднесена до комерційної таємниці. Її треба охороняти навіть від власного персоналу до моменту впровадження у банківське виробництво.

4. Необхідно враховувати вартість засобів охорони інформації, віднесеної до комерційної таємниці банку. Згідно з практикою закордонних банків витрати на охорону комерційної таємниці становлять 10-15% від витрат на банківське виробництво.

5. Особливу увагу треба приділяти охороні інформації, що міститься у договорах, які укладає банк. В окремих випадках охороні підлягає не тільки окреме положення договору, а і факт його укладання.

Перелік інформації, яка може бути віднесена до комерційної таємниці, дуже великий і, виходячи з необхідного мінімуму, розроблений перелік інформації, що може бути віднесена до комерційної таємниці банку згідно з наведеними рекомендаціями та ознаками, який наведений у додатках. Такий перелік повинен затверджуватись наказом по банку і доводиться до всіх працівників.

Для фіксації всіх висловлених раніше відомостей по функціонуванню та захисту комерційної таємниці у банку доцільно розробити ***"Положення про комерційну таємницю та правила й зберігання і порядок доступу до неї"***, яке затверджується наказом по банку. Це положення передбачає перелік відомостей, що становлять комерційну таємницю і конфіденційну інформацію банку. В ньому визначають зміст комерційної таємниці та перелік осіб з їх повноваженнями доступу до інформації, порядок захисту і призначення відповідальних за нього, а також відповідальність за розголошення комерційної таємниці банку. Додатково може бути утворена комісія, яка буде розглядати і визначати цінність банківської інформації, подавати пропозиції керівництву банку про прийняття рішення про надання або зняття статусу комерційної таємниці чи конфіденційної інформації.

Положення про комерційну таємницю та порядок доступу до неї може складатися із розділів:

Загальні положення;

- права і обов'язки посадових осіб у відношенні доступу виконавців до документів, відомостей, що містять комерційну таємницю;
- права і обов'язки підрозділів безпеки банку у відношенні доступу співробітників до документів, що містять комерційну таємницю;
- повноваження посадових осіб у відношенні доступу до документів, що містять комерційну таємницю;
- оформлення доступу виконавцям до документів і відомостей, що містять комерційну таємницю;

- порядок надання документів, що містять комерційну таємницю;
- порядок доступу до документів з грифом таємності;
- порядок доступу виконавців до документів оперативного листування;
- порядок розмноження і адресування документів, що складають комерційну таємницю, в зовнішні організації;
- порядок доступу до документів, що містять комерційну таємницю, осіб, що звільняються;
- порядок доступу на наради і засідання, на яких обговорюються питання, пов'язані з комерційною таємницею банку.

Дуже важливо встановити термін дії відомостей, що становлять комерційну таємницю, бо це допоможе скоротити витрати на її захист.

Наступним кроком на шляху захисту комерційної таємниці є запис у колективному договорі взаємних зобов'язань адміністрації і колективу по забезпеченню збереження комерційної таємниці і встановлення єдиного порядку роботи з такою інформацією, визначення відповідальності за порушення правил роботи з інформацією. У договорі записується, що адміністрація повинна організувати та забезпечити систему заходів для захисту комерційної таємниці, а працівники підприємства повинні виконувати встановлені правила та інструкції по збереженню комерційної таємниці.

Базовим документом для організації роботи з питань функціонування та захисту комерційної таємниці є *Концепція безпеки банку*. Відповідно до неї проводять усі заходи захисту комерційної таємниці та вона визначає:

- Напрямки організації безпеки банку (планування заходів, функції підрозділів банку по виконанню заходів безпеки, їх взаємовідносини між собою, з іншими суб'єктами підприємницької діяльності та державними органами);
- функції підрозділів безпеки банку;
- забезпечення та проведення заходів безпеки.

З комерційною таємницею пов'язане таке поняття, як інтелектуальна власність, що можна визначити як комерційно цінні ідеї. Не треба, щоб ці ідеї були нові чи запатентовані, головне, щоб інформація не відносилася до числа загальновідомої.

Механізм захисту комерційної таємниці банку дуже складний і складається з багатьох блоків, основними з яких є:

- Законодавчі норми, спрямовані на захист її власників;

- морально-етичні норми, спрямовані на додержання правил поведінки, які склалися у колективі; фізичний захист (замки, ґрати та інші засоби);
- адміністративні заходи (пропускний режим, утворення служби безпеки, робота з персоналом);
- технічні заходи (системи охорони, спостереження, виявлення ін. прилади);
- криптографічний захист (шифрування інформації);
- програмні заходи (застосування спеціальних програм для захисту інформації).

