# Реферат

# на тему:

# ІНФОРМАЦІЙНА СФЕРА В УКРАЇНІ,

# ЗАХИСТ ІНФОРМАЦІЇ:

ПРОБЛЕМИ І ПЕРСПЕКТИВИ РОЗВИТКУ

# Вступ

В наш час інформація перетворюється на найдорожчий ресурс. Оперативне отримання інформації дає перевагу над конкурентами, які її не мають, конфіденційна інформація про вас та вашу діяльність, що потрапила до зловмисників може серйозно вам нашкодити(наприклад, про вашу унікальну технологію дізнаються конкуренти і просто-напросто скопіюють її, уникнувши витрат на дослідження; або ваші плани стануть відомі і нечесні суперники вживуть упереджувальних заходів).

Для полегшення пошуку, обміну, обробки інформації як фізичні особи, так і фірми використовують персональні комп'ютери приєднані до мережі Інтернет. Комп'ютеризація та Інтернет заторкнули майже всі аспекти діяльності людини(маю на увазі розвинуті країни): від укладення договорів до особистих відносин, від придбання товарів через Інтернет-магазин до навчання. Комп'ютери значно спростили діяльність людини, виконуючи за неї машинну роботу. Світова павутина (World Wide Web - WWW) зменшили час на пошук необхідної інформації шляхом використання пошукових серверів – служб, що здійснюють пошук за заданим користувачем запитом. За їх допомогою навіть не досвідчений користувач зможе знайти необхідну інформацію ввівши перелік слів, які як він вважає присутні в потрібному документі. В розвинених країнах комп'ютеризовано всі галузі господарства, в тому числі державний сектор. Так, в США інформатизовано телекомунікаційну інфраструктуру, банківську і фінансову системи, систему електропостачання й інші енергетичні системи, такі як нафто- і газопроводи, транспортні мережі, системи водопостачання, системи медичних послуг і охорони здоров'я, поліцію, пожежну і рятувальну служби, а також державні органи й установи всіх рівнів. Переваги очевидні, але ціна переваг також досить висока: полегшується анонімний доступ до конфіденціальної інформації.

Мабуть, для кожного було б неприємним сюрпризом, коли б мишка його комп'ютера перестала реагувати на дотик, раптово з'явилось повідомлення, що Metallica is the best group in the world, або пропав фінансовий звіт за минулий рік. Це лише дрібна частинка тих “приємних” несподіванок, які може принести Інтернет або дискета, що побувала на зараженому комп'ютері. Кількість комп'ютерних вірусів- програм, що приводять до збоїв програмного забезпечення росте з кожним роком, і далеко не в арефметичній прогресії. Якщо в 1992 році Євген Кашперський(керівник фірми відомої своїм антивірусним пакетом AVP) констатував факт, що існує від 1000 до 2000 вірусів, то зараз кількість лише тих вірусів, що знешкоджується AVP перевищила 50 тис. Якщо в не так далекому 1992-му Кашперський назвав більшість вірусів витівками студентів, що не мають чого робити, то зараз значно зросла кількість вірусів, що становлять загрозу для нормального функціювання цілих корпорацій, державних установ, врешті національної беспеки:

"*Нам загожує небезпека. Життя в Америці багато в чому залежить від комп'ютерів. За допомогою комп'ютерів здійснюється керування системами розподілу електроенергії, системами зв'язку, засобами авіації і фінансами. Комп'ютери використовуються для збереження найважливішої інформації, починаючи з історій хвороби і бізнес-планів і закінчуючи даними про судимість. І хоча ми довіряємо комп'ютерам, вони піддані ризику як випадкових збоїв у результаті недосконалої конструкції чи недостатнього контролю за якістю, так і що більш тривожно -ризику навмисних зазіхань. Озброївши комп'ютером, сучасний злодій може украсти більше, ніж використовуючи вогнепальну зброю. Завтрашній терорист зможе заподіяти більш серйозний збиток за допомогою клавіатури, ніж за допомогою бомби*".

