**Завдання на виконання контрольної роботи**

Теоретична частина

Засоби захисту інформації

Теоретична частина

1. Інформація: сутність, види та конфіденційність

2. Програмні засоби забезпечення захисту інформації

3. Технічні засоби забезпечення захисту інформації

Практична частина

Скласти опис сайту електронної комерції на обрану тему: „продаж музичних дисків”. Описати основні маркетингові заходи використані для просування своєї продукції. Обґрунтувати необхідність існування такого сайту, як ресурсу Internet

**Зміст**

Вступ

Теоретична частина

1. Інформація: сутність, види та конфіденційність

2. Програмні засоби забезпечення захисту інформації

3. Технічні засоби забезпечення захисту інформації

Практична частина

Література

**Вступ**

Проблема захисту інформації не є новою. Вона з'явилася ще задовго до появи комп'ютерів. Стрімке вдосконалювання комп'ютерних технологій позначилося й на принципах побудови захисту інформації.

З самого початку свого розвитку системи інформаційної безпеки розроблялися для військових відомств. Розголошення такої інформації могло привести до величезних жертв, у тому числі й людським. Тому конфіденційності (тобто нерозголошенню інформації) в перших системах безпеки приділялася особлива увага. Очевидно, що надійно захистити повідомлення й дані від розголошення і перехоплення може тільки повне їхнє шифрування.

Принципова особливість сучасної ситуації полягає в тому, що найважливішим завданням сьогодні стає захист інформації в комп'ютерних системах й мережах.

Широке впровадження комп'ютерів в усі види діяльності, постійне нарощування їхньої обчислювальної потужності, використання комп'ютерних мереж різного масштабу привели до того, що загрози втрати конфіденційної інформації в системах обробки даних стали невід'ємною частиною практично будь-якої діяльності.

**Теоретична частина**

**1. Інформація: сутність, види та конфіденційність**

Інформація - абстрактне поняття, що має різні значення залежно від контексту. Походить від латинського слова «informatio», яке має декілька значень:

- роз'яснення; виклад фактів, подій, витлумачення;

- представлення, поняття;

- ознайомлення.

Тобто, інформація – це нові знання, які отримує споживач (суб’єкт) у результаті сприйняття і переробки певних відомостей.

Види інформації

Інформацію можна поділити на види за кількома ознаками:

За способом сприйняття

Для людини інформація поділяється на види залежно від типу рецепторів, що сприймають її.

* Візуальна — сприймається органами зору.
* Аудіальна — сприймається органами слуху.
* Тактильна — сприймається тактильними рецепторами.
* Нюхова — сприймається нюховими рецепторами.
* Смакова — сприймається смаковими рецепторами.

За формою подання

За формою подання інформація поділяється на наступні види.

* Текстова — що передається у вигляді символів, призначених позначати лексеми мови.
* Числова — у вигляді цифр і знаків, що позначають математичні дії.
* Графічна — у вигляді зображень, подій, предметів, графіків.
* Звукова — усна або у вигляді запису передача лексем мови аудіальним шляхом.

За призначенням

* Масова — містить тривіальні відомості і оперує набором понять, зрозумілим більшій частині соціуму.
* Спеціальна — містить специфічний набір понять, при використанні відбувається передача відомостей, які можуть бути не зрозумілі основній масі соціуму, але необхідні і зрозумілі в рамках вузької соціальної групи, де використовується дана інформація.
* Особиста — набір відомостей про яку-небудь особистість, що визначає соціальний стан і типи соціальних взаємодій всередині популяції.

Конфіденційність інформації [information confidentiality] — властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

Слід відзначити, що в Україні інформація з обмеженим доступом поділяється на два різновиди – таємну і конфіденційну. Відповідно до Закону України „Про інформацію” до таємної інформації відносять такі відомості, розголошення яких завдає шкоди особі, суспільству і державі, та яка включає до свого складу державну або іншу визначену законом таємницю. Перелік видів таємної інформації визначається державою і закріплюється законодавчо. Державна таємниця включає в себе 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 визначені у встановленому законом порядку державною таємницею і підлягають охороні державою.

