Львівська комерційна академія

кафедра міжнародних економічних відносин

Лектор: к.е.н. Флейчук М.І.

Ознаки економічної злочинності

Львів – 2009

Ознаки економічної злочинності:

1. **Корисливий характер -** їх метою є одержання вигоди у результаті присвоєння економічних ресурсів з порушенням принципу еквівалентності. Дана ознака визнається обов'язковою. При цьому злочин може бути здійснений з метою одержання особистої вигоди, в інтересах третіх осіб або організації; **Відбувається у процесі професійної діяльності;**
2. **Пов'язана із договорами і зобов'язаннями, що виникають у суб'єктів між собою і з державою**, необхідними для виробництва, переробки, придбання, розподілу та обміну матеріальних благ і послуг;
3. **Колективність жертв -** прихований для суспільства характер злочинів, велика відстань між жертвою і злочинцем. Об'єктом зазіхання є економіка загалом, окремі сектори, приватнопідприємницькі структури, групи громадян;

5. **Анонімність жертв -** процес віктимізації (порушення закону) відбувається, в основному, приховано від самої жертви;
6. **Наявність двох суб'єктів** - юридичної (злочинність корпорацій) і фізичної осіб (злочинність по роду зайнятості), що діють від імені та в інтересах підприємства. Юридична особа є суб'єктом злочину лише у тих країнах, де законодавством передбачена кримінальна відповідальність юридичних осіб (США, Франція);
7. **Істотний збиток,** заподіяний економічним інтересам держави, частки підприємництва і громадян.
8. **Множинний характер;**
9. **Перерозподіл матеріальних благ** як наслідок економічних злочинів;
10. **Тривалий, систематичний характер;**
11. **Здійснення, без використання насильства.**

Види економічної злочинності:

- Фінансові;
- що зазіхають на правила конкуренції;
- що зазіхають на права споживачів;
- що зазіхають на порядок державного регулювання економіки;
- комп'ютерні злочини;
- пов'язані з незаконною експлуатацією природного середовища;
- пов'язані із навмисним порушенням правил техніки безпеки, що наносять збиток найманим робітникам.

Підвиди:

- злочини, що посягають на принципи чесної конкуренції;
- фінансові;
- проти інтересів кредиторів;
- комп'ютерна злочинність;
- з використанням банківських карт (кардинг);
- економічна злочинність в Інтернеті;
- у сфері стільникового телефонного зв'язку;
- що зазіхають на права споживачів

.

Оценка стоимости 20-ти самых дорогих торговых марок мира

Торговая марка	Страна	Стоимость (в млрд.долл.)
Coca-Cola	США	72,5
Microsoft	США	70,2
IBM	США	53,2
Intel	США	39,0
Nokia	Финляндия	38,5
General Electric	США	38,1
Ford	США	36,4
Disney	США	33,6
McDonald's	США	27,9
AT&T	США	25,5
Mariboro	США	22,1
Mercedes	Германия	21,1
Hewlett-Packard	США	20,6
Cisco Systems	США	20,0
Toyota	Япония	18,9
Citibank	США	18,9
Gillette	США	17,4
Sony	Япония	16,4
American Express	США	16,1
Honda	Япония	15,2

Источник: Monde. — P., 2001. — 10 mai. — С. 21.

Происхождение подделок, обнаруженных французской таможней в 1999 г.

Страна происхождения подделок	Численность арестованных подделок	Доля в общей численности (в процентах)
Китай	708478	59,0
Тайвань	195803	16,3
Гонконг	64629	5,4
Египет	60609	5,0
Турция	46454	3,9
Италия	42154	3,5
Португалия	39526	3,3
Таиланд	18061	1,5
Южная Корея	13352	1,1

Источник: MOCI. — P., 2000. — № 1467. — С. 77.