Не всі компоненти визначеної системи захисту рівноцінні. Частіше за все основу становлять правові, адміністративні та фізичні заходи. А останні, певною мірою, доповнюють один одного, і відсутність одного з них може призвести до руйнування всієї системи.

На першому місці знаходяться правові заходи захисту комерційної таємниці банку. Вони базуються на нормах діючого законодавства і встановлюють порядок функціонування комерційної таємниці та право на її захист. Враховуючи недосконалість існуючої законодавчої бази її доповненням може бути власна нормативна база банку з питань функціонування та захисту комерційної таємниці. Серед її елементів необхідно відпрацювати внутрішній розпорядок роботи, загальні правила зберігання таємниць банку, посадові інструкції та зобов'язання по збереженню таємниць банку, контракти та договори при вступі на роботу, накази про зміст комерційної таємниці та конфіденційної інформації, перелік осіб, які допущені до таємниць банку.

Морально-етичні норми мають також велике значення у захисті таємниць банку. Вони можуть представляти собою як неписані (загальноприйняті норми поведінки), так і передбачені у статуті банку. Дуже доцільним є розробка Кодексу банківського працівника, який би встановлював правила поведінки, права та обов'язки персоналу.

Фізичні заходи – це замки на дверях, ґрати на вікнах, різні механічні та інші пристрої охорони будівель та приміщень. Необхідно чітко визначити місця обов'язкового встановлення технічних пристроїв захисту. Для роботи з таємними документами слід виділяти спеціальні приміщення, доступ до яких дозволяється тільки окремим працівникам. Зберігання документів, що містять таємниці, здійснюється у сейфах та металевих шафах.

Адміністративні заходи практично завжди здійснюються разом з фізичними. Особливу увагу слід приділяти режиму діяльності банку, причому, повинна бути така система режиму, яка б передбачала його посилення у разі непередбачених і екстремальних ситуацій.

Контроль за зберіганням, правилами обробки та рухом таємної і нетаємної інформації повинен бути чітко визначеним і задокументованим, через те, що у своїй сукупності вони становлять велику цінність. Документи, що містять таємниці банку, необхідно зберігати у спеціальних папках, обов'язково підшивати та реєструвати у журналах обліку. Для таємних документів необхідно продумати питання про встановлення різного ступеня таємності документів. На лицьовому боці документа слід позначати ступінь його конфіденційності.

Крім контролю за документами необхідно чітко визначити порядок, який гарантує правильну циркуляцію документів, що дозволить виключити доступ до інформації тих, хто не повинен бути проінформований про неї.

Необхідно визначити систему копіювання та розмножування документів і встановити конкретну відповідальність службовців за ці дії.

Контроль за циркуляцією копій включає їх реєстрацію, складання списку осіб, що отримали копії, фіксування часу отримання та повернення копій.

Дуже важливе місце в організації захисту комерційної таємниці слід відводити роботі з кадрами. Згідно зі статистикою збереження секретів на 80% залежить від підбору, розстановки і виховання кадрів.

Окремим напрямком у роботі з кадрами є проведення виховної роботи. У ході проведення роботи треба сконцентрувати увагу на таких моментах:

- 1) що являє собою комерційна таємниця банку;
- 2) які реальні загрози існують для таємниць банку;
- 3) які конкретно зобов'язання повинен виконувати кожний службовець по захисту таємниць банку.

Після розподілу інформації по категоріях необхідно визначити види документів, до яких має доступ кожний співробітник.

Технічні засоби захисту таємниць банку призначені для автоматизування охорони приміщень банку та зменшення можливості витоку інформації через різноманітні канали. Ці засоби включають засоби охоронного освітлення, спостереження, виявлення, сигналізації, розмежування доступу, контролю функціонування технологічних систем та інші.

Криптографічні заходи захисту дозволяють шифрувати інформацію таким чином, щоб її зміст був зрозумілим тільки при наявності деякої специфічної інформації – ключа.

У зв'язку з розповсюдженням обчислювальної техніки дуже ускладнений контроль за розповсюдженням інформації, тому криптографічні заходи мають дуже важливе значення для захисту таємниць банку.

Зазначені заходи захисту комерційної таємниці необхідні та достатньо ефективні, але тільки поєднання всіх зазначених механізмів захисту комерційної таємниці банку може зробити її справді надійною.