Виходячи з наведеного можна говорити про те, що захист інформації, віднесеної до конфіденційної, і перш за все до державної таємниці, слід вважати невід’ємною складовою національної безпеки України. Іншими словами, можна стверджувати, що інформаційна безпека визначається як захищеність важливих інтересів особи, суспільства та держави в інформаційній сфері, за якою забезпечується використання інформації в інтересах її суб’єктів, сталий розвиток держави, виявлення, попередження і ліквідація загроз національним інтересам.

Категорія національних інтересів в інформаційній сфері в повній мірі узгоджується з іншою категорією – національною безпекою, і співвідноситься між собою за схемою «частина» і «ціле». При цьому слід ураховувати, що інформаційна складова не може існувати поза цілями загальної національної безпеки, так само, як і національна безпека не буде всеохоплюючою без інформаційної безпеки.

У цілому політика національної безпеки держави спрямована на мінімізацію та, по можливості, уникнення існуючих чи потенційних внутрішніх або зовнішніх загроз розвитку держави у відповідності з її цілями.

Для застосування в мережних рішеннях обов'язковим є наявність засобів централізованого керування безпекою, ідентифікації, аутентифікації і засобів аудиту.

У комп'ютерних системах зосереджується інформація, право на користування якої належить визначеним обличчям чи групам обличч, що діє в порядку особистої ініціативи чи відповідно до посадових обов'язків. Щоб забезпечити безпеку інформаційних ресурсів, усунути можливість несанкціонованого доступу, підсилити контроль санкціонованого доступу до конфіденційного або до підлягаючого засекречуванню інформації, упроваджуються різні системи впізнання, установлення дійсності об'єкта (суб'єкта) і розмежування доступу. В основі побудови таких систем знаходиться принцип допуску і виконання тільки таких звертань до інформації, у яких присутні відповідні ознаки дозволених повноважень.

Ключовими поняттями в цій системі є ідентифікація й аутентифікація. Ідентифікація - це присвоєння якому-небудь чи об'єкту суб'єкту унікального імені чи образа. Аутентифікація - це встановлення дійсності, тобто перевірка, чи є об'єкт (суб'єкт) дійсно тим, за кого він себе видає.

Кінцева мета процедур ідентифікації й аутентификации об'єкта (суб'єкта) - допуск його до інформації обмеженого користування у випадку позитивної перевірки або відмовлення в допуску у випадку негативного результату перевірки.

Об'єктами ідентифікації й аутентификации можуть бути: люди (користувачі, оператори й ін.); технічні засоби (монітори, робочі станції, абонентські пункти); документи (ручні, роздруківки й ін.); магнітні носії інформації; інформація на екрані монітора й ін.

Установлення дійсності об'єкта може вироблятися апаратним пристроєм, програмою, людиною і т.п.

Пароль може використовуватися для ідентифікації і встановлення дійсності термінала, з якого входить у систему користувач, а також для зворотного встановлення дійсності комп'ютера стосовно користувача.

**2. Програмні засоби забезпечення захисту інформації**

Програмні засоби - це спеціальні програми і програмні комплекси, призначені для захисту інформації в ІС, наприклад, антивірусні програми, програми кілоггери (антікіллогери).

З засобів ПЗ системи захисту необхідно виділити ще програмні засоби, що реалізують механізми шифрування (криптографії), наприклад, програми генерації електронно-ціфрового підпису. Криптографія - це наука про забезпечення таємності і/чи автентичності (дійсності) переданих повідомлень.