"Комп'ютери в небезпеці", Національна дослідницька рада, США, 1991. – Красномовний факт, що свідчить про масштабність проблеми.

Несанкціонований доступ крім всього іншого зменшує довіру до фірми, копоративну мережу якої було зламано. Крім збитків, що їх вона понесла беспосередньо від злому, вона несе непередбачувані збитки в майбутньому, оскільки від неї відвернеться значна кількість її потенціальних клієнтів. Ще остаточно не відомо як відбилася поява в світовій мережі вірусів Red Code та інших, заснованих на помилках Windows2000, на популярності нового продукту корпорації Microsoft: WindowsXP. Зрозуміло лиш одне: недовіра до нього збільшилась, а це – мільйони неотриманих коштів. Тож не дивно, що і фірми і приватні особи намагаються захистити свою інформацію від недозволеного доступу, руйнівного впливу вірусів.

## Мета роботи

Глобальна інформатизація і комп'ютеризація призвела до стрімкого розвитку ринку програмного забезпечення, що забеспечує як пошук так і захист інфомації. Але одні з економічних гравців в цих галузях щороку збільшують свої прибутки, інші – навпаки – несуть збитки. Особливе місце в цих галузях належить органам держави. Тому метою роботи є визначення факторів, які надають переваги підприємстам в кожній з перелічених галузей.

Сфера захисту інформації від прослуховування а також інформації, що збережена не на комп′ютерних носіях.

Як вже було сказано вище, інформація про вас, вашу діяльність, що потрапила до недоброзичливців, конкурентів може призвести до величезних збитків. Тому, якщо така інформація існує і її можна дістати потайки від вас, її краще захистити всіма можливими способами. Оскільки питання захисту інформації так важливе при веденні бізнесу, є великий попит на різноманітні засоби обмеження несанціонованого доступу, і, як наслідок, значна кількість фірм працює в цій галузі.

(пропозиціїї щодо розв′язання проблеми)

Розглянемо спочатку фірми, які працюють в сфері захисту приміщень від несанкціонованого доступу і прослуховування.

Всі фірми, цієї галузі можна розділити на наступні групи:

1. Охоронні фірми
2. Фірми-виробники броньованих дверей, сейфів,і т.і.
3. Виробники систем безпеки світового масштабу та їх дистриб'ютори
4. Фірми, що займаються інтелектуальним захистом приміщень.

Охоронні фірми – найбільша категорія серед представлених(В Москві серед 26 фірм, що працюють в цій галузі та сайти яких є в Інтернеті – 18 охоронних). Фірми працюють переважно на місцевому рівні. Продукт охоронних фірм найменш наукоємкий, співробітники переважно мають лиш середню освіту. Вони надають послуги з захисту банківських приміщень, приміщень магазинів, особистої охорони, супроводять проведення важливих переговорів, охороняють вантажі, встановлюють сигналізацію, якщо остання спрацьовує оперативно з'являються на місце події. В функції співробітників цих фірм крім забеспечення охорони майна та персоналу об'єктів входить перевірка службових приміщень на наявність підслуховуючих пристроїв.

(обгрунтування пропозицій та вибір альтернатив)

В цій групі конкуренція найбільша серед усіх представлених: на цей ринок легко ввійти, набір послуг стандартний і тому споживач може легко змінити фірму на іншу, з меншою вартістю послуг. Щоб якось виділитися охоронні фірми надають послуги з встановлення відеонагляду, детективні послуги, встановлюють системи контролю і управління доступом.

(Здійснення пропозицій урядовими і неурядовими організаціями)

Серед охоронних структур(принаймні, в Україні, Росії ) значна частка державних. Оскільки за цими фірмами стоїть держава, то в свідомості споживачів вони будуть надійнішими проти приватних. Існують також випадки, коли такі фірми використовували свою приналежність до влади: на кількох рекламних щитах в місті Києві висіла реклама державного охоронної структури, причому без проплати рекламних площ цією структурою, в той час як безкоштовно(за законодавством про рекламу) має виділятися лиш незначний відсоток рекламних площ і лише під соціальну рекламу. Такі випадки негативно впливають на конкуренцію.