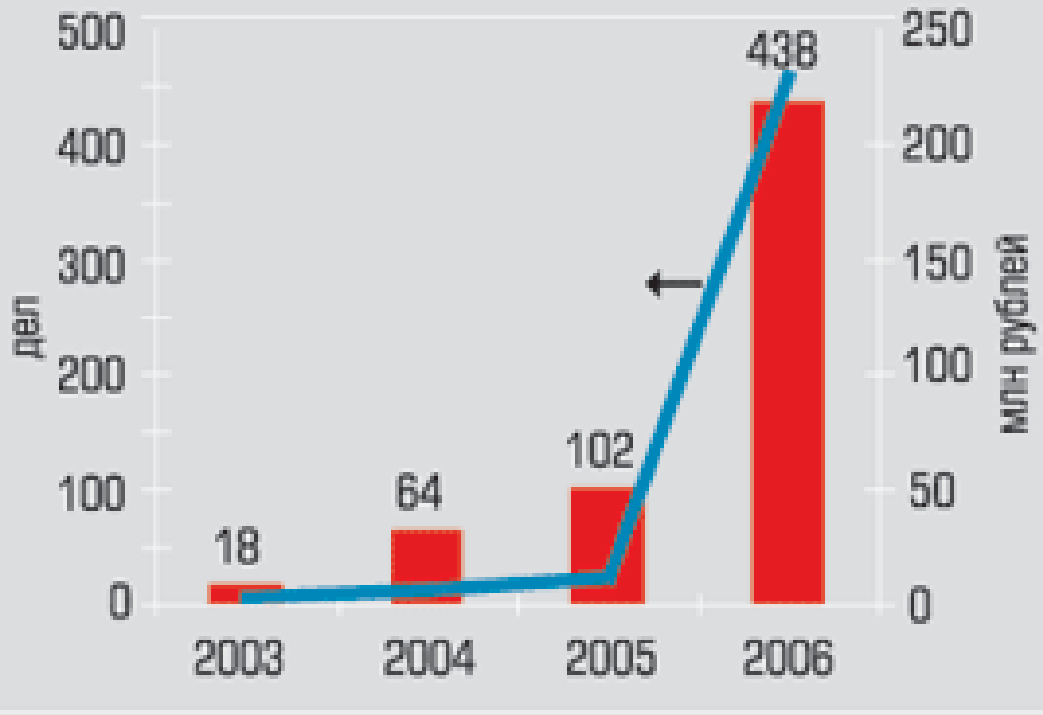
Издержки и продолжительность рассмотрения споров о незаконном использовании торговых марок, дизайна и образцов

	Суды первой инстанции		Апелляция		Всего: суды первой инстанции, апелляция и кассация	
	В тыс. франков	В месяцах	В тыс. франков	В месяцах	В тыс. франков	В месяцах
Простые дела:						
Франция	80	9	70	15	172	48
Германия	40	10	30	18	—	52
Великобритания	550	12	250	14	—	—
Испания	65	9	65	12	180	45
США	800	6	200	—	—	—
Нидерланды	45	12	45	12	190	48
Сложные дела:						
Франция	160	15	135	18	925	57
Германия	130	12	140	19	—	58
Великобритания	1900	16	900	18	—	—
Испания	100	15	65	16	230	61
США	2240	9	560	—	—	—
Нидерланды	120	18	115	18	375	60
Комплексные дела:						
Франция	240	18	180	24	480	66
Германия	150	15	170	20	500	60
Великобритания	4800	21	1200	29	—	—
Испания	130	20	80	19	300	75
США	5600	12	1400	—	—	—
Нидерланды	150	24	150	20	400	68

