

Інформаційна безпека в готельно-ресторанному господарстві

Гоблик-Маркович Н.М.

кандидат економічних наук, доцент,
доцент кафедри готельно-ресторанної справи
Мукачівського державного університету

Молнар Д.І.

кандидат хімічних наук, доцент,
доцент кафедри готельно-ресторанної справи
Мукачівського державного університету

Ільтьо Т.І.

старший викладач кафедри готельно-ресторанної справи
Мукачівського державного університету

У статті розкрито актуальне питання забезпечення інформаційної безпеки на підприємствах готельно-ресторанного господарства. Зокрема, виділено джерела інформаційних загроз, обґрунтовано, що безпека готельно-ресторанних підприємств забезпечує стабільність їх функціонування, стійкий розвиток і здатність протистояти небезпеці та перешкодам у досягненні бізнесових цілей, ефективність інформаційної діяльності та особисту безпеку персоналу й клієнтів. На теоретичному рівні визначено зміст поняття інформаційна безпека підприємства готельно-ресторанного господарства. Проаналізовано джерела загроз інформаційній безпеці на підприємствах готельно-ресторанного господарства, наведено класифікацію основних видів інформаційних загроз, виділено підсистеми ефективного захисту інформації на підприємствах. Досліджено, що процес забезпечення безпеки підприємства є трудомістким і потребує значних матеріальних, інформаційних, фінансових ресурсів, що є об'єктами інформаційної безпеки підприємства. На практиці підприємства готельно-ресторанного господарства зіштовхуються з низкою проблем при забезпеченні інформаційної безпеки. Використання інформаційних технологій в підприємницькій діяльності значно підвищує ефективність процесів, зменшує затрати на їх проведення, проте в той же час зумовлює виникнення нових загроз для функціонування підприємства. Тому, за результатами проведеного дослідження визначено, що необхідним є створення системи аналізу можливих інформаційних загроз, розробка методики оцінки інформаційних ризиків, вживання заходів для забезпечення економічного захисту інформаційної безпеки, адже інформаційна безпека фактично відображається у ступені захищеності важливої для підприємства інформації від впливу дій випадкового або навмисного характеру, які можуть завдати збитків підприємству. Доведено, що підприємствам необхідно завчасно виявляти проблеми та вживати заходи, що спрямовані на запобігання загроз інформаційній безпеці в готельно-ресторанному господарстві. Проведений нами аналіз підходів до оцінки процесу забезпечення безпеки дав можливість виявити, що нині актуальною є проблема подальшого пошуку комплексних складових підвищення рівня безпеки підприємств готельно-ресторанного господарства, що може стати предметом подальших досліджень.

Ключові слова: безпека підприємства, інформаційна безпека, інформаційні загрози, інформаційні небезпеки, інформаційні системи.

Гоблик-Маркович Н.М., Молнар Д.І., Ільтьо Т.І. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ГОСТИНИЧНО-РЕСТОРАННОМ ХОЗЯЙСТВЕ

В статье раскрыто актуальный вопрос обеспечения информационной безопасности на предприятиях гостинично-ресторанного хозяйства. В частности, выделены источники информационных угроз, обосновано, что безопасность гостинично-ресторанного предприятия обеспечивает стабильность их функционирования, устойчивое развитие и способность противостоять опасности та препятствиям в достижении бизнесовых целей, эффективность информационной деятельности и личную безопасность персонала и клиентов. На теоретическом уровне определено содержание понятия информационная безопасность предприятий гостинично-ресторанного хозяйства. Проанализированы источники угроз информационной безопасности на предприятиях гостинично-ресторанного хозяйства, приведена классификация основных видов информационных угроз, выделены подсистемы эффективной защиты информации на предприятиях. Исследовано, что процесс обеспечения безопасности предприятий является трудоемким и требует значительных материальных, информационных, финансовых ресурсов, что является объектами информационной безопасности предприятия. На практике предприятия гостинично-ресторанного хозяйства сталкиваются с рядом проблем при обеспечения информационной безопасности. Использование информационных технологий в предпринимательской деятельности

