УДК 347
DOI: 10.31891/2307-5740-2018-266-1-115-118

ГЕЙДАРОВА О. В.,
ПАЮК В. П.
Хмельницький національний університет

ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ В УПРАВЛІННІ ГОТЕЛЬНО-РЕСТОРАННИМ БІЗНЕСОМ

Розглянуто можливість захисту інформаційних систем управління готельно-ресторанним бізнесом в сучасних умовах. Запропоновано інформаційну технологію виявлення помилок у комп'ютерних системах та мережах. Обґрунтовано впровадження поетапного здійснення технічного захисту інформації з урахуванням динаміки зміни можливих загроз.

Ключові слова: готельно-ресторанний бізнес, інформаційні системи, мережі, технології, управління, комп'ютерні програми, програмне забезпечення, захист.

HEIDAROVA O.,
PAIUK V.
Khmelnytskyi National University

PROTECTION OF INFORMATION SYSTEMS AND TECHNOLOGIES IN MANAGEMENT HOTEL-RESTAURANT BUSINESS

Influence of information technologies on hotel management is enormous as it is directly connected with increase of efficiency of work of each manager separately, and hotel as a whole. They directly affect the competitiveness of today's market. The use of computer networks, the Internet and Internet technologies, automation software for all business processes of the hotel today is not just a matter of leadership and the creation of competitive advantages, but also the survival of the market in the near future. The possibility of protecting the information management systems of hotel and restaurant business in the present conditions is considered. The information technology of detection of errors in computer systems and networks is proposed. The introduction of a phased implementation of technical protection of the information based on the dynamics of change of possible threats has been grounded. The developed software allows you to perform error detection on the network based solely on observation of the network, providing the benefits of secrecy and diagnostics capabilities improve the reliability of identification, because the approach allows analysis of DNS-requests as individual computer systems and automated computer behaviour computer network.

Keywords: hotel and restaurant business, information systems, networks, technology, management, computer software, software, protection.

Вступ. Підприємствам готельно-ресторанного бізнесу доводиться функціонувати в умовах високої складності, невизначеності і динамічності навколишнього середовища. За рахунок інформатизації світового ринку суб'єкти господарювання мають доступ до будь-якої інформації, що створює конкуренцію у готельно-ресторанній сфері. У зв'язку з цим виникає потреба у створенні не тільки єдиного інформаційного простору, але й адекватного механізму організації інформаційної безпеки на підприємствах. Ця діяльність набуває особливої актуальності на сучасному етапі, коли поширюються різноманітні способи ворожого конкурентного впливу. Не менш важливим є забезпечення інформаційної безпеки на рівні країни.

Вплив інформаційних технологій на управління готелем величезний, оскільки прямо пов'язаний з підвищенням ефективності роботи як кожного менеджера окремо, так і готелю в цілому. Вони прямо впливають на конкурентоздатність на сьогоднішньому ринку. Використання комп'ютерних мереж, інтернету та інтернет-технологій, програмних продуктів наскрізної автоматизації всіх бізнес-процесів готелю сьогодні не просто питання лідерства і створення конкурентних переваг, але і виживання на ринку в найближчому майбутньому.

Інформаційно-технічна революція змінила характер і методи ведення бізнесу. Використання можливостей технічного обміну сьогодні дозволяє легше і швидше створювати і продавати пакети послуг споживачам, вирішувати завдання фінансово-операційного управління, маркетингового планування, підвищувати конкурентоздатність і кількість продажів.

Аналіз останніх досліджень. Питання про можливості сучасних інформаційних систем та технологій в готельному бізнесі розглядаються такими відомими українськими вченими, як Роглєв Х., Скопень М., Худо В., Кияниця А., Кабушкин Н., Агафонова Л. та іншими. Вивченням питання інформаційної безпеки займалися такі вчені, як С. Ф. Гуцу, Б. А. Кормич, А. І. Марущак, О. А. Сороківська

Виклад основного матеріалу. У сьогоднішніх економічних умовах жорстокої конкуренції та ринкової економіки жоден успішний гостинний комплекс не може повноцінно розвиватися та ефективно просуватися без сучасних автоматизованих інформаційних технологій.

Інформаційні технології готельного управління з'явилися у світовій готельній індустрії давно — біля двадцяти п'яти років тому і пройшли великий шлях розвитку. На українському ринку IT управління готелем присутні відносно недавно. Експерименти з впровадження даних систем в готелях України стали проводиться з середини 90-х років.