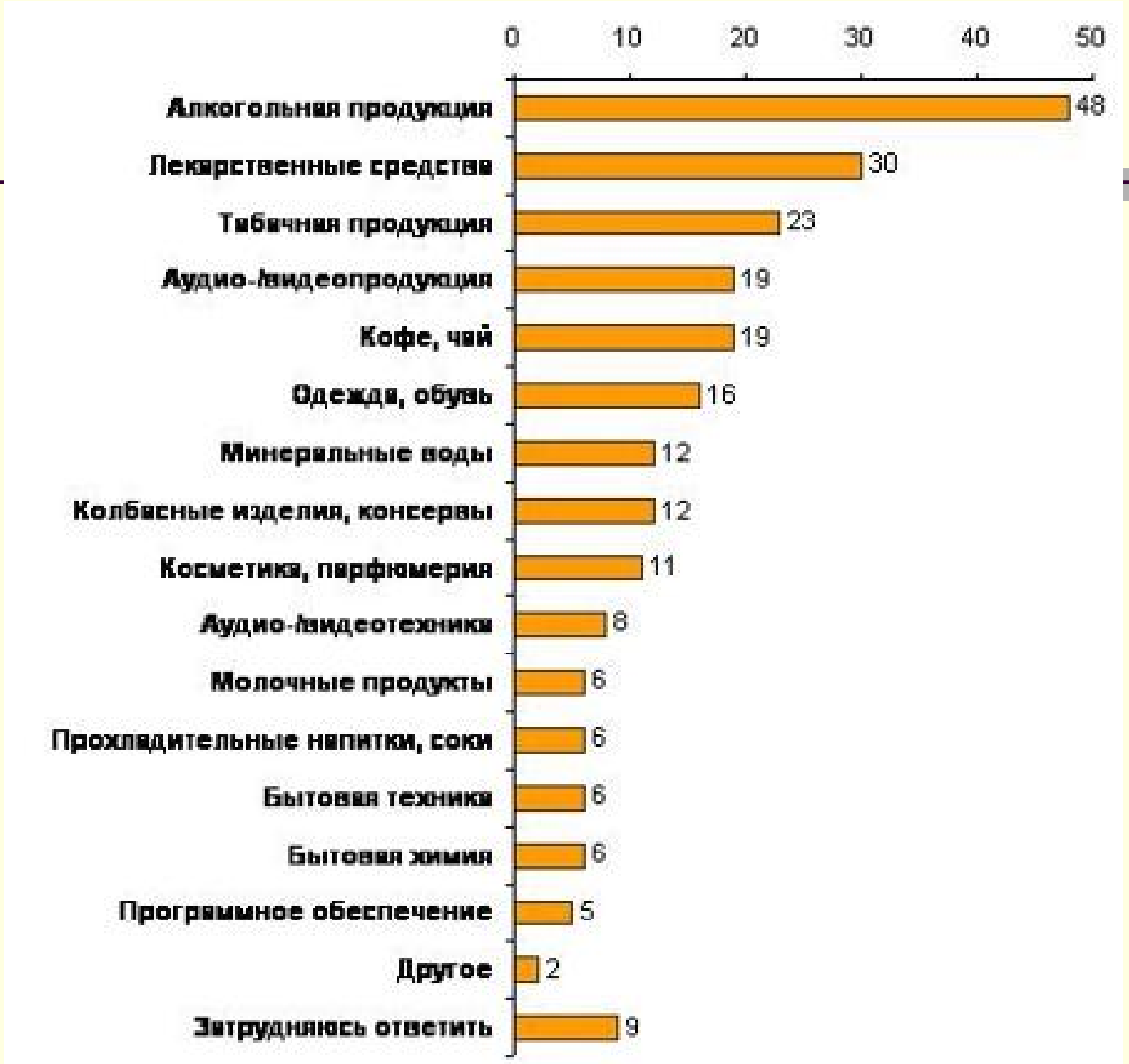
Источник: MOCI. — P., 2000. — № 1467. — С. 84.