значительно повышает эффективность процессов, уменьшает затраты на их проведение, однако в то же время обуславливает возникновение новых угроз для функционирования предприятия. Поэтому, по результатам проведенного исследования определено, что необходимым является создание системы анализа возможных информационных угроз, разработка методик оценки информационных рисков, принятие мер для обеспечения экономической защиты информационной безопасности, ведь информационная безопасность фактически отражается в степени защищенности важной для предприятия информации от воздействия действий случайного или умышленного характера, которые могут нанести ущерб предприятию. Доказано, что предприятиям необходимо заранее выявлять проблемы та принимать меры, что направлены на препятствия угроз информационной безопасности в гостинично-ресторанном хозяйстве. Проведенный нами анализ подходов к оценке процесса обеспечения безопасности дал возможность обнаружить, что на данное время актуальной является проблема дальнейшего поиска комплексных составляющих повышения уровня безопасности предприятий гостинично-ресторанного хозяйства, что может стать предметом дальнейших исследований.

Ключевые слова: безопасность предприятия, информационная безопасность, информационные угрозы, информационные опасности, информационные системы.

Goblik-Markovich N.M., Molnar D.I., Iltlo T.I. INFORMATION SECURITY IN THE HOTEL AND RESTAURANT BUSINESS

In article disclosed topical issues saving information security on hotel and restaurant domestic economy. In particular, identified the source of information threats soundly that security hotel and restaurant enterprises provides stability their functioning, sustainable development and ability confront danger and business obstacles in achieving objectives, efficiency of information activities ta personal safety personnel and clients. On theoretical level concepts information identified contents security company of hotel and restaurant domestic economy. Sources of information security threats to enterprises of hotel and restaurant business, the classification of basic types of information threats are highlighted subsystem effective information security in enterprises. We have studied the process providing security of company is consuming and require considerable, information, financial resources that are objective information security confirmation. On practice hotel and restaurant business face a number of problems with providing information security. Use of information technology in business processes increases efficiency, reduces the cost of their conduct, but at the same time lead to the emergence of new threats to the functioning of the company. Therefore, the results of the study identified that necessary is the creation of analysis possible information threats, development of methodology for assessing information risks, measures to ensure the economic protection of information security because information security is actually reflected in the degree of protection is important for enterprise information on the impact of actions accidental or intentional nature that can cause damage to the company. Proved that confirmation necessary to detect problems beforehand and take measures that directed on prevent threats information security of a hotel and restaurant business. We conducted determination approaches to safety assessment process provision of opportunity to discover that today is problem further comprehensive search components increase of safety level business hotel and and restaurant domestic economy that can stat further subject of research.

Keywords: security enterprise information security, information threats, information security, information systems.

Постановка проблеми в загальному вигляді. В наш час інформація, як і будь-який інший ресурс, потребує захисту. Для суспільства вона є стратегічним ресурсом, який сприяє подальшому розвитку самого суспільства.

Щодо інформаційної безпеки у готельно-ресторанному господарстві, то до цього питання потрібно поставитись серйозно, оскільки воно є досить таки значущим. Оскільки готельне господарство є однією із високорентабельних галузей нашої країни, важливо забезпечити високий рівень безпеки, в тому числі і інформаційної, задля стабільності функціонування закладів готельно-ресторанного господарства, ефективності економічної діяльності закладів та особистої безпеки персоналу та клієнтів.

Аналіз останніх досліджень і публікацій.

Суттєвий доробок у вивченні питання безпеки в готельно-ресторанному бізнесі зробили провідні вітчизняні та зарубіжні науковці, серед яких: З. Варналій, В. Микитенко, С. Покропив-

ний, А. Соснін, Н. Стельмащук, Н. Внукова, М. Єрмошенко, Є. Картузов, Н. Іванченко, В. Лугова та ін. Проте більшість науковців зовсім не приділяють увагу існуванню проблем з безпеки готельно-ресторанного господарства та шляхів забезпечення нею.