(необхідні ресурси та умови)

Для дотримання чесної конкуренції, а звідси – поліпшення якості послуг, необхідно відділити охоронні фірми від держави, зробивши їх такими ж економічними гравцями як і інші приватні структури.

Ресурсом робочої сили дані структури забеспечені, і, якщо навіть попит на дані послуги різко збільшиться, то проблеми в її нестачі не буде, оскільки робота не вимагає виняткових знань.

В країнах з перехідною економікою, малі фірми часто не мають коштів на утримання охорони, через це збільшується рівень злочинності. Тому держава зацікавлена надавати їм податкові знижки, в обмін на належне утримання охорони(це також стосується і наступних пунктів)

(обгрунтування пропозицій та вибір альтернатив)

Друга група містить в собі дві підгрупи:

* виробники світового рівня та їх дистриб'ютори
* місцеві фірми

В кожній з груп конкуренція дуже сильна, але вона значно слабша між представниками різних груп. Місцеві фірми можуть краще забеспечити індивідуальні вимоги споживача, врахувати можливості споживача і видозмінити свій продукт, дистриб'ютори ж обмежені в цій можливості.

Дистриб'ютори ж використовують добре ім'я фірми-виробника, чого місцеві конкуренти не в змозі протипоставити(тому такі фірми лідирують в поставці броньованих автомобілів, автомобілів VIP-класу).

(пропозиціїї щодо розв′язання проблеми)

Виробники систем безпеки світового масштабу поширюють свою продукцію на місцевому ринку через дистриб'юторів. Це такі фірми, як MITSUBISHI ELECTRIC, Полмі Групп(Россія). Серед їх продукції: відеокамери, спецвідеомагнітофони, цифрові системи безпеки.

Найбільш наукомістку продукцію серед представлених надають фірми, що займаються інтелектуальним захистом прміщень. Переважна більшість з них надає такі послуги(такі послуги та продукція представлені на сайтах цих підприємств, що полегшує вихід на них клієнтів; на сайтах міститься детальна інформація про послуги фірм, їх продукти, параметри продуктів, практичні поради):

# проведення практичних робіт з виявлення в приміщеннях (офісах, кабінетах, квартирах, дачах) Замовника:

- радіовипромінювальних засобів негласного одержання інформації (ЗНОІ);

- ЗНОІ, встановлених на телефонних лініях зв'язку;

- ЗНОІ, що використовують для передачі інформації різні дротові комунікації;

- ЗНОІ, що працюють в інфрачервоному діапазоні;

- недієві на момент перевірки ЗНОІ;

- акустичних і віброакустичних каналів витоку мовної інформації (через суміжні стіни, вікна, по системах центрального опалення і вентиляції);

- інших технічних каналів витоку акустичної інформації.

2. Проведення робіт з пошуку ЗНОІ в автомашинах Замовника.

3. Контроль радіоэфіру під час відповідальних нарад і переговорів, проведених Замовником, з метою виявлення фактів витоку інформації з радіоканалу.

4. Здійснення апаратурних перевірок, у тому числі з застосуванням методів нелінійної радіолокації і контролю, що не руйнує (рентгеноскопія):

- технічних засобів, встановлюваних у приміщеннях Замовника, на наявність у них ЗНОІ чи каналів витоку інформації. Перевірка може проводитися як у приміщеннях Замовника, так і в лабораторних умовах ;

- провідних комунікацій, телефонів, комп'ютерів і інших засобів побутовий і оргтехніки на наявність побічних електромагнітних випромінювань і наведень, що створюють можливість витоку оброблюваної чи переданої інформації обмеженого доступу.

5. Укомплектувати службу безпеки устаткуванням по пошуку і захисту інформації , навчання фахівців.

Такі послуги, як зазначалось вище - доволі стандартні, і частково надаються вже охоронними фірмами. Тому логічним наслідком надання лиш стандартного пакету послуг було б послаблення позицій фірми на ринку, витіснення її фірмами з більш широким і оригінальним набором послуг. Лідери в цій області намагаються виокремитися серед інших наданням унікальної послуги(послуг).