Взагалі програмні кілоґґери (антікіллогери) належать до тієї групи програмних продуктів, які здійснюють контроль над діяльністю користувача персонального комп'ютера. Спочатку програмні продукти цього типу призначалися виключно для запису інформації про натиснення клавіш клавіатури, у тому числі і системних клавіш, в спеціалізований журнал реєстрації (Log-файл), який згодом вивчався людиною, що встановила цю програму (це може бути адміністратор безпеки, а може бути й зловмисник, дивлячись на те з якою цілью встановлена ця програма). Log-файл міг відправлятися по мережі на мережевий диск, ftp сервер в мережі Інтернет, по E-mail і так далі. В даний час програмні продукти, що зберегли «по-старому» дану назву, виконують ще й багато додаткових функцій — це перехоплення інформації з вікон, перехоплення кліків миші, перехоплення буфера обміну, «фотографування» знімків екрану і активних вікон, ведення обліку всіх отриманих та відправлених E-mail, моніторинг файлової активності, моніторинг системного реєстру, моніторинг черги завдань, відправлених на принтер, перехоплення звуку з мікрофону та відеозображення з веб-камери, підключених до комп'ютера і так далі, тобто вони фактично відносяться до абсолютно іншого класу програмних продуктів, а саме до моніторингових програмних продуктів.

Тільки метод застосування кілоґґерів (зокрема програмних продуктів, що включають кілоггер як модуль) дозволяє побачити грань між управлінням безпекою та порушенням безпеки.

Несанкціоноване застосування — встановлення кілоггера (зокрема апаратних або програмних продуктів, що включають кілоґґер як модуль) відбувається без відома власника (адміністратором, чи зловмисником) автоматизованої системи або без відома власника конкретного персонального комп'ютера. Несанкціоновано вживані кілоґґери (програмні або апаратні) іменуються як шпигунські програмні продукти або шпигунські пристрої. Несанкціоноване застосування, як правило, пов'язане з незаконною діяльністю (illegal activity). Як правило, несанкціоновано встановлювані шпигунські програмні продукти мають можливість конфігурації і отримання «скомплектованого» здійснимого файлу, який при інсталяції не виводить ніяких повідомлень і не створює вікон на екрані, а також мають вбудовані засоби доставки і дистанційної установки конфігурованого модуля на комп'ютер користувача, тобто процес інсталяції відбувається без безпосереднього фізичного доступу до комп'ютеру користувача і часто не вимагає наявності прав адміністратора системи.

Санкціоноване застосування — встановлення кілоґґера (зокрема апаратних або програмних продуктів, що включають кілоґґер як модуль) відбувається з відома власника (адміністратором безпеки) автоматизованої системи або з відома власника конкретного персонального комп'ютера. Санкціоновано вживані кілоґґери (програмні або апаратні) називаються моніторинговими програмними продуктами, англ. employee monitoring software, parental control software, access control software, personnel security programs і тому подібне. Як правило, санкціоновано встановлені програмні продукти вимагають фізичного доступу до комп'ютера користувача і обов'язкової наявності прав адміністратора для конфігурації і інсталяції;

За наявністю сигнатури в базах кіллоггери поділяються.

Відомі кілоґґери. До даної категорії відносяться кілоґґери, сигнатура яких вже включена до сигнатурних баз основних відомих фірм-виробників анти-шпигунських програмних продуктів і/або антивірусних програмних продуктів.

Невідомі кілоґґери. До даної категорії відносяться кілоґґери, сигнатура яких не включена до сигнатурних баз основних відомих фірм-виробників анти-шпигунських програмних продуктів і/або антивірусних програмних продуктів і, ймовірно, ніколи не буде в них включена з різних причин, а саме:

* кілоґґери (модулі), що розробляються під егідою різних урядових організацій;
* кілоґґери (модулі), які можуть створюватися розробниками різних закритих операційних систем і включатися до складу ядра операційної системи;
* кілоґґери, які розроблені в обмеженій кількості (часто тільки в одній або декількох копіях) для вирішення конкретного завдання, пов'язаного з отриманням критичної інформації з комп'ютера користувача (наприклад, програмні продукти, що вживаються мережевими адміністраторами, а можливо й зловмисниками). Дані програмні продукти можуть бути трохи видозміненими відкритими початковими кодами кілоґґерів, що взяті з мережі Інтернет та скомпільовані самим зловмисником, що дозволяє змінити сигнатуру кілоґґера;
* комерційні, особливо, включені як модулі в корпоративні програмні продукти, які дуже рідко вносяться до сигнатурних баз відомих фірм-виробників анти-шпигунських програмних продуктів і/або антивірусних програмних продуктів. Це приводить до того, що публікація зловмисниками в мережі Інтернет повнофункціональної версії даного комерційного моніторингового програмного продукту перетворює останній на програмний продукт, який не виявляється анти-шпигунськими програмними продуктами і/або антивірусними програмними продуктами;
* кілоґґери, що є модулями для перехоплення натискань клавіш на комп'ютері користувача, що включаються до складу програм-вірусів. До моменту внесення сигнатурних даних до вірусної бази ці модулі є невідомими. Приклад — всесвітньо відомі віруси, що натворили багато бід в останні роки, мають в своєму складі модуль перехоплення натиснень клавіатури і відправки отриманої інформації в мережу Інтернет.

**3. Технічні засоби забезпечення захисту інформації**

До технічних мір можна віднести захист від несанкціонованого доступу до системи, резервування особливо важливих комп'ютерних підсистем, організацію обчислювальних мереж з можливістю перерозподілу ресурсів у випадку порушення працездатності окремих ланок, установку устаткування виявлення і гасіння пожежі, вживання конструкційних заходів захисту від розкрадань, саботажу, диверсій, вибухів, установку резервних систем електроживлення, оснащення приміщень замками, установку сигналізації і багато чого іншого.

Вся сукупність технічних засобів захисту підрозділяється на апаратні і фізичні.

Апаратні засоби - пристрою, що вбудовуються безпосередньо в обчислювальну техніку, чи пристрою, що сполучаються з нею по стандартному інтерфейсі.

Системи будь-якої складності будуються на базі одних і тих же технічних пристроїв. При рішенні технічних завдань захисту й охорони в першу чергу необхідно вибрати основні параметри пристроїв, які забезпечать достатню надійність виконання покладених на них функцій. Система охоронна сигналізація фіксують факт несанкціонованого доступу на територію, що охороняється, передають сигнал тривоги, наприклад, на пульт охорони і включають виконуючі пристрої. Система охоронна сигналізація включають: датчики, пульт-концентратор, виконуючі пристрої.

Апаратні пристрої є мініатюрними пристроями, які можуть бути прикріплені між клавіатурою і комп'ютером або вбудовані в саму клавіатуру. Вони реєструють всі натиснення клавіш, зроблені на клавіатурі. Процес реєстрації абсолютно невидимий для кінцевого користувача. Щоб успішно перехоплювати всі натиснення клавіш, апаратні кейлоггери не вимагають установки ніякої програми на комп'ютері. Коли апаратний пристрій прикріплюють, абсолютно не має значення, в якому стані знаходиться комп'ютер — ввімкненому або вимкненому. Час його роботи не обмежений, оскільки він не вимагає для своєї роботи додаткового джерела живлення.

Об'єми внутрішньої незалежної пам'яті даних пристроїв дозволяють записувати до 20 мільйонів натиснень клавіш, причому з підтримкою юнікода. Дані пристрої можуть бути виконані у будь-якому вигляді, так що навіть фахівець не в змозі іноді визначити їх наявність при проведенні інформаційного аудиту. Залежно від місця прикріплення аппаратні кейлоггери підрозділяються на зовнішні і внутрішні.

Сучасні комп'ютерні засоби побудовані на інтегральних схемах. При роботі таких схем відбуваються високочастотні зміни рівнів напруги і струмів, що приводить до виникнення в ланцюгах живлення, в ефірі, у близькорозташеваної апаратурі і комп'ютерах у мережі і т.п. електромагнітних полів і наведень, що за допомогою спеціальних засобів (умовно назвемо їхній "шпигунськими") можна трансформувати в оброблювану інформацію. Тому, зі зменшенням відстані між приймачем порушника й апаратних засобів імовірність такого роду знімання і розшифровки інформації збільшується, унаслідок чого повинні дотримуватися нормативної відстані і ставитися захисні екрани і фільтри.

