

коналення наявної системи управління земельними ресурсами, відкривши при цьому нові можливості та перспективи розвитку прозорого механізму управління, що за своєю суттю має стратегічно важливе значення для системи державного управління загалом.

Література

1. Биков І.Ю. Microsoft Office в задачах економіки та управління / І.Ю. Биков, М.В. Жирнов, І.М. Худякова. – К. : ВД "Професіонал", 2006. – 264 с.
2. Лозниця В.С. Психологія менеджменту : навч. посібн. – К. : УВПК "Екс об", 2000. – 512 с.
3. Мошек Г.Є. Організація праці менеджера / Г.Є. Мошек. – К. : Вид-во КДТЕУ, 1995. – 186 с.
4. Немцов В.Д. Менеджмент організацій : навч. посібн. / В.Д. Немцов, Л.Є. Довгань, Г.Ф. Сініок. – К. : УВПК "Екс об", 2000. – 392 с.
5. Скороходов В.А. Менеджмент вищої школи : навч. посібн. / В.А. Скороходов. – Миколаїв : Вид-во ПСІ КСУ; вид-во "Гінкул Г.Р.", 2003. – 356 с.
6. Сохнич А.Я. Проблеми використання і охорони земель в умовах ринкової економіки : монографія / А.Я. Сохнич – Львів : Вид-во "Українські технології", 2002. – 252 с.
7. Сохнич А.Я. Стан наукової думки в сучасних реаліях : монографія / А.Я. Сохнич. – Львів : ТзОВ "Ліга-Прес", 2009. – 152 с.
8. Хміль Ф.І. Основи менеджменту : підручник / Ф.І. Хміль. – К. : Вид-во "Академвидав", 2003. – 608 с.

Сохнич А.Я., Худякова І.М., Сохнич А.А. Геоинформационные системы в управлении земельными ресурсами

Раскрыты вопросы геоинформационных систем и их использование в управлении земельными ресурсами. Установлено, что развитие государственной системы подготовки, переподготовки и повышения квалификации кадров в сфере землепользования приведет к совершенствованию имеющейся системы управления земельными ресурсами, открыв при этом новые возможности и перспективы развития прозрачного механизма управления, которое по своей сути имеет стратегически важное значение для системы государственного управления в целом.

Ключевые слова: геоинформационные системы, информационные технологии, управление земельными ресурсами.

Sokhnych A.Ya., Hudyakova I.M., Sokhnych O.A. Geoinformation systems in land resources management

It is considered question of geoinformation systems and their application in management of land resources. Described that development of the state system of preparation, retraining and in-plant of shots training in the field of land-tenure will bring to perfection of the present system a management over the landed resources, opening new possibilities and prospects of development of clear mechanism of management which on the essence has strategically an important value for the whole system of state administration.

Keywords: geoinformation systems, information technologies, management of land resources.

УДК 332.025:334

Доц. М.І. Бублик, канд. фіз.-мат. наук;
магістрант І.С. Войтух – Львівський ДІНТУ ім. В. Чорновола

ЗАХИСТ І БЕЗПЕКА МАРКЕТИНГОВОЇ ІНФОРМАЦІЇ

Досліджено потребу у створенні різних систем захисту з урахуванням особливостей та умов їхнього функціонування. Розглянуто основні засоби, методи і напрямки захисту маркетингової інформації, а також висвітлено регулювання цього пи-

тання на державному рівні. Запропоновано систему заходів з формування ринку послуг із захисту маркетингової інформації в Україні.

Ключові слова: інсайдери, Spectog 360, технічний та мережевий захист інформації, розподіл доступу, метод паролів.

Проблема безпеки інформації завжди хвилювала суспільство. Вона полягає в тому, що за певних умов, уся інформація, якою володіють організації, фірми, корпорації та інші економічні одиниці, потребує постійного захисту. Серед загроз можна виокремити несанкціоновані знищення, зміну, копіювання, блокування санкціонованого доступу до даних тощо. По суті, будь-яке втручання в інформаційну систему здійснюють з метою доступу до інформації. Тому система захисту інформації сьогодні стає невід'ємним складником господарської діяльності бізнесу.