Так, найбільше мене вразила пропозиція російської фірми “Спецлабораторія”:

В приміщенні замовника встановлюється обладнання, що викоує дії, якщо хтось несанкціоновано проник в приміщення. Ця функція корисна в тому випадку, коли для порятунку життя чи майна злочинцю потрібно показати, що його дії записуються і знищити запис неможливо. Наприклад, при захопленні заручників.  
 Так, якщо в момент здійснення акції зловмисник побачить на телевізорі в чи кімнаті на екрані комп'ютера себе і свої дії вже в записі, а також відеокоментар до них, у якому докладно пояснюється, що це значить і чим йому загрожує, то у всякої більш-менш розсудливої людини пропаде бажання продовжувати заробляти собі в’язничний термін.

*Вся інформація може записуватися в "чорний ящик", до якого може бути виключений доступ навіть хазяїна, він може бути перенесений до сусідів, замурований у стіну і т.і., тобто встановлений так, що найближчим часом доступ до нього виключений.*

*Тут ви можете задати автоматичне відтворення тільки що записаної відеоінформації через ...секунд після закінчення запису після спрацювання якої-небудь події чи датчика, а також для більшої переконливості супроводити демонстрацію відеокоментарем.*

(обгрунтування пропозицій та вибір альтернатив)

Надання такої послуги немов закріплює за фірмою певну область розвитку систем інтелектуального захисту приміщень, оскільки

* право надавати певні унікальні послуги дуже часто закріплено патентом, бо послуга ґрунтується на винаході;
* невизначеність: чи буде отримано прибуток від входу на цей ринок, чи будуть виправдані затрати?

Тому конкуренція в цій області не така сильна як серед охоронних фірм, але потреби споживачів, що зростають, примушують фірми вдосконалювати свої продукти знов і знов, тим більше, що споживачу дешевше замовити захист свого приміщення в охоронній фірмі. Отже, сильною є конкуренція між різними групами однієї галузі.

Через те, що багато країн не дотримують належним чином захист прав інтелектуалної власності, фірми інтелектуального захисту приміщень в більшості випадків є регіональними, але аж ніяк не міжнародними.

Сфера захисту інформації, що збережена на комп′ютерних носіях.

“Комп′ютерні віруси – міф, на кшталт казок про крокодилів в каналізації Нью-Йорка”, - заявив у 1988 році Пітер Нортон, директор фірми Symantec, що займається випуском програмних продуктів. Ці слова, однак, не завадили фірмі через деякий час наладити випуск власного антивірусного пакету, що є одним з самих популярних на даний момент: Norton Antivirus.

(аналіз проблеми)

Перші комп′ютерні віруси з′явились в кінці 1960-х, їх основна шкода на той час полягала в тому, що вони швидко створювали копії самих себе і зменшували таким чином продуктивність системи. Зараз тільки відомих вірусів більше 50000 і деякі з них призводять до повного знищення інформації, що присутня на комп′ютері шляхом форматування диску. Програми-шпіони можуть записати ваші дії за комп′ютером і потім в непомітний для вас спосіб передати цю інформацію через Інтернет. Загрузивши необхідний для вашої праці продукт з Інтернету, ви можете непомітно для себе “скачати” троянський вірус, остання модифікація якого навмисне шукає на вашому комп′ютері файли платіжної системи WebMoney і надсилає цю інформацію через Інтернет зловмиснику. Потреба в захисті інформації породила цілу галузь фірм-виробників антивірусних програм.