Підводячи підсумок, можна стверджувати, що інформаційна безпека передбачає можливість безперешкодної реалізації суспільством і окремими його членами своїх конституційних прав, пов’язаних з можливістю вільного одержання, створення й розповсюдження інформації. Поняття інформаційної безпеки держави слід також розглядати у контексті забезпечення безпечних умов існування інформаційних технологій, які включають питання захисту інформації, як такої інформаційної інфраструктури держави, інформаційного ринку та створення безпечних умов існування і розвитку інформаційних процесів.

Необхідний рівень інформаційної безпеки забезпечується сукупністю політичних, економічних, організаційних заходів, спрямованих на попередження, виявлення й нейтралізацію тих обставин, факторів і дій, які можуть вчинити збиток чи зашкодити реалізації інформаційних прав, потреб та інтересів країни і її громадян.

Слід зазначити, що поняття „інформаційної безпеки держави” розглядали Бондаренко В.О., Литвиненко О.В., Кормич Б.А., Остроухов В.В., Стрельцов А.А., Расторгуев С.П., Баринов А., Бучило И.Л., але, на наш погляд, інформаційна безпека держави – це стан її інформаційної захищеності, за якої спеціальні інформаційні операції, акти зовнішньої інформаційної агресії та негласного зняття інформації (за допомогою спеціальних технічних засобів), інформаційний тероризм і комп’ютерні злочини не завдають суттєвої шкоди національним інтересам.

**Практична частина**

* + - * скласти опис сайту електронної комерції на обрану тему: „продаж музичних дисків”. Описати основні маркетингові заходи використані для просування своєї продукції. Обґрунтувати необхідність існування такого сайту, як ресурсу Internet.

Здійснимо пошук інформації за музичними DVD дисками з записом у пошуковій системі загального призначення Rambler http://www.rambler.ru/ (рис.1).

Rambler — це рейтингова система, що володіє всіма основними функціями пошукових покажчиків. Як пошуковий покажчик, служба володіє одним з найбільших індексів в Росії, але їй явно бракує швидкодії і сучасних алгоритмів рейтингування результатів пошуку. Втім, це не дуже істотно, адже основну популярність служба придбала в першу чергу як рейтингова система. Вона дозволяє швидко виявити круг Web-вузлів, що поставляють інформацію на задану тему і оцінити їх популярність по кількості відвідин за останню добу. Ця характеристика якісності Web-ресурсу є відносною, але в тих випадках, коли йдеться про тему, що має суспільний інтерес, їй можна довіряти.