3.2. Організація захисту банківської інформації

З наведеної раніше інформації бачимо, що існує значна кількість посягань на комерційну таємницю банків та велика їх кількість вдало закінчилася. Саме тому стає актуальним питання оцінки ефективності систем захисту комерційної таємниці.

У розвинутих країнах (США, Німеччина, Франція, Великої Британії, Японія) захист комерційної таємниці виконується завдяки розвинутій системі "промислової секретності", яка базується на відповідному правовому забезпеченні.

Сполучені Штати Америки не мають національного закону про охорону комерційної таємниці, але 22 штати мають власні закони на цю тему. Окрім цього, у законодавстві існує поняття "торговельних секретів" – відомостей про засоби, технології та процеси виробництва, які можуть дати перевагу їх володарю над конкурентами.

Забезпеченням захисту комерційної таємниці у США займаються:

- приватні детективні агентства (охорона власності, майна та об'єктів; захист інформаційних систем від витоку інформації; аналіз і виявлення конкурентів та інші дії, спрямовані на захист комерційної таємниці);
- приватні інформаційно-аналітичні агентства;
- приватні агентства промислової розвідки.

У Німеччині діє закон про недобросовісну конкуренцію, який виділяє два види таємниць – виробничі та комерційні. Цей закон регулює всі відносини, які пов'язані з комерційною таємницею, і встановлює кримінальну відповідальність (до трьох років тюремного ув'язнення) за посягання на комерційну таємницю і протиправні дії з нею. Організацією захисту комерційної таємниці у цій країні займаються:

- детективні агентства (оперативно-розшукова діяльність; охорона об'єктів та інші дії по забезпеченню безпеки);
- служби внутрішньої безпеки банків (робота з персоналом; захист інформації; вивчення і локалізація каналів витоку інформації та інші дії по забезпеченню безпеки).

Великобританія також має досить досконале законодавство по захисту комерційної таємниці. Організацією захисту комерційної таємниці у цій країні займаються:

- приватні детективні агентства (розслідування промислового шпигунства; розробка комплексних систем безпеки; отримання, різноманітної інформації про партнерів та конкурентів);
- служби промислової та комерційної безпеки, які знаходяться у складі банків, промислових концернів та страхових організацій (технічний захист інформації; контроль персоналу; боротьба з шахраями; організація охорони тощо).

У Японії немає ні законів, ні яких-небудь інших нормативних актів, що передбачають відповідальність за розголошення комерційної таємниці. Там ця проблема зважується в такий спосіб: на департаменти кадрів, що мають у кожній японській фірмі, покладається контроль за неухильним дотриманням режиму таємності, що ґрунтується на кодексі поведінки службовців. У ньому містяться положення, що забороняють:

- передавати стороннім особам зведення, що містять комерційну таємницю;
- укладати угоди, що можуть підірвати довіру до компанії з боку клієнтів;
- улаштовуватися без дозволу керівництва на роботу за сумісництвом;
- навмисне завдавати економічної шкоди;
- давати й одержувати хабара.

Слід зазначити, що японський бізнес менш всього страждає від витоку інформації. Це зв'язано з властивий цій країні системою "довічного наймання" і вихованням у співробітників почуття патріотизму, коли вони вважають себе членами однієї родини.

Керівник фірми "Sony" Акио Морита затверджує, що коли немає відданості, що приходить з довгостроковою зайнятістю, те немає можливості покласти кінець витокам інформації і злочинству, від яких повсякденно страждає бізнес на Заході.

На відміну від розвинутих країн, у нас недосконале законодавство про інформацію, що сприяє "законним" посяганням на комерційну таємницю. Відсутність законодавства "Про зброю", "Про приватну детективну діяльність" не дає можливості утворення приватних служб безпеки, які б мали певні повноваження. У більшій кількості випадків організація безпеки банку покладена на службу безпеки банку, але практично неможлива її співпраця з правоохоронними органами, оскільки законами не визначене її становище, а право отримання інформації надано тільки правоохоронним органам, тобто зворотний зв'язок практично відсутній. Невизначений законодавством статус служби безпеки банків робить її функціонування неповноцінним.

Системи захисту комерційної таємниці банків досить різноманітні, тому зробимо узагальнену характеристику основних існуючих складових елементів систем захисту комерційної таємниці банку.