На сучасному етапі функціонування підприємств готельного бізнесу виникають об’єктивні фактори, що ускладнюють процеси прийняття управлінських рішень, в умовах прискореного темпу суспільно-політичного життя. Збільшується обсяг "фахової" інформації, яку слід опановувати й використовувати у повсякденній діяльності, бурхливо розвивається наука й техніка, що спонукає до впровадження більш продуктивних і якісно нових технологій, новітніх інформаційних технологій та надання широкого спектра послуг.

Усі економічно розвинуті країни світу використовують переваги інформаційних технологій у виробничій, комерційній та банківських сферах. Це пояснюється тим, що традиційні методи не дозволяють зорієнтуватись в сучасному інформаційному потоці і проаналізувати динамічні процеси економічної діяльності підприємства. Швидше за все розвиваються технології, по’вязані з глобальною комп’ютерною мережею Інтернет, що призвело до появи таких нових категорій, як електронна торгівля, електронний бізнес, електронний уряд та ін.

Для регулювання економічної безпеки на підприємстві створюється служба інформаційної безпеки, що має виявляти і наочно демонструвати власникам підприємства весь спектр загроз в інформаційній сфері. Завдання керівників служби переконати, що протистояти загрозам можна тільки на основі створення і упровадження ефективних систем захисту інформації.

Виділимо найпоширеніші види потенційних загроз безпеці діяльності підприємства у сфері інформаційних технологій [5]:

– відсутність регламентованого доступу до файлів даних;

– вільне втручання в програмне забезпечення;

– відсутність протоколювання змін у програмному забезпеченні;

– відсутність регламентації користувачів інформації;

– відсутність дублювання важливих документів на документальних носіях даних;

– часті удосконалення одного і того ж програмного забезпечення різними особами;

– відсутність схем інформаційного забезпечення рівнів управління;

– наявність непідзвітних посадових осіб у системі управління тощо.

Система захисту інформації в інформаційних системах підприємств повинна будуватися на засадах комплексності й адаптивності. Доцільно розробляти організаційну структуру і впроваджувати систему захисту інформації в інформаційних системах підприємств відповідно до рекомендацій міжнародних стандартів і чинного законодавства України. Такими стандартами є: ISO/IEC 27002 «Інформаційні технології. Методи захисту. Кодекс практики для управління інформаційною безпекою"; ISO/IEC 27003 «Інформаційні технології. Методи захисту. Керівництво з застосування системи менеджменту захисту інформації"; ISO/IEC 27004 «Інформаційні технології. Методи захисту. Вимірювання"; ISO/IEC 27005 «Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки"; ISO/IEC 27006 «Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікування систем управління інформаційною безпекою"; ISO/IEC 27011 «Інформаційні технології. Керівництво з управління інформаційною безпекою для телекомунікацій" [5].

Загрози інформаційній безпеці – це можливі дії або події, які можуть вести до порушень ІБ. Загроза розкриття інформаційних ресурсів полягає у тому, що дані, інформація і знання стають відомими тим, кому не слід цього знати. У межах нашої роботи під загрозою розкриття розумітимемо такий стан, коли отриманий несанкціонований доступ до ресурсів системи, при чому йдеться як про відкриті, такі і ті ресурси, які мають обмежений доступ. Ці ресурси мають передаватися один одному і зберігатися у єдиній інформаційній системі.

Загроза порушення цілісності інформаційних ресурсів полягає в умисному антропогенному впливі (модифікація, видалення, зниження) даних, які зберігаються в інформаційній системі суб'єкта управління, а також передаються від даної інформаційної системи до інших. Серйозною загрозою можуть бути програмні віруси. Водночас дотримання правил користування комп'ютерною технікою, а також наявність у штаті співробітників органу управління відповідного фахівця з даних питань значно полегшить розв'язання зазначених завдань.

Джерелами помилок у програмному забезпеченні (ПЗ) можуть бути:

- логічні помилки розробників програмного забезпечення;

- непередбачені ситуації, які проявляються під час модернізації, заміни чи додавання нових апаратних засобів, встановлення нових додатків, виходу на нові режими роботи ПЗ, появи раніше не зафіксованих нештатних ситуацій;

- віруси, якими інфіковані програми;

- спеціальні програмні компоненти, які передбачені розробниками ПЗ для різного роду цілей.