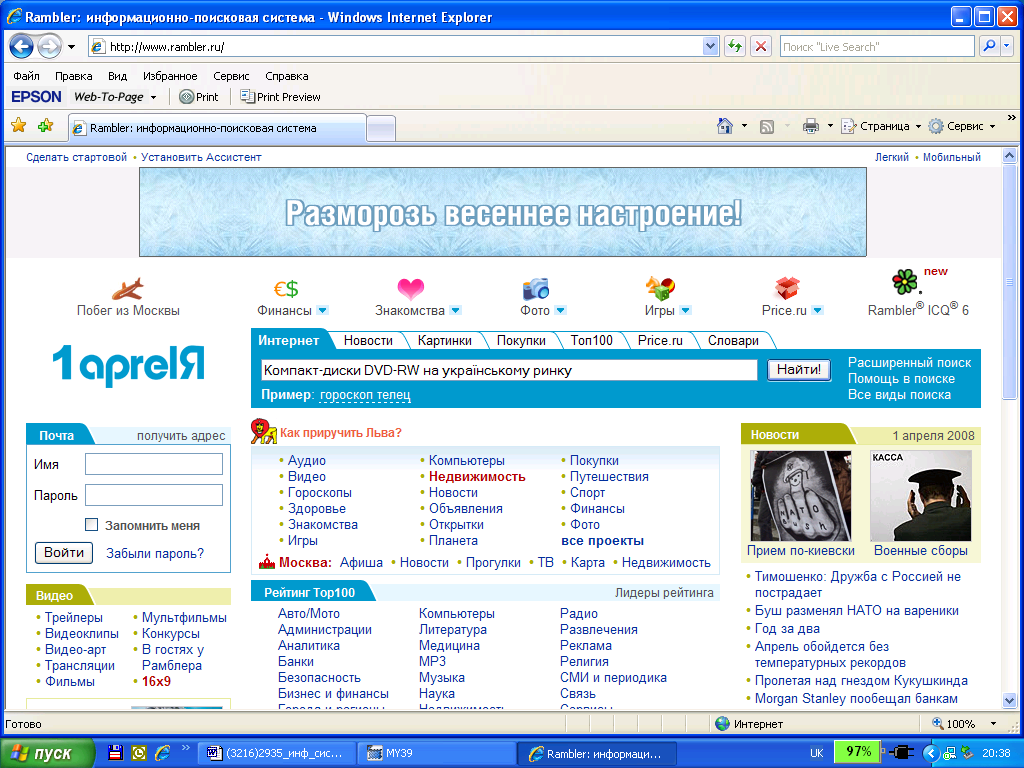


Рис.1.

Rambler - ймовірно, сама відвідувана інформаційно-пошукова система російського Інтернету та зони СНД (близько напівмільйона відвідувачів в день). Тут можна провести запит за допомогою ключових слів, пройтися по тематичному каталогу, поглянути на рейтингові таблиці, отримати останні огляди фінансових, політичних, комп'ютерних і інших новин.

Господар цієї мекки, Дмитро Крюков, переводить назву своєї системи як "гуляща людина". Проте, хай Вас не збентежує несерйозність назви. На сьогоднішній день Rambler, видно, є не тільки найпопулярнішим, але і наймогутнішим пошуковим механізмом в Мережі СНД. Пошукова база містить мільйони документів з більш ніж 20,000 сайтів (імен DNS). Має розвинуту мову запитів і гнучку форму виведення результатів. Rambler включений в стандартну поставку російської версії Microsoft Internet Explorer.

Мова запитів в Rambler стандартна і не вимагає спеціальних коментарів. Просунутим користувачам рекомендується скористатися можливістю детального запиту. Побачив наступне вікно (рис.2) натиснемо на гіперпосилання www.market.tut.ua .



Рис.2.

Назва магазину. MARKET.TUT - це всеукраїнський Інтернет-гіпермаркет, лідер в Україні серед 8000 сайтів торгової аудіо (відео) музичної тематики (рис.3).

Кожну добу MARKET.TUT допомагає тисячам людей знайти улюблене і необхідне, будучи глобальною торговою платформою. MARKET.TUT- популярний посередник, що допомагає продавцю і покупцю знайти один одного.

* 250 000 відвідувачів на місяць зі всіх регіонів України;
* 200 000 товарів і послуг.