Нормативно-правова система захисту – базується на діючому законодавстві та нормах міжнародного права. У зв'язку з недосконалістю законодавства додатково використовується нормативна система банку, яка має наступні складові:

1. Закріплення у статуті банку права на комерційну таємницю.
2. Правила внутрішнього розпорядку.
3. Накази про встановлення переліку відомостей, що становлять комерційну таємницю та перелік осіб, які мають доступ до неї.
4. Контракти та угоди з працівниками.
5. Угоди про нерозголошення комерційної таємниці зі службовцями та партнерами банку.
6. Інструкції по роботі з комерційною таємницею.
7. Колективний договір.

На жаль, наведеного переліку нормативних документів банку у повному обсязі немає у жодному з банків, або вимоги іноді не виконуються при кадрових та організаційних змінах. У багатьох банках не укладаються угоди про нерозголошення комерційної таємниці зі службовцями та партнерами банку, а також контракти з працівниками, в яких обумовлена відповідальність за неправомірні дії з комерційною таємницею. Це сприяє посяганням на комерційну таємницю з боку службовців банку.

Організаційна система захисту – регламентація виробничої діяльності банку та взаємовідносин між службовцями, яка виключає можливість

нанесення збитків. Ця система досить велика, тому розглядати її будемо по складових елементах (робота з персоналом та адміністративні заходи).

Робота з персоналом є одним з найважливіших етапів побудови системи захисту комерційної таємниці банку. Вона має наступні складові механізми:

- підбір та розподіл кадрів;
- виховна робота з кадрами та формування банківського патріотизму;
- проведення інструктажу працівників, які мають доступ до комерційної таємниці та прийняття заліку;
- встановлення відповідного рівня заробітної плати.

На сьогоднішній день у багатьох банках не приділяється достатньо уваги кадровим питанням. Відсутність відповідної практики проведення виховної роботи та формування банківського патріотизму призводить до значних витрат на організацію захисту інформації.

Адміністративні заходи спрямовані на встановлення чітких правил роботи і полягають у:

- наявності служби безпеки та нормативних документів з її діяльності (Положення про службу, Положення про пропускний режим інші нормативні документи);
- наявності чітких правил роботи з документами, що містять комерційну таємницю (реєстрація, обіг, копіювання, збереження);
- наявності системи спеціального діловодства;
- перевірки виконання встановлених правил і вимог до роботи з документами, що містять комерційну таємницю;
- встановленні системи розподілу доступу до інформації для різних категорій службовців банку та закріплення наказом відповідальних.

Адміністративні засоби захисту присутні достатньою мірою у багатьох банках, але навіть наявність базових механізмів для функціонування системи захисту (служба безпеки та охорони, система спеціального діловодства та деякі правила роботи з документами) не дає повної впевненості у надійності захисту таємниць банку.

Інженерно-технічна система захисту – використання різноманітних технічних пристроїв для запобігання нанесенню збитків банку. Ця система з розвитком технології набуває все більшого і більшого значення, бо технічні пристрої дозволяють досить ефективно і практично без втручання людей здійснювати контроль за різноманітними приміщеннями, інформаційно-технологічними системами і іншими засобами банківського виробництва.

Вказана система має декілька складових (фізичні, апаратні, програмні та криптографічні засоби та методи).

Фізичні засоби захисту спрямовані на неможливість несанкціонованого доступу в приміщення і споруди банку. Вони існують у наступних засобах:

- обладнання споруд і приміщень банку відповідно до вимог технічних норм Національного банку України;
- наявність спеціальних приміщень для роботи з документами, що містять комерційну таємницю;
- наявність спеціальних приміщень для зберігання документів, що містять комерційну таємницю.

Обладнання багатьох банків виконано відповідно до вимог НБУ бо порушення встановлених правил може призвести до санкцій з його боку. А окремі приміщення для зберігання та обробки документів, що містять комерційну таємницю, є не у всіх банках, бо це потребує додаткових витрат.

Апаратні заходи захисту спрямовані на неможливість несанкціонованого доступу в приміщення та інформаційні мережі банку і існують у наступних формах:

- автоматизованих системах охорони, розподілу і контролю доступу;
- засобах охоронно-пожежної сигналізації;
- засобах комунікацій (міні-АТС, комунікаційні центри, поштові та комп'ютерні мережі);
- апаратних засобах захисту телекомунікаційних мереж банку;
- апаратних засобах захисту інформації;
- апаратних засобах контролю за функціонуванням систем банку.

Визначені засоби у багатьох банках не використовуються, оскільки вони мають велику вартість і є необхідність їх модернізації через декілька років. Із існуючих банків тільки невелика кількість великих та заможних мають практично повний набір апаратних засобів захисту. На жаль, практично всі банки не приділяють достатньо уваги захисту своїх інформаційних систем та контролю за їх функціонуванням, а саме це питання дуже важливе на сьогоднішній день.