Ежегодно число уголовных дел в отношении «пиратов» возрастает в разы

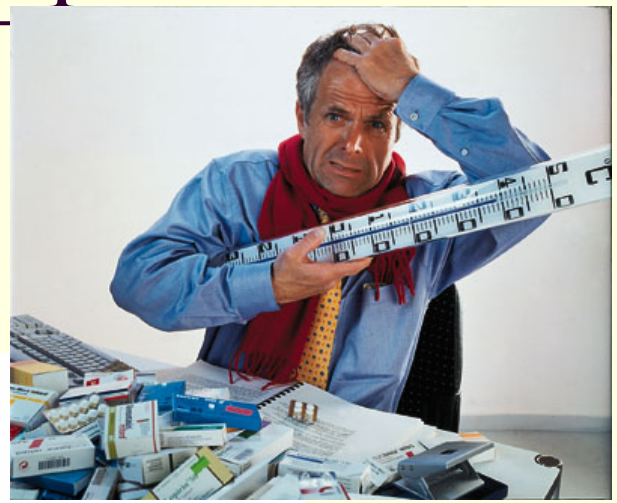
Количество возбужденных в УрФО уголовных дел по статье 146 УК РФ «Нарушение авторских и смежных прав» и суммарный ущерб по ним

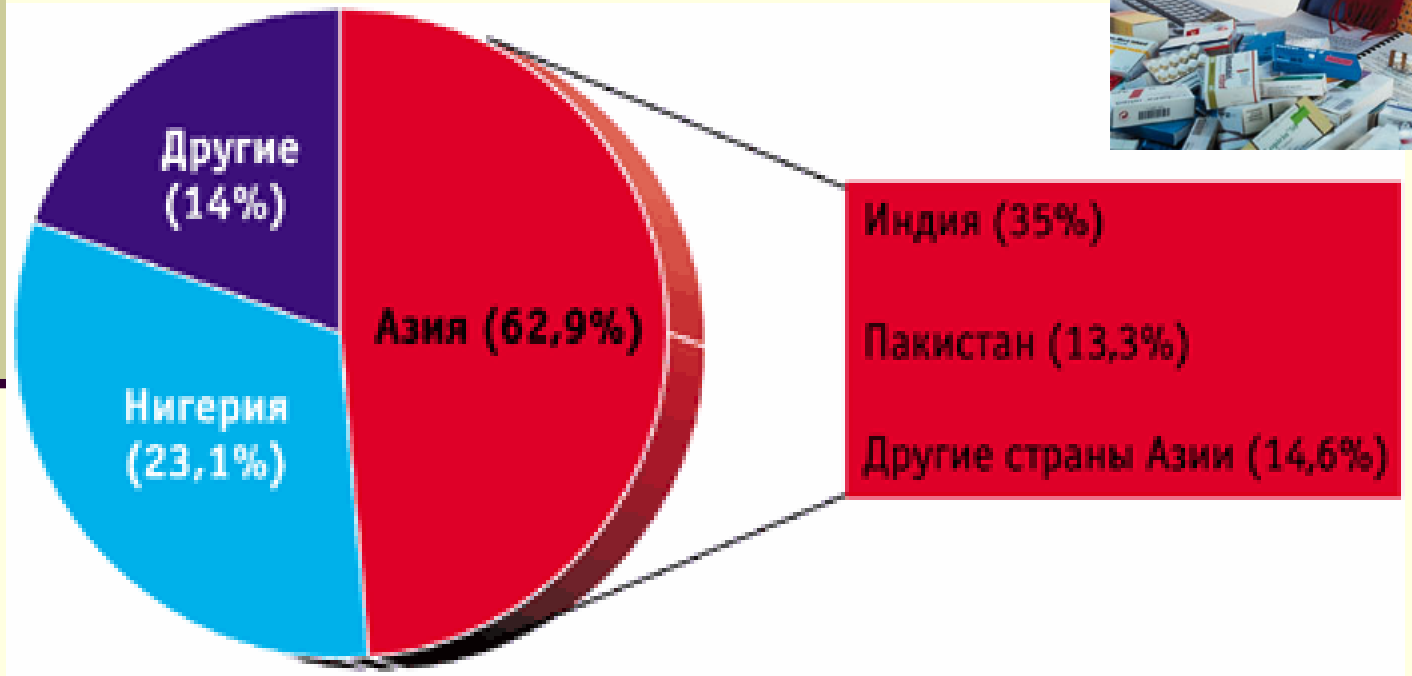


Источник: ГУМВД по УрФО


0
10
20
30
40
50
Алкогольная продукция
48
Лекарственные средства
30
Табачная продукция
23
Аудио-/видеопродукция
19
Кофе, чай
19
Одежда, обувь
16
Минеральные воды
12
Колбасные изделия, консервы
12
Косметика, парфюмерия
11
Аудио-/видеотехника
8
Молочные продукты
6
Прохладительные напитки, соки
6
Бытовая техника
6
Бытовая химия
6
Программное обеспечение
5
Другое
2
Затрудняюсь ответить
9