(пропозиціїї щодо розв′язання проблеми)

За визначенням журналу РС-magazine, стандартна антивірусна програма повинна вміти:

1. Створювати аварійну дискету;

2. Сканувати завантажувальний сектор і створювати копію вихідного завантажувального сектора;   
3. Сканувати файли, включаючи архівні (.ARJ, .ZIP, .RAR);   
4.Сканувати оперативну пам'ять;   
5. Автоматично сканувати диск по заздалегідь заданому розкладі. Наприклад, щоночі в 2 години;   
6. Перевіряти файли при їхньому надходженні на комп'ютер. При звертанні до дискового чи мережного пристрою, сканувати ці пристрої в пошуках вірусів. При перезавантаженні перевіряти, чи не залишилася в дисководу дискета, і попереджати про це   
користувача;

7. Сканувати диск у фоновому режимі. Тобто, поки ви працюєте, програма-антивірус повинна відслідковувати, "щоб звіриною стежкою в край навіки рідний ніколи не пройти ніякому ворогу";   
8. Виявляти макро-віруси в документах Word і Excel;   
9. Реєструвати результати перегляду у виді звіту на чи екрані в роздруківці.

(обгрунтування пропозицій та вибір альтернатив)

Ці функції стандартні, тому конкуренція розгортається в іншому наборі характеристик:

1. Вартість продукту;
2. Вірусна база(кількість вірусів, що їх програма може знешкодити);
3. Швидкість сканування на наявність вірусу;
4. Можливість оновлення продукту;
5. Авторитетність фірми-виробника;
6. Національний аспект.

Вартість продукту має в більшості випадків вирішальне значення, тому більшість споживачів у 1998 році надали б перевагу програмі Norton Antivirus 4.0 – найкращою програмою того року перед ТhunderByte 8.03, що була удвічі дорожчою.

Антивірусний пакет від McAfee взагалі можна скачати з Інтернету безкоштовно, але за кожне(!) оновлення вам буде запропоновано заплатити непогані гроші.

Кращу політику у сфері оновлення програми через Інтернет має AVP Кашперського: споживач платить одноразово досить велику суму, але отримує протягом року оновлення безкоштовно.

На даний момент найбільші антивірусні бази мають Panda Antivirus(> 52000) i AVP(~50000), при чому перший працює швидше.

Звичайно будь-якому споживачеві зручно користуватися програмним продуктом написаним його рідною мовою, тому на просторах СНД найпопулярнішим є російський AVP, хоча як було зазначено він поступається антивірусові Раnda.

(необхідні ресурси та умови)

Особливостями галузі є:

* Висока наукоємкість(спеціалісти цієї галузі є фактично хакерами-навпаки);
* Висока невизначеність, залежність від інших факторів(якщо за період не з′явилось потужного вірусу споживачі набагато менш купують антивірусні програми та їх оновлення, в періоди ж комп′ютерних пандемій або очікувань активізації вірусів продаж виростає в кілька разів)
* Затрати на доставку до споживача ~0, оскільки майже всі якщо не всі антивіруси можна скачати з Інтернету.

Тому можливо для зменшення невизначенності для цих фірм варто було б на конкурсній основі пропонувати розробляти програмні продукти для урядових органів. Таким чином, вони б мали постійне джерело надходження коштів.

(Здійснення пропозицій урядовими і неурядовими організаціями)

Спеціальні урядові органи, або підрозділи в органах мають здійснювати нагляд за нормальним фунціюванням комп′ютерних систем урядових організацій; оперативно повідомляти громадскість про можливу загрозу вірусу або спростовувати такі повідомлення.

Значна проблема полягає в різному ступені надійності різноманітних засобів захисту на ринку. В США з метою вирішення цього питання АНБ(Агенство Національної Безпеки) установило партнерські стосунки з Національним інститутом стандартів і технологій (НІСТ). У рамках цього партнерства АНБ і НІСТ будуть здійснювати атестацію комерційних лабораторій, для того, щоб вони могли проводити експертизу засобів захисту, підтверджуючи параметри захисту, про які заявляє продавець, або їхня відповідність критеріям захисту, застосовуваним у конкретній комп'ютерній мережі. Іспити продуктів будуть проводиться атестованими лабораторіями на платній основі; при цьому лабораторія і фірма, що реалізує продукт на ринку, будуть домовлятися про розміри оплати і терміни.

Галузь пошуку інформації.