Електронна адреса Інтернет-магазину: www.market.tut.ua/

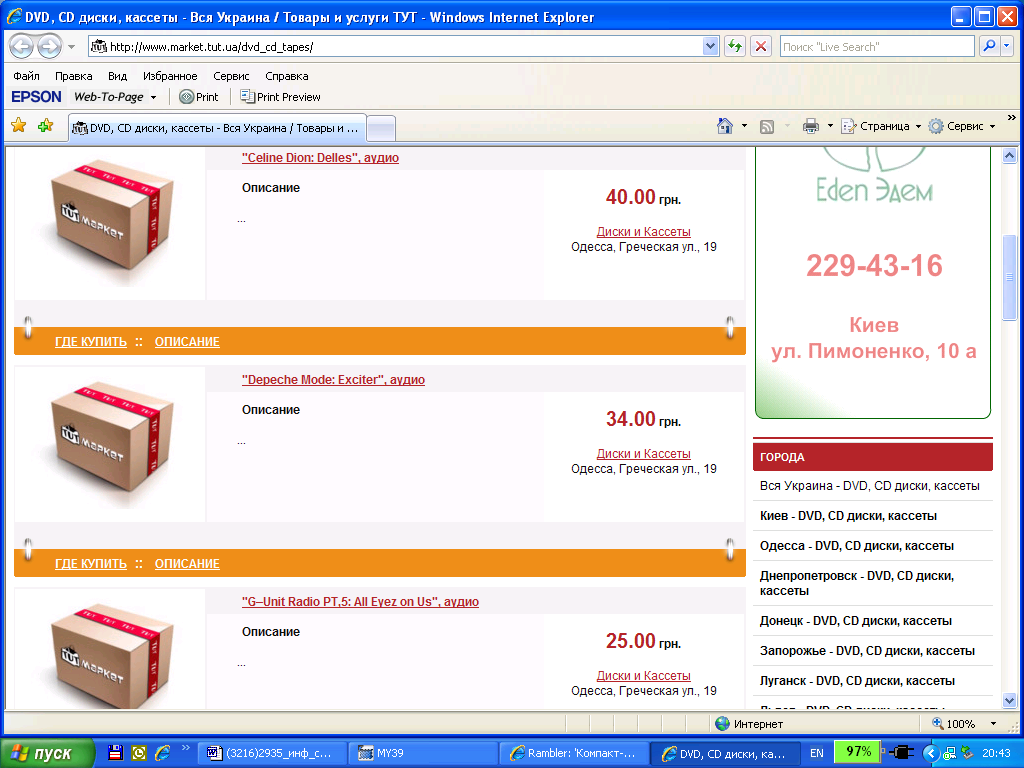


Рис.3

Географічний район діяльності Інтернет-магазину – вся Україна.

Напрямок діяльності магазину – торгівля товарами народного споживання, у тому числі аудіо, відео, побутової технікою й музичних дисків.

Групи товарів, якими торгує магазин:

|  |
| --- |
| Аудио Видео Теле Фото |
| Бытовая техника |
| Авто мото |
| Все для офиса |
| Все для дома |
| Домашние животные |
| Здоровье и красота |
| Компьютерная техника |
| Книги |
| Мебель |
| Мобильные телефоны и связь |
| Музыка, фильмы, игры, программы |
| Недвижимость |
| Нефтепродукты и хим. продукция |
| Одежда, обувь, галантерея |
| Охрана и безопасность |
| Продукты и напитки |
| Подарки, сувениры , цветы |
| Сад, ландшафт, озеленение |
| Спорт |

Меню гіперпосилань, що знаходиться праворуч надає можливість обрати місце України, у якому покупцеві буде найбільш зручніше придбати потрібний диск або касету. Головний лівий фрейм також містить гіперпосилання на адресу придбання, опис продукції, а також на назву конкретного диску чи касети.

Натиснув на гіперпосилання уверху отримаємо потрібну нам інформацію по музичним DVD дискам з записом, та зведемо цю інформацію до таблиці 1.