Програмні та криптографічні засоби можна об'єднати в одну групу, бо вони мають дуже багато спільного і практично завжди використовуються разом. Вони тісно пов'язані із зростанням ваги інформаційних технологій у банківському виробництві і існують у наступних формах:

- використанні сертифікованого програмного забезпечення;

- використанні сертифікованих засобів захисту інформації у ПЕОМ;
- наявності системи збереження ключів та кодів.

Як свідчить практика, у всіх банках з програмно-криптографічних засобів використовуються засоби захисту електронних платежів, розроблені НБУ та іншими організаціями, а інша інформація у комп'ютерних мережах банків практично не захищена криптографічними засобами.

Для комплексної оцінки ефективності систем захисту комерційної таємниці в банку розроблена методика оцінки ефективності системи захисту комерційної таємниці. Вона дозволяє здійснити як повний аналіз ефективності системи захисту, так і її складових елементів для подальшої побудови надійної системи захисту таємниць банку. Використавши розроблену методику, ви зможете дати оцінку ефективності системи захисту комерційної таємниці вашого банку.

Необхідність системи захисту комерційної таємниці на існуючому етапі банківського виробництва не потребує доведення, бо втрата інформації може призвести до втрати прибутків або до банкрутства банку. Саме це і є базою для утворення нових форм та методів захисту, рекомендації по утворенню яких будуть наведені у наступних розділах.

У загальному випадку захист інформації технічними засобами забезпечується в наступних варіантах:

- джерело й носій інформації локалізовані в межах об'єкта захисту і забезпечена механічна перешкода від контакту з ними зловмисника чи дистанційного впливу на них полів його технічних засобів добування;
- співвідношення енергії носія й перешкод на виході приймача каналу витоку таке, що зловмиснику не вдається зняти інформацію з носія з необхідною для її використання якістю;
- зловмисник не може знайти джерело чи носій інформації;
- замість дійсної інформації зловмисник приймає несправжню, котру він оцінює як дійсну.

Ці варіанти реалізують наступні методи захисту:

- запобігання безпосередньому проникненню зловмисника до джерела інформації за допомогою інженерних конструкцій і технічних засобів охорони;
- приховання достовірної інформації;
- "підсування" зловмиснику недійсної інформації.

Застосування інженерних конструкцій і охорона – найбільш древній метод захисту людей і матеріальних цінностей. Способи захисту на основі інженерних конструкцій у сполученні з технічними засобами охорони також поширені в даний час. Сукупність цих способів утворюють так званий фізичний захист. Але цей термін не можна вважати вдалим, тому що інші методи захисту інформації за допомогою технічних засобів також ґрунтуються на фізичних законах. З огляду на те, що основу розглянутого методу складає інженерні конструкції і технічні засоби охорони, доцільно його визначити як інженерний захист і технічна охорона об'єктів (ІЗТОО).

Основною задачею ІЗТОО є недопущення (запобігання) безпосереднього контакту зловмисника чи сил природи з об'єктами захисту. Під об'єктами захисту розуміються як люди і матеріальні цінності, так і носії інформації, локалізовані в просторі. До таких носіїв відносяться папір, машинні носії, фото й кіно плівка, продукція, матеріали і т.п., тобто усе, що має чіткі розміри й вагу. Носії інформації у виді електромагнітних і акустичних полів, електричного струму не мають чітких границь і для захисту інформації на цих носіях методи інженерного захисту не прийнятні – поле з інформацією не можна зберігати, наприклад, у сейфі. Для захисту інформації на таких носіях застосовують методи приховання інформації.

Приховання інформації передбачає такі зміни структури й енергії носіїв, при яких зловмисник не може безпосередньо чи за допомогою технічних засобів виділити інформацію з якістю, достатньою для використання її у власних інтересах.

Розрізняють інформаційне й енергетичне приховання. *Інформаційне приховання* досягається зміною чи створенням несправжнього інформаційного портрета семантичного повідомлення, фізичного об'єкта чи сигналу.

Інформаційним портретом можна назвати сукупність елементів і зв'язків між ними, що відображають зміст повідомлення (мовного чи даних), ознаки об'єкта чи сигналу. Елементами дискретного семантичного повідомлення, наприклад, є букви, цифри чи інші знаки, а зв'язок між ними визначає їх послідовність. Інформаційними портретами об'єктів спостереження, сигналів і речовин є їх еталонні ознаки структури.