Як вже було сказано вище, інформація на початку нового тисячоліття перетворюється в найдорожчий ресурс і оперативне отримання інформації дає перевагу над конкурентами, які її не мають. Є два основних види інформації:

1. Первинна – та, що отримується безпосередньо в місцях її виникнення, дані отримані шляхом проведення спеціальних досліджень;
2. Вторинна, відомості за результатами досліджень, що проводились раніше, аналітичні узагальнення(статистичні бюлетені, публікації, огляди).

Первинна інформація може бути отримана від:

* Власного, створеного “під дослідження” підрозділу фірми;
* Спеціалізованої консалтингової фірми(Агенство Маркетингових Досліджень, SOCIS Gallup-Ukrain);
* Рекламного агенства(TMA-Draft).

Після замовлення такого дослідження, перелічені структури розробляють анкету з ключовими запитаннями, наймають додатковий персонал, якщо такий потрібен, проводять збір даних шляхом телемаркетингу, опитування, систематизують дані, підбивають підсумки, передають результати замовнику.

(обгрунтування пропозицій та вибір альтернатив)

Перевагами в цій галузі вважається:

1. Вартість послуг,
2. Авторитетність,
3. Регіональна представленість.

# Ясно, що така авторитетна фундація як SOCIS Gallup-Ukrain, буде мати більшу вартість послуг, ніж скажімо TMA-Draft, але для проведення аналізу попиту на окремий вид цигарок запрошувати монстра SOCIS Gallup-Ukrain нема необхідності.

# Отримання первинної інформації часто потребує досить значних коштів, і отримана, скажімо, консалтинговою фірмою інформація часто “підбивається” під інтереси клієнта і не дає останньому справжнього стану справ. Тому вторинна інформація, що можливо й не повністю відповідає потребам, має свої переваги:

# Вона дешева;

* ЇЇ отримання швидке;
* Часто відомості можливо отримати лиш цим шляхом(держстатистика)

(пропозиціїї щодо розв′язання проблеми)

Вторинну інформацію можна знайти в спеціалізованих виданнях, таких як «Маркетинг», «Вісник АПК», «The Financial Times», але найшвидше це можна зробити за допомогою пошукових серверів Інтернету.

(Здійснення пропозицій урядовими і неурядовими організаціями)

Так, основні макроекономічні показники розміщені на сайтах державних комітетів зі статистики. В Україні на сторінці Держкомстату можна знайти інформацію про показники сільського господарства, промисловості, інвестиційної та будівельної діяльності, транспорту, структурні зміни, ексорт. Імпорт, споживчий ринок, ціни і тарифи, фінанси, грошові доходи, ринок праці, демографічну ситуацію і т.і. Така інформація безумовно потрібна для формування як державної політики щодо галузей господарства країни, так і для приватних підприємств та установ.

На серверах таких служб є спеціальні програми(їх називають роботами чи пауками), що збирають інформацію в Web і повертають на сервери всі знайдені сторінки. За їх допомогою навіть не досвідчений користувач зможе знайти необхідну інформацію ввівши перелік слів, які як він вважає присутні в потрібному документі.

(обгрунтування пропозицій та вибір альтернатив)

Факторами, за якими споживачі надають перевагу тому чи іншому пошуковому серверу є:

1. Пошукова база;
2. Розумний пошук(файли сортуються в категорії людьми, а не комп′ютером);
3. Простота в використанні;
4. Національна специфіка.

Лідером за пошуковою базою є Lycos з її 66-ма млн документами, вона також забезпечує розумний пошук документів(ранжування документів ведеться за кількістю пошукових слів в документі, інтервалу між словами в конкретній фразі документу). AltaVista ж наприклад дозволяє знайти документ, попередньо проранжувавши критерії пошуку (біля кожного слова, в міру його важливості споживач ставить ранг), таким чином найважливіші документи будуть в списку результатів першими, що дуже важливо в ситуації, коли таких результатів може бути кілька тисяч. Excite йде далі та пропонує знайти всі сторінки, схожі на вже знайдену(“more like this”), недостатком цієї пошукової системи є її хаотична побудова. Зразком простоти побудови титульної сторінки пошукового сайту може служити Google(http://www.google.com ), де крім пошукового віконця і опцій вибору мови нема більш нічого.