Формулювання цілей статті (постанова завдання). Метою дослідження за таких умов є обґрунтування основ щодо забезпечення безпеки закладів готельно-ресторанного бізнесу, аналіз наявних; викриття небезпек і вивчення ризиків, що негативно впливають на захищеність суб'єктів господарювання та споживачів.

Виклад основного матеріалу дослідження. Готельно-ресторанне господарство є однією із найважливіших ланок, що формує туристичний продукт на світовому ринку туристичних послуг. Зовнішнє середовище має прямий та опосередкований вплив на готельно-ресторанний бізнес, що в свою чергу створює ризики. Будь який заклад готельно-

ресторанного господарства відчуває ризики, в основному виробничі, комерційні, посередницькі, відповідно до видів діяльності. Фактор ризику змушує керівників готельно-ресторанних підприємств економити фінансові та матеріальні ресурси, розраховувати ефективність нових проектів, комерційних угод. Він визначає небезпеку втрати ресурсів або недоотримання доходів у порівнянні з раціональним використанням ресурсів.

Для будь-якого готелю чи ресторану безпека клієнтів є найважливішим аспектом його діяльності, яку повинні гарантувати, як ресторатори, так і готельєри.

У своєму виданні Іванченко Н.О. зазначила, що одним із актуальних питань безпеки підприємства готельного бізнесу є інформаційна безпека готелю, оскільки будь-яка цілеспрямована й недружня акція проти інтересів підприємства починається зі збору інформації. У зв'язку з погіршенням таких складових інформаційних ресурсів, як конфіденційність, цілісність, доступність і достовірність, спостерігаються збої у функціонуванні систем управління, розголошуються відомості, що становлять комерційну таємницю, порушується достовірність фінансової документації [1, с. 126].

Аналізуючи це джерело, можна виділити наступні інформаційні загрози:

- програмні (сюди відносять різноманітні комп'ютерні віруси, кіберзлочинність);
- технічні (можливе перехоплення інформації, придушення радіосигналу);
- фізичне (безпосереднє знищення засобів обробки та носіїв інформації (флеш-карти, диски));
- режимні (несанкціонований доступ до інформаційних ресурсів, незаконне копіювання даних, спотворення або ж приховування інформації, тощо).

Можна виділити цілу низку джерел загроз інформаційній безпеці сучасного підприємства:

- наявність агентурних джерел у закладах готельного господарства, які мають можливість отримання конфіденційної інформації;
- підкуп осіб, які працюють у готелі;
- перехоплення інформації, несанкціонований доступ до інформації і навмисні програмно-математичні дії на неї в процесі обробки і зберігання;
- підслуховування конфіденційних переговорів, які ведуться в службових приміщеннях готелю;
- необережне поводження з інформацією, проводячи переговори між готелем та фірмами, чи то вітчизняними, чи іноземними;

– працівники готелю, які готові «підзаробити», здаючи своє підприємство.

Серйозну загрозу інформаційній безпеці становлять також злочинні дії, спрямовані на розкрадання, привласнення, підміну, підключення, ламання (знищення), диверсію. Залежно від цього основні типи злочинних загроз інформації можна класифікувати в такий спосіб:

- до оброблення інформації та без доступу зловмисника до елементів інформаційної системи (підслуховування розмов; використання оптичних, візуальних чи акустичних засобів);
- у процесі оброблення інформації та без доступу зловмисника до елементів інформаційної системи (електромагнітні випромінювання; зовнішнє електромагнітне випромінювання; підключення реєструючої апаратури);
- до оброблення інформації з доступом зловмисника до елементів інформаційної системи, але без зміни останніх (копіювання магнітних чи інших носіїв, вихідних чи інших документів; крадіжка виробничих відходів);
- у процесі оброблення з доступом зловмисника до елементів інформаційної системи, але без зміни останніх (копіювання інформації у процесі оброблення; маскування під зареєстрованого користувача; використання недоліків мов програмування, програмних пасток, недоліків операційних систем та вірусів);
- до оброблення інформації з доступом зловмисника до елементів інформаційної системи зі зміною останніх (підміна машинних носіїв, вихідних документів, апаратури, елементів програм, елементів баз даних, розкрадання носіїв і документів; включення в програми «троянських коней», «бомб» тощо; читання залишкової інформації після виконання санкціонованих запитів);
- у процесі оброблення з доступом зловмисника до елементів інформаційної системи зі зміною останніх;
- незаконне підключення до апаратури і ліній зв'язку, зняття інформації на шинах живлення [2, ст. 168].