Країни-виробники фальсифікованих лікарських препаратів






ORIENT
1250.
ORIENT
1450.
ORIENT
1650.
OMEGA
2700.
2400.
Breaget
2100.
FRANK MILLER
1650.
Q&Q
440.


POLIZEI
EURO·2008
SALE

Злочини, що посягають на принципи чесної конкуренції:

- Злочини, пов'язані із монопольною діяльністю;
- Несумлінна конкуренція.

Злочини, пов'язані із монопольною діяльністю:

- ***Зговір про фіксування цін;***
- ***Зловживання переважаючою позицією;***
- ***Комерційний хабар.***

Види несумлінної конкуренції згідно з Паризькою конвенцією:

- усі дії, що приводять до того, що споживач може прийняти підприємство, товари, промислову або комерційну діяльність даної фірми за підприємство, товари, промислову або комерційну діяльність конкурента;
- помилкові заяви у ході комерційної діяльності, що дискредитують підприємство, товари, промислову або комерційну діяльність конкурента;
- використання у ході комерційної діяльності вказівок або позначень, що вводять споживача в оману щодо природи, способу виготовлення, характеристик, придатності для в певних цілей або кількості товарів.

Види несумлінної конкуренції у коментарі до Типового закону по товарних знаках, фірмових найменуваннях і актах несумлінної конкуренції для країн, що розвиваються:

1. підкуп покупців конкурентів, спрямований на те, щоб залучити їх як клієнтів і зберегти на майбутнє їхня вдячність;
2. з'ясування виробничих або комерційних таємниць конкурента шляхом шпигунства чи підкупу його службовців (промисловий шпіонаж);
3. неправомірне використання або розкриття ноу-хау конкурента;
4. спонукання службовців конкурента до порушення чи розриву їх контрактів з наймачем;
5. погроза конкурентам позовами про порушення патентів або товарних знаків, якщо це робиться несумлінно і з метою протидії конкуренції в сфері торгівлі;
6. бойкотування торгівлі іншої фірми для протидії чи недопущення конкуренції;

7. демпінг, тобто продаж своїх товарів нижче вартості з наміром протидіяти конкуренції або придушити її;
8. створення враження, що споживачеві надається можливість покупки на надзвичайно вигідних умовах, коли насправді цього немає;
9. навмисне копіювання товарів, послуг, реклами або інших аспектів комерційної діяльності конкурента;
10. заохочення порушень контрактів, укладених конкурентами;
11. випуск реклами, у якій проводиться порівняння із товарами або послугами конкурентів;
12. порушення правових положень, що не мають прямого відношення до конкуренції, коли таке порушення дозволяє домогтися невиправданої переваги перед конкурентами.

Фінансова злочинність -

сукупність злочинів, безпосередньо пов'язаних із зазіханням на відносини щодо формування, розподілу, перерозподілу та використання коштів (фінансових ресурсів) суб'єктів економічних відносин.

Класифікація фінансових злочинів:

1. **В залежності від рівня фінансових відносин, що є об'єктом зазіхань:**

   а) злочини, що зазіхають на фінансову систему держави (державні і муніципальні фінанси);

   б) злочини, що зазіхають на фінанси підприємств.

2.в залежності від сфери зазіхань:

а) у сфері оподатковування;

б) на ринку цінних паперів;

в) у сфері страхового ринку;

г) у сфері валютного ринку;

д) у сфері міжбанківського грошового ринку;

е) у сфері кредитного ринку;

ж) на ринку товарів і послуг.

3. **в залежності від виду операцій, використовуваних у злочинних цілях розрізняють злочини у сфері:**

- Кредитних;
- Розрахункових;
- Валютних;
- Фондових;
- облікових операцій.