Актуальність дослідження теми. З огляду на поширення використання інформаційних технологій у повсякденному житті, кожна людина дедалі частіше стикається з необхідністю захисту маркетингової інформації, і саме тому питання інформаційної безпеки стає таким важливим і актуальним. Пов'язано це з ростом можливостей обчислювальної техніки. Адже розвиток засобів, методів і форм автоматизації процесів оброблення інформації роблять інформацію набагато уразливішою.

Аналіз останніх публікацій та досліджень. На сьогодні проблемі захисту і безпеки інформації приділяють пильну увагу. Це питання дедалі актуальніше постає перед організаціями, адже втрата маркетингової інформації послаблює їхні позиції на ринку і робить їх менш конкурентоспроможними. Баглай А.В., А.О. Новіцький, М.В. Захарова у публікації [5] зазначають: "Різноманіття варіантів побудови інформаційних систем породжує необхідність створення різних систем захисту, що враховують індивідуальні особливості кожної з них. Від оптимальності вибору засобів захисту інформації залежить побудова будь-якої системи захисту інформації (СЗІ), тому потрібно сформулювати чітке уявлення про те, як побудувати СЗІ для конкретної інформаційної системи, з урахуванням властивих їй особливостей і умов функціонування".

Важливість захисту інформації коментує і О. Снитнікова у роботі [4]: "Треба зазначити, що суспільство усвідомлює гостру необхідність вирішення проблем безпеки інформації. Тому кожна інформаційна система, як правило, передбачає і власну систему інформаційного захисту, бо алгоритми, що були використані у попередніх розробленнях, можуть створювати потенційні загрози зовнішнього втручання у новій системі. Це залежить від платформи розробки, від її інформаційної структури, схеми взаємодії пов'язаних частин системи тощо. Підтвердженням важливості питання інформаційної безпеки є також збільшення годин та введення додаткових дисциплін, що стосуються захисту інформації, для студентів навчальних закладів, спеціальності яких пов'язані з інформаційними технологіями, програмуванням. В свою чергу, збільшення кваліфікованих спеціалістів у будь-якій сфері інформаційних технологій, завжди приводить до її швидкого і успішного розвитку".

У публікації [5] наголошено на тому, що, цитую: "Важливо, щоб засіб захисту не тільки виконував свої функції й забезпечував очікуваний захист,

але і не збільшував ризик функціонування інформаційної системи (ІС) через конфлікт із деякими іншими засобами захисту. Кожний засіб повинен спочатку бути перевіреним, щоб гарантувати, що він забезпечує очікуваний захист".

До програмних засобів, які відповідають за захист і безпеку маркетингової інформації варто віднести такі [3]: StrongDisk Server v.4.1, Смарт-карта NXP JCOP 21-72Kb, ACR12, Precise 100 PC-Card, Zlock.

Метою цієї роботи є аналіз систем захисту інформації (СЗІ) у контексті стрімкого розвитку інформаційних технологій, які збільшують ймовірність несанкціонованого доступу до них, а також пошук надійних складових систем захисту маркетингової інформації.

Виклад основного матеріалу. Для досягнення ринкового успіху підприємству необхідна актуальна, достовірна та вичерпна інформація про клієнтів, конкурентів, постачальників, посередників. Цінність маркетингової інформації полягає в тому, що вона створює передумови для здобуття конкурентних переваг, допомагає знизити рівень комерційного ризику, визначити й урахувати зміни в навколишньому бізнес-середовищі.

Враховуючи те, що маркетингова інформація, за визначенням [2, с. 5], – це сукупність даних, повідомлень, відомостей, які характеризують маркетингове середовище, об'єкти, явища, процеси, зв'язки тощо та які необхідно збирати, передавати, нагромаджувати та обробляти для прийняття управлінських рішень, її ототожнюють із ресурсом. Багато науковців [2, с. 7] застосовують ресурсний підхід до поняття інформації. У такому разі, як ресурс, інформація має властивості товару і її можна продати, купити, нагромаджувати, знищити і тощо. Тому важливим для утримання конкурентних переваг на ринку кожної фірми є питання конфіденційності, тобто захисту інформації від конкурентів.