Кіберзлочинність у сфері готельного господарства повинна стояти на одному із перших місць загроз інформаційній безпеці. Кількість кіберзлочинів в Україні за останні два роки збільшилася більш ніж на тисячу випадків.

Як наголошується, в 2014 році управління по боротьбі з кіберзлочинністю МВС зареєструвало 4800 злочинів у сфері ІТ, в 2015 році – 6025 [3].

Підприємствам готельної індустрії доводиться працювати з даними банківських кар-

ток та іншою конфіденційною інформацією своїх клієнтів, тому цей вид бізнесу є одним із найбільш вразливих до погроз витоку даних та троянських атак.

В інформаційних системах готельного бізнесу обробляються конфіденційні дані клієнтів і співробітників, у т. ч. поштові адреси, номери контактних телефонів, адреси електронної пошти, дані кредитних і дебетових карт.

Відтак готельний сектор залишається одним із найбільш бажаних та цікавих «приманок» для кіберзлочинців, адже на нього припадає близько 15% від загальної кількості випадків витоку даних. Існує цілий ряд різновидів шахрайства, з якими стикається готельна індустрія. Як правило, ці шахрайства здійснюються через Інтернет або електронну пошту. Шахрайство із кредитними картками – один з найпоширеніших видів злочинів, з яким стикаються підприємства, що обробляють фінансові дані клієнтів.

Існують випадки недбалості співробітників, коли виникає несанкціонований доступ до конфіденційної інформації, стається крадіжка ноутбука, тощо. У разі виникнення кібератаки, для готельного підприємства не виключеним буде різке зниження доходів компанії, юридичні наслідки, погіршення іміджу бренда.

Відзначимо, що на сьогодні більшість керівників підприємств готельного сектора розуміє важливість підтримки високого рівня інформаційної безпеки. Зі зростанням рівня кіберзлочинності ступінь цієї поінформованості також зростає, і керівники готельних компаній почали з більшою відповідальністю ставитись до забезпечення інформаційної безпеки як одного з головних завдань.

Ресторанний бізнес в наш час займає досить високий щабель в сфері обслуговування. Як і в готельному господарстві, так і в ресторанному, важливим є збереження інформаційної безпеки на належному рівні.

З точки зору інформаційної безпеки критичні ризики ресторанного бізнесу виглядають наступним чином:

- можливість вилучення інформації при веденні управлінського обліку;
- несумлінність співробітників;
- можливість проникнення сторонніх осіб [4].

Подвійна бухгалтерія – поширене явище для ресторанного бізнесу. Безліч спеціалістів рекомендують організувати захищене шифрування сховища бухгалтерської інформації. Більш радикальним засобом захисту може стати система екстреного знищення даних. У першому випадку, навіть при фізичному

вилучення носіїв цих даних, бухгалтерія буде недоступна без наявності спеціальних ключів дешифрування. Друге рішення дозволяє миттєво знищити всю інформацію на носії без можливості відновлення, що може заподіяти певні незручності для власника цієї інформації, але повністю убезпечить його від загрози вилучення.

Сучасне підприємство повинне вміти належним чином будувати політику інформаційної безпеки, тобто розробляти і ефективно впроваджувати комплекс превентивних заходів по захисту конфіденційних даних та інформаційних процесів. Така політика передбачає відповідні вимоги для персоналу, менеджерів і технічних служб [5].

Головними етапами побудови політики інформаційної безпеки є:

- 1) реєстрація всіх ресурсів, які мають бути захищені;
- 2) аналіз та створення переліку можливих загроз для кожного ресурсу;
- 3) оцінка ймовірності появи кожної загрози;
- 4) вжиття заходів, які дозволяють економічно ефективно захистити інформаційну систему [6].