Але це все – англомовні сайти(виняток http://www.google.ru ), тому споживачі України часто користуються послугами як українських (http://www.meta-ukraine.com ) так і російських ( http://www.list.ru ) пошукових серверів. Основною перевагою яких є врахування специфіки мов, та пошук в межах вітчизняних ресурсів. Тому, крім випадку з появою http://www.google.ru , російські разом з українськими пошуковими сайтами не є на мій погляд конкурентами.

(Необхідні ресурси та вимоги)

Кадри для збору первинної інформації в більшості випадків не потребують спеціальної освіти, тому забеспечення ними – не становить проблеми. Спеціалісти в галузі web-дизайну, що їх потребує галузь вторинного пошуку інформації є поки що не в достатній кількості, тому й відносно високими є їх доходи.

Висновки:

Таким чином, на початку 21-го століття інформація перетворюється на найдорожчий ресурс. Оперативне отримання інформації частіш і частіш визначає, хто буде лідером в конкурентному середовищі.

Для полегшення пошуку, обміну, обробки інформації як фізичні особи, так і фірми використовують персональні комп'ютери приєднані до мережі Інтернет. Інформація, збережена на комп′ютерних носіях більш уразлива до зовнішнього несанкціонованого доступу порівняно з інформацією на папері, тому не дивно, що і фірми і приватні особи намагаються захистити свою інформацію від недозволеного доступу, руйнівного впливу вірусів.

Глобальна інформатизація і комп'ютеризація призвела до стрімкого розвитку ринку програмного забезпечення, що забезпечує як пошук так і захист інфомації.

Конкурентноздатність у цих галузях залежить від наступних факторів:

1. В сфері захисту інформації від прослуховування а також інформації, що збережена не на комп′ютерних носіях:

* Врахування потреб споживача;
* Авторитетність фірми-виробника;
* Забезпечення додаткових послуг, порівняно з конкурентами;
* Підтримка продукту в експлуатації;
* Оригінальна технологія виготовлення;
* Захищеність продукту патентами та ліцензіями;
* Здатність продукту виконувати як мога більше функцій;

1. В сфері захисту інформації, що збережена на комп′ютерних носіях:

* Вартість продукту;
* Вірусна база(кількість вірусів, що їх програма може знешкодити);
* Швидкість сканування на наявність вірусу;
* Можливість оновлення продукту;
* Авторитетність фірми-виробника;
* Національний аспект.

1. В галузі пошуку інформації.
2. Пошук первинної інформації:

* Вартість послуг,
* Авторитетність,
* Регіональна представленість.

1. Пошук вторинної інформації:

* Пошукова база;
* Розумний пошук(файли сортуються в категорії людьми, а не комп′ютером);
* Простота в використанні;
* Національна специфіка.

Загалом конкурентність продукції вища, якщо вона, маючи високі якісні показники, дешевша від аналогів; якщо вона краще задовільняє потреби споживача(національна специфіка) та якщо вона заснована на унікальній технології.

На мою думку, роль державних органів в цих галузях повинна полягати не в створенні підприємств, конкурентів приватних(так чи інакше – це буде нечесна конкуренція), а в контролі конкуренції, атестації підприємств, підтримання стабільного функціювання цих галузей шляхом урядових замовлень послуг(на конкурсній основі) в підприємств цих напрямків.

**ВИКОРИСТАНА ЛІТЕРАТУРА:**

1. Электронная энциклопедия вирусов AVP
2. Евгений Касперский, - Компьютерные вирусы в Ms-Dos, Москва-1992
3. С.В.Глушаков, Д.В. Ломотько, В.В.Мельников, - Работа в сети Интернет: учебній курс, Москва-2001
4. Internet: русские ресурсы - 1998
5. В.Н.Парсяк, Г.К.Рогов,- Маркетинговые исследования, Київ-2000
6. ОБОРОНА СТРАНЫ ОТ КИБЕРНЕТИЧЕСКОЙ АТАКИ: ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНОЙ СРЕДЕ
7. http://www.goal.ru