4.в залежності від суб'єкта економічних відносин, на права якого здійснюється зазіхання:

а) що зазіхають на права кредиторів, гарантів;

б) що зазіхають на права інвесторів (вкладників, акціонерів, пайовиків);

в) що зазіхають на інтереси держави (податкові і митні злочини);

5.в залежності від суб'єкта :

а) платників обов'язкових платежів (податків, зборів, тарифів, внесків);

б) менеджерів підприємств, установ;

в) найманих робітників комерційних і некомерційних підприємств;

г) державних службовців;

д) осіб, що є сторонами у зобов'язальних відносинах (боржників, страхувальників, страховиків, емітентів, клієнтів і ін.)

Види злочинів, що зазіхають на фінансову систему держави:

- податкові злочини;
- ухилення від сплати митних платежів;
- ухилення від сплати обов'язкових внесків у цільові державні фінансові фонди;
- нецільове використання бюджетних коштів (шахрайства із субсидіями);
- незаконне одержання і нецільове використання державних кредитів;
- фальшивомонетництво;
- легалізація доходів, отриманих злочинним (незаконним) шляхом;
- пов'язані із незаконним вивозом капіталу або неповерненням валютних коштів, якщо таке повернення є обов'язковим.

Злочини проти інтересів кредиторів:

а) злочини, пов'язані з банкрутством (лжебанкрутство, фіктивне банкрутство, неправомірні дії при банкрутстві);

б) різні види розкрадання майна із використанням відносин позики, кредитування;

г) злісне ухилення від погашення кредиторської заборгованості.

Стадії лжебанкрутства:

- Одержання кредиту;
- придбання товару в кредит;
- продаж або інші дії, що сприяють продажу придбаного;
- приховання своїх дій;
- несплата кредиторам;
- подача заявки про банкрутство.

До числа неправомірних дій при банкрутстві відносять:

- приховування майна або майнових зобов'язань;
- приховання відомостей про майно, про його розмір, місцезнаходження або іншу інформацію про майно;
- передача майна у володіння іншої особи;
- знищення майна;
- приховування, знищення, фальсифікація бухгалтерських та інших облікових документів, що відображають економічну діяльність,

Дії, що вказують на навмисне погіршення фінансового стану:

- зменшення активів, шляхом зняття із розрахункового рахунка коштів, і їх присвоєння;
- зниження ліквідності активів;
- старіння кредиторської заборгованості;
- перерахування грошей контрагентові на підставі фіктивного договору;
- відсутність у бухгалтерських документах зазначення куди витрачені кошти, виручені за проданий товар або майно;
- збільшення заборгованості перед акціонерами, фінансовими органами;
- різке зменшення матеріальних запасів (перебої у виробництві, постачанні) у результаті чого не виконуються зобов'язання перед покупцями.

Комп'ютерна злочинність -

злочини, вчинені за допомогою комп'ютерів, інформаційно-обчислювальних систем і засобів телекомунікацій, або спрямовані проти них з корисливими цілями.

Комп'ютерний злочин (КЗ)-

навмисне порушення чужих прав та інтересів у відношенні до автоматизованих систем обробки даних, що приносить шкоду та підлягає правовій охороні прав та інтересів фізичних і юридичних осіб, суспільства і держави.

Цілі КЗ:

- підробка звітів і платіжних відомостей;
- приписка понаднормових годин роботи;
- фальсифікація платіжних документів:
- розкрадання грошових фондів;
- добування запасних частин і рідких матеріалів;
- крадіжка машинного часу:
- вторинне одержання вже зроблених виплат;
- фіктивне просування по службі;
- одержання фальшивих документів;
- внесення змін у програми і машинну інформацію;
- перерахування грошей на фіктивні рахунки;
- здійснення покупок з фіктивною оплатою й ін.