На жаль, однією з головних загроз для компаній з точки зору захисту інформації є власні співробітники, яких називають інсайдерами. Інсайдери – це співробітники, які навмисно, через необережність або незнання стають причиною витоку конфіденційної інформації, до якої вони мають доступ для виконання службових обов'язків. Найбільшого збитку завдають ті з них, хто продає дані конкурентам компанії. Для боротьби з цим американська компанія Spector Soft Corporation [6] розробила продукт Spector 360, який призначений для централізованого моніторингу співробітників. Антиінсайдерна програма досліджує, як співробітники використовують свої робочі комп'ютери та мережу Інтернет. Spector 360 дає змогу інспектувати діяльність всієї організації за допомогою графічних діаграм.

Крім цього, проаналізуємо поняття "захист інформації", під яким у роботі [1, с. 67] розуміють комплекс заходів для забезпечення фізичної цілісності інформації, запобігання несанкціонованим змінам і отриманню даних, а його характеристиками є достовірність даних, конфіденційність, цілісність та доступність інформації.

Ієрархічно задачі захисту ІС можна поділити на 2 рівні, які, своєю чергою, мають підрівні, а саме:

1. Вчасне забезпечення процесів ухвалення рішень достовірною інформацією на основі введених до ІС даних.

1.1. Достатня повнота даних для процесів підтримки ухвалення рішень (ПППР).

1.2. Достовірність вихідних даних для процесів прийняття рішень.

1.3. Достатня швидкість прийняття рішень.

1.3.1. Доступність механізмів прийняття рішень.

1.3.2. Гарантованість відповіді після отримання запиту.

2. Забезпечення конкурентоспроможності діяльності фірми.

2.1. Збереження конфіденційності.

2.2. Дезінформація зловмисника.

Весь цей комплекс дасть змогу сформувати систему захисту маркетингової інформації як програмно-апаратний комплекс, до складу якого варто залучити антиінсайдерну програму.

У теорії інформаційної безпеки захист інформації пов'язують із криптографією. Головними характеристиками є тільки її доступність і цілісність. Будь-який ресурс системи в разі дотримання прав доступу мав бути доступним в будь-який час, інакше – він ставав безкорисним.

Серед ключових напрямків захисту інформації в ІС є технічний захист інформації, який розбивається на два великих класи, а саме: системи захисту інформації від несанкціонованого доступу (НСД) і системи захисту інформації від витоку технічними каналами. Під НСД автори роботи [7] розуміють доступ до інформації, що порушує становлення в ІС політику розмежування доступу. Під технічними каналами розглядаються канали сторонніх електромагнітних випромінювань і наведень, акустичні канали, оптичні канали і інше.

Захист від НСД здійснюють у різних складових ІС: 1) прикладне і системне ПЗ; 2) апаратна частина серверів робочих станцій; 3) комунікаційне устаткування й канали зв'язку; 4) периметр ІС. Для захисту інформації на рівні прикладного і системного ПЗ використовують: 1) системи розмежування доступу до інформації; 2) системи ідентифікації й аутентифікації; 3) системи аудиту й моніторингу; 4) системи антивірусного захисту. Для захисту інформації на рівні апаратного забезпечення використовують: апаратні ключі, системи сигналізації, засоби блокування пристроїв і інтерфейсів вводу-виводу інформації.

У комунікаційних системах використовують такі засоби мережевого захисту інформації [7]:

- міжмережеві крани (Firewall), які управляють проходженням мережевого трафіка відповідно до правил безпеки;
- системи виявлення вторгнень (IDS – Intrusion Detection System), які здатні запобігати шкідливим діям, що дає змогу значно знизити час простою внаслідок атаки й витрати на підтримку працездатності мережі;
- засоби створення віртуальних приватних мереж (VPN – Virtual Private Network), які забезпечують прозоре для користувача з'єднання локальних мереж, зберігаючи при цьому конфіденційність і цілісність інформації шляхом її динамічного шифрування;

- засоби аналізу захищеності, які дають змогу запобігти можливим атакам на корпоративну мережу, оптимізувати витрати на захист інформації й контролювати поточний стан захищеності мережі.

Для захисту периметра ІС створюють системи охоронної й пожежної сигналізації, системи цифрового відео-спостереження, системи контролю й керування доступом.