Віруси самі по собі також становлять небезпеку і можуть знаходити свій вияв у видаванні повідомлень на екран монітора; затиранні інформації на дисках; переміщенні фалів до інших папок; уповільненні роботи комп'ютера; зборі інформації про роботу організації тощо.

Зважаючи на компетенцію органів державного управління, на наш погляд, загрози атаки на їх інформаційні системи може здійснюватися з метою:

- встановлення доступу до інформації з обмеженим доступом;

- викрадення ключів, паролів, ідентифікаторів, списку користувачів;
- ініціалізації контрольованого алгоритму роботи комп'ютерної системи;
- приведення у непридатність частини або всієї системи органів державного управління.

Відповідно виділяють і види загроз. Через їх чисельність нами була зроблена спроба, з урахуванням існуючих напрацювань щодо питань класифікації загроз національній безпеці, виокремити загрози інформаційній безпеці (таблиця 1).

Таблиця 1

Види загроз інформаційної безпеки

Ознака	Види загроз
За джерелами походження:	Природного походження; техногенного походження; антропогенного походження
За ступенем гіпотетичної шкоди	Явні чи потенційні дії, які ускладнюють або унеможливлюють реалізацію національних інтересів в інформаційній сфері та створюють небезпеку для системи державного управління, життєзабезпечення її системостворюючих елементів; небезпека
За повторюваністю вчинення	Повторювані; продовжувані
За сферами походження	Екзогенні; ендогенні
За ймовірністю реалізації	Імовірні; неможливі; випадкові
За рівнем детермінізму	Закономірні; випадкові
За значенням	Допустимі; недопустимі
За структурою впливу	Системні; структурні; елементні
За характером реалізації	Реальні; потенційні; здійснені; уявні
За ставленням до них	Об'єктивні; суб'єктивні
За об'єктом впливу	На державу; на людину; на суспільство
За формами закріплення	Нормативні; ненормативні

З метою усунення недоліків інформаційних систем та технологій та підвищення достовірності виявлення помилок в корпоративних мережах було розроблено інформаційну технологію виявлення помилок на основі аналізу DNS-трафіка. Результати оцінки достовірності виявлення помилок програмним забезпеченням розробленої інформаційної технології в порівнянні з відомими антивірусними засобами представлено в табл. 2 [2].

Таблиця 2

Результати експериментальних досліджень: оцінка достовірності виявлення помилок розробленою інформаційною технологією в порівнянні з відомими антивірусними засобами

№ зп	Засіб антивірусного діагностування	Середня достовірність виявлення, %	Середнє значення помилки 1-го роду, %	Середнє значення помилки 2-го роду, %	Середня тривалість часу, затраченого на виявлення, хв.
1.	Розроблена ІТ	96,22	3,78	3,44	30
2.	Avast Endpoint Protection Suite	84,80	15,20	11,66	25
3.	Avira Small Business Security Suite	86,38	13,62	9,52	42
4.	Dr.Web CureNet!	86,18	13,82	10,28	38
5.	ESET Endpoint Security	86,92	13,08	7,48	24
6.	Kaspersky Endpoint Security	88,86	11,14	8,30	31
7.	McAfee Endpoint Protection Suite	85,92	14,08	9,24	33
8.	Microsoft System Center Endpoint Protection	78,58	21,42	3,94	21
9.	Panda Endpoint Protection	83,56	16,44	5,84	29

Результати проведених експериментальних досліджень показують, що рівень достовірності виявлення помилок під час застосування розробленого антивірусного засобу складає близько 96%, що на 8–22% вище в порівнянні з відомими програмними засобами. Застосування розробленого програмного засобу дозволяє досягти зниження рівня помилок другого роду до 4%, що на 13–70% нижче в порівнянні з відомими антивірусними програмними засобами.

Дослідження характеристик розробленої інформаційної технології надало можливість визначити загальну ефективність виявлення помилок в мережах. В ході проведених експериментів було отримано наступні показники:

- показник ефективності витрат часу $T_E = 0{,}997$;
- показник ефективності ресурсоспоживання $C_E = 0{,}954$;
- достовірність виявлення $D_E = 0{,}962$.

Таким чином, загальна ефективність роботи розробленого програмного засобу складає $E \approx 0{,}997 \times 0{,}954 \times 0{,}962 \approx 0{,}91$.