Класифікація КЗ:

- Фізичні зловживання, що містять руйнування устаткування, знищення даних або програм, введення помилкових даних, крадіжку інформації, записаної на різних носіях;
- Операційні зловживання, що передбачають: шахрайство (видача себе за іншу особу або використання прав іншої особи), несанкціоноване використання різних пристроїв ;
- Програмні зловживання, що містять у собі: різні способи зміни системи математичного забезпечення ("логічна бомба" - введення у програму команди комп'ютерові здійснити у певний момент певну несанкціоновану дію; "троянський кінь" - включення в звичайну програму свого завдання);
- Електронні зловживання, що містять у собі схемні та апаратні зміни, що призводять до того ж результату, як і зміна програми.

Методи КЗ:

- перехоплення;
- несанкціонованого доступу;
- маніпуляції.

1. Методи перехоплення:

- **Безпосереднє перехоплення** - здійснюється або безпосередньо через зовнішні комунікаційні канали системи, або шляхом безпосереднього підключення до ліній периферійних пристроїв. При цьому об'єктами безпосереднього підслуховування є кабельні і провідні системи, наземні мікрохвильові системи, системи супутникового зв'язку, а також спеціальні системи урядового зв'язку.

- **Електромагнітне перехоплення**. Перехоплення інформації здійснюється за рахунок випромінювання центрального процесора, дисплея, комунікаційних каналів, принтера і т.д. Може здійснюватися злочинцем, що знаходиться на достатній відстані від об'єкта перехоплення.

2. Методи несанкціонованого доступу:

- **Метод слідування "За дурнем".** Має на меті несанкціоноване проникнення у просторові та електронні закриті зони. Наприклад: якщо набрати у руки різні предмети, пов'язані із роботою на комп'ютері, і проходжуватися з діловим виглядом біля замкнених дверей, де перебуває термінал, то, дочекавшись законного користувача, можна пройти у двері приміщення разом з ним.

- **Метод "За хвіст".** Використовуючи цей метод, можна підключатися до лінії зв'язку законного користувача і, вичисливши, коли останній закінчує активний режим, здійснювати доступ до системи.

- **Метод "Комп'ютерний абордаж".** Звичайно використовується для проникнення у чужі інформаційні мережі. Зловмисник намагається за допомогою автоматичного перебору абонентських номерів з'єднатися із тим або іншим комп'ютером, підключеним до телефонної мережі. Робиться це доти , поки на іншому кінці лінії не відгукнеться інший комп'ютер. Після цього досить підключити власний комп'ютер. Угадавши код можна впровадитися в чужу інформаційну систему.

2. Методи несанкціонованого доступу:

- **Метод слідування "За дурнем".** Має на меті несанкціоноване проникнення у просторові та електронні закриті зони. Наприклад: якщо набрати у руки різні предмети, пов'язані із роботою на комп'ютері, і проходжуватися з діловим виглядом біля замкнених дверей, де перебуває термінал, то, дочекавшись законного користувача, можна пройти у двері приміщення разом з ним.

- **Метод "За хвіст".** Використовуючи цей метод, можна підключатися до лінії зв'язку законного користувача і, вичисливши, коли останній закінчує активний режим, здійснювати доступ до системи.

- **Метод "Комп'ютерний абордаж".** Звичайно використовується для проникнення у чужі інформаційні мережі. Зловмисник намагається за допомогою автоматичного перебору абонентських номерів з'єднатися із тим або іншим комп'ютером, підключеним до телефонної мережі. Робиться це доти , поки на іншому кінці лінії не відгукнеться інший комп'ютер. Після цього досить підключити власний комп'ютер. Угадавши код можна впровадитися в чужу інформаційну систему.

- **Метод "Неспішного вибору".** У цьому випадку несанкціонований доступ до баз даних і файлів законного користувача здійснюється шляхом перебування слабких місць у захисті систем. Один раз знайшовши їх, зловмисник може спокійно читати та аналізувати інформацію, що міститься у системі, копіювати її, повертатися до неї у міру необхідності.

- **Метод "Пошук пролому**". Даний метод заснований на використанні помилки або невдалій логіці побудови програми. Виявлені проломи можуть експлуатуватися неодноразово.