Захист інформації від її витоку технічними каналами зв'язку можна забезпечити такими засобами й заходами [7]:

- використанням екранованого кабелю й прокладанням проводів і кабелів в екранованих конструкціях;
- установленням на лініях зв'язку високочастотних фільтрів;
- побудовою екранованих приміщень ("капсул");
- використанням екранованого устаткування;
- установленням активних систем зашумлення.

Вибір засобів захисту інформації в автоматизованій СЗІ – складне завдання, у вирішенні якого потрібно враховувати імовірності різних загроз інформації, вартість реалізації різних засобів захисту і наявність різних зацікавлених сторін. Сучасна наука має в своєму розпорядженні методи, що дають змогу вибрати таку сукупність засобів захисту, яка забезпечить максимізацію міри безпеки інформації за певних витрат або мінімізацію витрат за заданого рівня безпеки інформації.

Проте найпоширенішим захистом є розподіл доступу, за допомогою якого можна реалізувати такі функції:

- ідентифікацію користувачів персоналу і ресурсів системи;
- аутентифікацію;
- авторизацію (перевірку повноважень);
- дозвіл доступу і створення умов роботи в межах встановленого регламенту;
- реєстрацію звернень до ресурсів, що захищаються;
- реагування на спроби несанкціонованих дій.

Серед методів встановлення автентичності є метод паролів – рядок символів, який користувач повинен ввести в систему яким-небудь засобом (надрукувати, набрати на клавіатурі тощо).

На державному рівні питання захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах регулюють Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" [8], міжнародні угоди, інші нормативно-правові акти. Так, зазначений вище Закон України здійснює підтвердження відповідності та проведення державної експертизи засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи.

Розглянуті вище засоби, методи та напрямки захисту маркетингової інформації часто не досить ефективні. Тому для повного її захисту потрібно розробити систему заходів з формування ринку послуг із захисту маркетингової інформації в Україні, а саме:

- програму, яка б надала змогу мінімізувати ризики навмисного і випадкового витоку корпоративної інформації;

- під час збору і передачі суворо конфіденційних даних варто використовувати технологію шифрування Secure Sockets Layer для того, щоб прочитати інформацію не зміг ніхто, крім Вас;
- методичні підходи до організації моніторингу ринку послуг із захисту інформації для створення системи інформаційно-аналітичного забезпечення процесу розробки та прийняття науково-обґрунтованих управлінських рішень з метою розвитку ринку засобів захисту інформації та вдосконалення системи державного регулювання ринку;
- здійснювати політику запровадження у свідомість громадян інформації та культурних стандартів, певним чином орієнтувальних, і мотивувати їх діяльність, підтримувати традиційні духовні цінності;

Висновки та перспективи подальших досліджень

Отже, аналіз існуючих СЗІ засвідчив, що маркетингові системи повинні мати в своїй основі технічний та мережевий засоби захисту інформації, серед яких: система захисту від інсайдерів, охоронна та пожежна сигналізація, цифрове відео-спостереження, контроль й управління доступом до системи, які регулюють на законодавчому рівні як Закони України, так і міжнародні угоди. Такі засоби повинні забезпечувати ідентифікацію та аутентифікацію користувачів, розподіл повноважень доступу до системи, реєстрацію та облік спроб несанкціонованого доступу. Однією з найважливіших складників цього процесу має бути кваліфікований вибір засобів захисту інформації, який повинен починатися з визначення основних переліків загроз, вибору заходів щодо забезпечення цієї безпеки та існуючих засобів захисту, запровадження й тестування засобів захисту інформації.

Таким чином, побудова СЗІ – це складний і трудомісткий процес, що потребує застосування широкого спектру знань з інформаційної безпеки і є безумовною необхідністю сьогодення та гарантією високого рівня захищеності маркетингової інформації у майбутньому.

Зауважимо, що загальної теорії безпеки інформації досі не створено. Наявні підходи і засоби нерідко мають істотні вади і не досить надійні, тому перспективою подальших досліджень з цієї теми є удосконалення існуючих маркетингових СЗІ відповідно до розвитку новітніх інформаційних технологій.