Висновки. В сучасних умовах інформаційна безпека є невід'ємною складовою системи економічної безпеки господарюючого суб'єкта. Своєю чергою, надійне забезпечення інформаційної безпеки є

неодмінною умовою переходу на модель стійкого розвитку не тільки окремого підприємства, але й національної економіки в цілому. Щоб зберегти бізнес, розвиватися і бути конкурентоспроможним, підприємствам необхідно створити ефективну систему управління інформаційною безпекою. Результати дослідження достовірності розробленої інформаційної технології виявлення помилок на основі аналізу DNS-трафіка показують, що використання розробленого програмного забезпечення дозволяє підвищити рівень достовірності виявлення помилок на 8–22% в порівнянні з відомими антивірусними програмними засобами.

Література

1. Гейдарова О.В. Інформаційні технології у формуванні ефективних комунікаційних мереж підприємницьких структур / О.В. Гейдарова // Сборник научных статей Международной научно-практичной конференции "Информационные технологии в системе подготовки и повышения квалификации специалистов в области образовательного менеджмента". – Хмельницкий : ТРИАДА, 2011. – С. 278–282.

2. Гейдарова О.В. Інформаційні технології у моделюванні процесів прийняття рішень на підприємстві / О.В. Гейдарова, В.П. Паюк // Вісник Хмельницького національного університету. – Хмельницький : ХНУ, 2018. – С. 228–230.

3. Рудий Т. Засади захисту інформації в інформаційних системах підприємств / Т.В. Рудий, Л.М. Романевич, О.І. Руда // Актуальні проблеми економіки. – 2014. – № 2 (152). – С. 551–557.

4. Савенко О.С. Інформаційна технологія виявлення бот-мереж на основі аналізу DNS-трафіка / О.С. Савенко, С.М. Лисенко, К.Ю. Бобровнікова // Радіоелектронні і комп'ютерні системи. – 2016. – № 5 (79). – С. 38–42.

5. Северина С.В. Інформаційна безпека та методи захисту інформації / С.В. Северина // Вісник Запорізького національного університету. – 2016. – № 1 (29). – С. 155–161.

6. Черевко О.В. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системи інформаційного захисту [Електронний ресурс] / О.В. Черевко // Ефективна економіка. – 2014. – № 5. – Режим доступу : http://www.economy.nayka.com.ua/?op=1&z=3304.

References

1. Heidarova O.V. Informatsiini tekhnolohii u formuvanni efektyvnykh komunikatsiinykh merezh pidpryiemnytskykh struktur / O.V. Heidarova // Sbornyk nauchnykh statei Mezhdunarodnoi nauchno-praktychnoi konferentsyy "Ynformatsyonnыe tekhnolohyy v systeme podhotovky y povyshenyia kvalyfykatsyy spetsyalystov v oblasty obrazovatelnoho menedzhmenta. – Khmelnytskyi : TRYADA, 2011. – S. 278–282.

2. Heidarova O.V. Informatsiini tekhnolohii u modeliuvanni protsesiv pryiniattia rishen na pidpryiemstvi / O.V. Heidarova, V.P. Paiuk // Herald of Khmelnytskyi national University. – Khmelnytskyi : KhNU, 2018. – S. 228–230.

3. Rudyi T. Zasady zakhystu informatsii v informatsiinykh systemakh pidpryiemstv / T.V. Rudyi, L.M. Romanevych, O.I. Ruda // Aktualni problemy ekonomiky. – 2014. – № 2 (152). – S. 551–557.

4. Savenko O.S. Informatsiina tekhnolohiia vyiavlennia bot-merezh na osnovi analizu DNS-trafika / O.S. Savenko, S.M. Lysenko, K.Iu. Bobrovnikova // Radioelektronni i kompiuterni systemy. – 2016. – № 5 (79). – S. 38–42.

5. Severyna S.V. Informatsiina bezpeka ta metody zakhystu informatsii / S.V. Severyna // Visnyk Zaporizkoho natsionalnoho universytetu. – 2016. – № 1 (29). – S. 155–161.

6. Cherevko O.V. Teoretychni zasady poniattia informatsiinoi bezpeky ta klasyfikatsiia zahroz systemy informatsiinoho zakhystu [Elektronnyi resurs] / O.V. Cherevko // Efektyvna ekonomika. – 2014. – № 5. – Rezhym dostupu : http://www.economy.nayka.com.ua/?op=1&z=3304.

Рецензія/Peer review : 19.12.2018 Надрукована/Printed : 01.02.2019
Прорецензовано редакційною колегією