- **Метод "Люк"** є розвитком попередніх. У знайденому "проломі" програма "розривається" і туди вставляється необхідне число команд у міру необхідності "люк" відкривається, а вбудовані команди автоматично здійснюють своє завдання.

- **Метод "Маскарад".** У цьому випадку зловмисник з використанням необхідних засобів проникає в комп'ютерну систему, видаючи себе за законного користувача.

- **Метод "Містифікація".** Використовується при випадковому підключенні "чужої" системи. Зловмисник, формуючи правдоподібні відгуки, може підтримувати в омані користувача, що помилково підключився, протягом якогось проміжку часу й одержувати деяку корисну для нього інформацію, наприклад коди користувача.

- **Метод "Аварійний"**. Цей прийом заснований на використанні тієї обставини, що у будь-якому комп'ютерному центрі є особлива програма, що застосовується як системний інструмент у випадку виникнення збоїв або інших відхилень у роботі ЕОМ. Така програма - могутній і небезпечний інструмент у руках зловмисника.

- **Метод "Склад без стін".** Несанкціонований доступ здійснюється у результаті системної поломки. Наприклад, якщо деякі файли користувача залишаються відкритими, він може одержати доступ до не приналежним йому частинам банку даних.

3. Методи маніпуляції:

Суть методів маніпуляції полягає у підміні даних, що здійснюється, як правило, при вводі-виводі даних.

- **Маніпуляція із пультом управління -** відноситься до зловживання механічними елементами управління ЕОМ. Полягає у тому, що у результаті механічного впливу на технічні засоби машини створюються можливості маніпуляції даними.

- **"Троянський кінь" -** полягає у таємному введенні в чужу програму таких команд, що дозволяють здійснювати інші, що не планувалися власником програми функції, але одночасно зберігати і колишню працездатність;

- **"Логічна бомба"** - таємне вбудовування в програму набору команд, що повинен спрацювати лише один раз, але за певних умов.

- **"Тимчасова бомба"** - різновид логічної бомби, що спрацьовує при досягненні певного моменту часу.

- **"Асинхронна атака"** полягає у змішуванні команд двох або декількох користувачів, чиї команди комп'ютерна система виконує одночасно.

Реверсивна модель. Суть методу полягає у створенні моделі конкретної системи. В неї вводяться реальні вихідні дані і враховуються плановані дії. Потім, виходячи з отриманих правильних результатів, підбираються правдоподібні бажані результати. Потім модель проганяється назад, до вихідної точки, і стає ясно, які маніпуляції із вхідними даними потрібно здійснювати.

- **Повітряний змій".** У найпростішому випадку потрібно відкрити у двох банках по невеликому рахунку. Далі, гроші переводяться з одного банку в інший і назад і поступово підвищуються суми. Хитрість полягає у тому, щоб до того, як у банку виявиться, що доручення про переказ не забезпечене необхідною сумою, приходило би повідомлення про переказ у цей банк, так, щоб загальна сума покривала вимогу про перший переказ. Цей цикл повторюється велике число разів доти , поки на рахунку не виявляється пристойна сума (фактично, вона постійно "перескакує" з одного рахунка на інший, збільшуючи свої розміри). Тоді гроші швидко знімаються і власник рахунків ховається. Цей спосіб вимагає дуже точного розрахунку, але для двох банків його можна зробити і без комп'ютера. На практиці, у таку гру включають велике число банків: так сума накопичується швидше і число доручень про переказ не досягає підозрілої частоти. Але керувати цим процесом можна тільки за допомогою комп'ютера.

Види атак, виявлені за останні 12 місяців	
Вірус	83%
Зловживання співробітниками компанії доступом до Internet	69%
Крадіжка мобільних комп'ютерів	58%
Неавторизований доступ зі сторони співробітників компанії	40%
Шахрайство при передачі засобами телекомунікацій	27%
Крадіжка внутрішньої інформації	21%
Проникнення у систему	20%
Допускалось декілька варіантів відповідей.	
Джерело: Computer Security Institute	

Дякуємо за увагу!