Література

- 1. Глобальні інформаційні системи та технології: моделі ефективного аналізу, опрацювання та захисту даних :** монографія / В.В. Пасічник, П.І. Жежнич, Р.Б. Кравець, А.М. Пелешин, Д.О. Тарасов. – Львів : Вид-во НУ "Львівська політехніка", 2006. – 348 с.
- 2. Пінчук Н.С.** Інформаційні системи і технології в маркетингу : навч. посібн. / Н.С. Пінчук, Г.П. Галузинський, Н.С. Орленко. – К. : Вид-во КНЕУ, 1999. – 328 с.
- 3. Програми.** [Електронний ресурс]. – Доступний з <http://www.infobezpeka.com/products>.
- 4. Проблема безпеки** інформації в умовах становлення інформаційного суспільства / О. Снитнікова. [Електронний ресурс]. – Доступний з http://www.soippo.narod.ru/documents/konf_zhuk/snitnikova_zhuk.doc.
- 5. Вибір засобів** захисту інформації в інформаційній системі / Баглай А.В., Новіцький А.О., Захарова М.В. [Електронний ресурс]. – Доступний з http://www.rusnauka.com/11_NPRT_2007/Informatica/22338.doc.htm.
- 6. Захист від інсайдерів** – порожній звук або необхідність. [Електронний ресурс]. – Доступний з <http://www.infobezpeka.com/publications/?id=285>.
- 7. Технічні засоби** захисту інформації. [Електронний ресурс]. – Доступний з <http://www.ulussys.com/i/lng.ua/page.security>.

8. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" // Відомості Верховної Ради (ВВР), 1994. – № 31. – С. 286.

9. Захист від інсайдерів – порожній звук або необхідність. [Електронний ресурс]. – Доступний з <http://www.infobezpeka.com/publications/?id=285>.

Бублык М.И., Войтук И.С. Защита и безопасность маркетинговой информации

Исследована необходимость создания различных систем защиты с учетом особенностей и условий их функционирования. Рассмотрены основные средства, методы и направления защиты маркетинговой информации, а также освещено регулирование этого вопроса на государственном уровне. Предложена система мер по формированию рынка услуг по защите маркетинговой информации в Украине.

Ключевые слова: инсайдеры, Spector 360, технический и сетевую защиту информации, распределение доступа, метод паролей.

Bubluk M.I., Voytukh I.C. Protection and security of marketing information

The article explored the need for different protection systems with regard to the characteristics and conditions of their operation. The main tools and methods for the protection of marketing information, as well as highlights of that issue at the state level. The system measures the formation of market services to protect the marketing information in Ukraine.

Keywords: insiders, Spector 360, the technical and network information security, distribution, access, method generator.

УДК 064.94 + 674.047

Асист. І.М. Крошній – НЛТУ України, м. Львів

АНАЛІТИЧНИЙ РОЗРАХУНОК ВОЛОГІСНИХ ПОЛІВ І НАПРУЖЕНО-ДЕФОРМІВНОГО СТАНУ ВИСУШУВАНОЇ ДЕРЕВИНИ

Розглянуто розподіл вологісного поля та зумовлений ним напружено-деформівний стан циліндра, під дією зовнішнього середовища, відносна вологість якого залежить від часу. Методом лінеаризуючих параметрів з використанням перетворення Лапласа розв'язано нелінійну задачу вологопровідності. Методом простих ітерацій розв'язані зведена до інтегрального рівняння Вольтера другого роду квазістатична задача для пружної моделі і нестационарна задача для в'язкопружної моделі.

Вступ. Зменшення запасів лісових промислових порід зумовлює розширення сфери застосування і перероблення низькоякісної деревинної сировини, зокрема круглих сортиментів, які отримують у процесі рубань і лісосічних робіт. Тонкомірну деревину круглого перерізу використовують для виготовлення торцевих підставок щитового паркету, певних столярно-будівельних виробів. Гальмівним чинником використання круглої деревини є ускладнення технологічного процесу сушіння, оскільки анізотропія фізико-механічних властивостей у цьому випадку є значнішою, ніж для пиломатеріалів. Важливою проблемою у цьому аспекті є розрахунок та аналіз напружено-деформівного стану матеріалу, дослідження реологічних властивостей у різних вологісних умовах.

При цьому особливу цінність мають аналітичні розв'язки задач вологоперенесення. Вони зручні для числового аналізу та є корисними в побудові розв'язків задач оптимального за швидкодією керування процесами сушіння деревини.