Можливі наступні способи зміни інформаційного портрета:

- видалення частини елементів і зв'язків, що утворюють інформаційний вузол (найбільш інформативну частину) портрета;

- зміна частини елементів інформаційного портрета при збереженні незмінності зв'язків між елементами, що залишилися;

- чи видалення зміна зв'язків між елементами інформаційного портрета при збереженні їх кількості.

Зміну інформаційного портрета об'єкта (банка) викликає зміна зображення його зовнішнього вигляду (видових демаскуючих ознак), характеристик випромінюваних їм полів чи електричних сигналів (ознак сигналів), структури і властивостей речовин. Ці зміни спрямовані на зближення знакових структур об'єкта і навколишнього його фону.

В умовах ринку, коли виробник змушений рекламувати свій товар, найбільш доцільним способом інформаційного приховання є виключення з реклами чи відкритих публікацій найбільш інформаційних зведень чи ознак інформаційних вузлів, що містять охороняєму таємницю. До інформаційних вузлів відносяться принципово нові технічні, технологічні рішення й інші досягнення, що складають ноу-хау. Вилучення з технічної документації інформаційних вузлів не дозволить конкуренту скористатися інформацією, що міститься в рекламі чи публікаціях.

Цей спосіб дозволяє:

- зменшити обсяг інформації, що захищається, і тим самим спростити проблему захисту інформації;

- використовувати в рекламі нової продукції відомості про неї, не побоюючись розголошення.

Інший метод інформаційного приховання полягає в трансформації вихідного інформаційного портрета в новий, який відповідає недійсній інформації чи несправжній знаковій структурі, і "нав'язуванні" нового портрета органу розвідки. Такий метод ще називається дезінформуванням.

Дезінформування відноситься до числа найбільш ефективних способів захисту інформації з наступних причин:

- створює у власника інформації, що захищається, запас часу, обумовлений перевіркою розвідкою вірогідності отриманої інформації;

- наслідки прийнятих конкурентом на основі удаваної інформації рішень можуть бути для нього гіршими в порівнянні з рішеннями, прийнятими при відсутності інформації, що добувається.

Розрізняють наступні способи дезінформування:

- заміна реквізитів інформаційних портретів, що захищаються, у тому випадку, коли інформаційний портрет об'єкта захисту схожий на

інформаційні портрети інших "відкритих" об'єктів і не має специфічних інформативних ознак. У цьому випадку обмежуються розробкою й підтримкою версії про інший об'єкт, видаючи в якості його ознак ознаки об'єкта, що захищається. Наприклад, у даний час велика увага приділяється продукції подвійного застосування: військового і цивільного. Поширення інформації про виробництво продукції суцільно цивільного використання є надійним прикриттям для варіантів військового призначення;

- підтримка версії з ознаками, запозиченими з різних інформаційних портретів реальних об'єктів. Застосовується в тих випадках, коли в організації одночасно виконується трохи закритих тем. Шляхом різних ознак, що відносяться до різних тем, можна нав'язати протилежній стороні неправильне уявлення про роботи, що ведуться, без імітації додаткових ознак;

- сполучення дійсних і недійсних ознак, причому недійсними замінюється незначна, але сама коштовна інформація, що відноситься до об'єкта, що захищається;

- зміна тільки інформаційних вузлів із збереженням незмінної іншої частини інформаційного портрета.

Як правило, використовуються різноманітні комбінації цих варіантів.

Іншим ефективним методом приховання інформації є *енергетичне приховання* полягає в застосуванні способів і засобів захисту інформації, що виключають утрудняють чи виконання енергетичної умови розвідувального контакту.

Енергетичне приховання досягається зменшенням відносини енергії (потужності) сигналів, тобто носіїв (електромагнітного чи акустичного полів і електричного струму) з інформацією, і перешкод. Зменшення відносини сигнал/перешкода (слово «потужність», як правило, опускається) можливо двома методами: зниженням потужності сигналу чи збільшенням потужності перешкоди на вході приймача.

Для конкретних видів інформації й модуляції сигналу існують граничні значення відносини сигнал/перешкода, нижче яких забезпечується енергетичне приховання інформації.

Необхідність і ефективність інженерного захисту і технічної охорони підтверджується статистикою, відповідно до якої більш 50% вторгнень відбувається на комерційні об'єкти з вільним доступом персоналу й клієнтів і

тільки 5% - на об'єкти з посиленням режимом охорони, із застосуванням спеціально навченого персоналу і складних технічних систем охорони.