Більшість фахівців у галузі захисту інформації вважають, що інформаційна безпека підтримується на належному рівні, якщо для всіх інформаційних ресурсів системи підтримується відповідний рівень конфіденційності (неможливості несанкціонованого отримання будь-якої інформації), цілісності (неможливості навмисної або випадкової її модифікації) і доступності (можливості оперативно отримати запитувану інформацію).

Об'єктом інформаційної безпеки готельного чи ресторанного закладу є вся система його повноцінного функціонування. Вразивши хоча б один із об'єктів безпеки підприємства (економічної, кадрової, екологічної), остання зазнає відповідного впливу на окрему ділянку фірми, що може обернутися небезпекою або загрозою втрати балансу рівноваги виробничо-господарського механізму підприємства [7].

На сьогодні безліч спеціалізованих компаній пропонують великий вибір засобів захисту інформаційних систем, враховуючи їх вартісні показники та функціональні можливості. При побудові політики інформаційної безпеки варто звернути увагу, в першу чергу, на розмір готельно-ресторанного підприємства, його ресурсні та фінансові можливості, поточний рівень інформаційної безпеки, стадію функціонування фірми.

Висновки з цього дослідження. Результати цього дослідження дають змогу стверджувати, що інформаційна безпека в готельно-ресторанному бізнесі в наш час потребує пильного нагляду та захисту.

Однією з найнеобхідніших умов ефективності діяльності готельного підприємства є безперебійна робота в сфері підтримки інформаційної безпеки на належному рівні.

Отже, для забезпечення інформаційної безпеки в готельно-ресторанних підприємства необхідно:

- аналізувати та створювати перелік можливих загроз;
- проводити оцінку появи ймовірних загроз;
- розробляти методики оцінки інформаційних ризиків;
- проводити інформаційні обстеження ресурсів підприємства;
- розробляти політику та концепції інформаційної безпеки;
- вживати заходи, які дозволяють економічно ефективно захистити інформаційну систему.

ЛІТЕРАТУРА:

1. Іванченко Н.О. Інформаційна складова економічної безпеки підприємства та її значення для забезпечення стійкого розвитку національної економіки /Н.О. Іванченко // Стратегія розвитку України. – 2011. – № 3. – С. 124–128.
2. Економічна безпека: [навч. посібник] / О.Є. Користін, О.І. Барановський, Л.В. Герасименко та ін.; за ред. О.М. Джужі. – К.: Алерта; Центр учбової літератури, 2010. – 368 С.
3. Економічна правда [Електронний ресурс]. – Режим доступу: <http://www.epravda.com.ua/news/2016/03/28/587044/>
4. Системна інтеграція. Консалтинг. [Електронний ресурс]. – Режим доступу: <http://efsol.ru/articles/safety-restaurant-business.html>
5. Власова Л.А. Защита информации / Л.А. Власова. – Хабаровск: РИЦ ХГАЭП, 2007. – 84 с.
6. Батюк А.Є. Інформаційні системи в менеджменті / А.Є. Батюк, З.П. Дзуліт, К.М. Обельовська, І.М. Огороднік, Л.П. Фабрі. – Львів: «Інтелект-Захід», 2004. – С. 343–384.
7. Гоблик-Маркович Н.М., Ільтьо Т.І. Забезпечення економічної безпеки на підприємствах ресторанного господарства [Електронний ресурс] / Електронне фахове видання. Економіка та суспільство. – МДУ – 2016. Вип.6 – Режим доступу: <http://economyandsociety.in.ua/journal-6/13-stati-6/426-goblik-markovich-n-m-ilto-t-i>
8. Стройко Т.В. Неприбуткові організації в системі світових соціально-економічних процесів: [монографія] / [Т.В. Стройко, І.О. Іртицева, М.І. Стегней та ін.]. – Херсон: Гельветика, 2014. – 172 с.