Таблиця 1 Диски і касети

|  |  |  |  |
| --- | --- | --- | --- |
| Адреса | г. Одеса, Грецька. вул., 19 | | |
| Характеристики товару | DVD - оптичний диск, який майже не відрізним від звичайного CD, але він вміщає в 7 разів більше інформації. Що це дає Вам: більш якісний звук і високу якість зображення. | | |
| Місця постачання | Одеса | | |
| Телефон | 8 (048) 711-78-86 | | |
| Факс | 8 (048) 711-78-86 | | |
| Моб. телефон |  | | |
| Режим роботи | цілодобово, без вихідних. | | |
| Як проїхати | Грецька кут Решильевська, магазин "Диски та Касети". | | |
| E-mail | | office@dtak.ua | | | |
| URL | | http://www.dtak.ua | | | |
| DVD, CD диски, касети | | | |
|  | "Celine Dion: Delles", аудіо | 40.00 |  |
|  | "Depeche Mode: Exciter", аудіо | 34.00 |  |
|  | "G–Unit Radio PT,5: All Eyez on Us", аудіо | 25.00 |  |
|  | "G–Unit Radio Pt,7: King of New York", аудіо | 25.00 |  |
|  | "Nelly Furtado: Loose", аудіо | 25.00 |  |
|  | "Suzanne Vega: Beauty & Crime", аудіо | 34.00 |  |
|  | "The Police, Synchronicity Concert", відео | 35.00 |  |
|  | "В ожидании чуда", відео | 59.00 |  |
|  | "Верка Сердючка: Dancing lasha tumbai", аудіо | 25.00 |  |
|  | "Груз 200", відео | 40.00 |  |
|  | "Жатва", відео | 42.00 |  |

Натиснув кнопку „Купить”, та заповнивши коротку анкету, що з’явилась треба натиснути кнопку Заказати. Товар – диск Depeshe Mode попаде у кошик.

Далі надамо інформацію про кошик на мові оригіналу:

Чтобы положить что-нибудь в корзину, выбирайте товары или услуги через наш каталог. Когда товар заинтересует Вас, нажмите и товар попадет в корзину.



в каталоге TUT.MARKET



О корзине

* Заказ из Вашей корзины уходит к продавцу/ам товара или услуги
* Выбранные позиции хранятся в корзине 7 дней
* Историю своих заказов Вы сможете просматривать в сервисе Мой кабинет, в том случае если Вы являетесь зарегистрированным покупателем

Оплату за товар можна здійснити кредитною пластиковою картою, наприклад, банку Форум чи Приватбанку.

Ціна доставки товару включено у ціну товару. Доставка здійснюється по пошті на адресу покупця, яку він вказує в анкеті.

Інтернет-магазином дійсно вдобно користуватися. Він вдало продуманий й організований. Але не сподобалась деякі завищені ціни на певні види аудіо- відео-дисків.

На закінчення, можна дати наступні висновки й рекомендації по пошуку в Інтернеті потрібного продукту:

• для реферативного пошуку користуйтеся пошуковими каталогами;

• для поглибленого пошуку користуйтеся пошуковими покажчиками;

• для спеціального пошуку заздалегідь розшукайте персональні списки посилань, що складені колегами;

• для пошуку "скомпрометованої інформації", наприклад складеної з явними помилками, користуйтеся рейтинговими системами;

• при виборі служби для контекстного пошуку в СНГ краще зупинитися на "Апорт 200" або "Yandeх", а за рубежем альтернативи таки - краще всього використовувати пошукові служби Yahoo, Google і Alta Vista.

**Література**

1. Закон України "Про електронні документи та електронний документообіг" від 22 травня 2003 p. № 851-IV;
2. Закон України "Про цифровий підпис" від 22 травня 2003 p. № 852-IV;
3. Быков ВЛ. Электронный бизнес и безопасность. — М.: Радио и связь, 2000;
4. Голдовский И. Безопасность платежей в Интернете. — СПб.: Питер, 2001. — 240 с.;
5. Електронна комерція: Навч. посібник / А.М. Береза, І.А. Козак, Ф.А. Шевченко та ін. – К.: КНЕУ, 2002. – 326 с.;
6. Задірака В.К., Олексюк О.С. Методи захисту фінансової інформації: Навч. посіб.— Т.: Збруч, 2000. — 460 с.;
7. Затонацька Т.Г., Плескач В.Л. Електронна комерція. Підручник. – К.: Знання. – 2007. – 535 с.;
8. Макарова М.В. Електронна комерція: Посіб. – К.: Академія, 2002. – 272 с.;
9. Обеспечение безопасности коммерческой информации в интернет/интранет-сетях. // http://www.ibdarb.ru/publication/Scorod\_paper5.htm
10. Search Engine Colossus – поисковые системы от A до Z.