Список використаних джерел

1. Про електронні документи та електронний документообіг : Закон України : прийнятий ВР України 22 травня 2003 р. // Відомості Верховної Ради України. – 2015. – № 36. – С. 275–276.
2. Борисова О. В. Тенденції розвитку готельно-ресторанного бізнесу в Україні / О. Б. Борисова // Економічна стратегія і перспективи розвитку сфери торгівлі та послуг. – 2012. – Вип. 1 (2). – С. 331–338.
3. Нечаюк Л. Готельно-ресторанний бізнес: менеджмент : навч. посіб. для. студ. вищ. навч. закл. / Л. Нечаюк, Н. Телеш. – Київ : Центр навч. л-ри, 2013. – 346 с.
4. Худолій Л. М. Управління якістю як один із головних важелів конкурентоздатності готелю / Л. М. Худолій, Г. Б. Мунін // Формування ринкових відносин в Україні : зб. наук. пр. – Київ : Обрій, 2012. – № 17. – С. 147–151.
5. Актуальні питання документознавства та інформаційної діяльності: теорії та інновації : зб. матеріалів ІІ Міжнар. наук.-практ. конф., Одеса, 24–25 березня 2016 р. – Дніпропетровськ : ПП Середняк Т. К., 2016. – 526 с.

УДК 023

ОРГАНІЗАЦІЯ І ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПІДПРИЄМСТВА

О. І. Яременко, *магістр спеціальності Інформаційна, бібліотечна та архівна справа освітня програма «Документознавство та інформаційна діяльність»*
Л. М. Колєчкіна, *д. ф.-м. н., професор – науковий керівник*

Анотація. Слід зазначити, що на сьогодні становлення ефективної державної влади є пріоритетним напрямом в загальній стратегії розвитку України, водночас інформаційне забезпечення підприємства є його основою і має розглядатися як один з основних напрямів вдосконалення. Більш того, аналіз спеціальної літератури, а також масивів практичної інформації дає змогу говорити про відсутність єдиної концепції підходу до інформаційного забезпечення системи підприємства. Частими залишаються випадки неефективного використання сил і засобів безпеки підприємства в процесі забезпечення їх інформаційної безпеки.

В роботі розглядаються основні аспекти визначення поняття інформаційної безпеки та інформаційного захисту підприємства,

а також описано методи та засоби забезпечення інформаційної безпеки підприємства, та шляхи її вдосконалення.

Abstract. It should be noted that today the formation of an effective state power is a priority direction in the overall strategy of Ukraine's development, while information provision of the enterprise is its basis and should be considered as one of the main areas of improvement. Moreover, the analysis of special literature, as well as arrays of practical information, makes it possible to speak of the lack of a unified concept of approach to information provision of the enterprise system. Incomplete cases of inefficient use of forces and security of the enterprise in the process of ensuring their information security.

The paper considers the main aspects of defining the notion of information security and information protection of the enterprise, as well as describes the methods and means of ensuring information security of the enterprise, and ways of its improvement.

Ключові слова: інформацій, інформаційна безпека, забезпечення інформаційної безпеки

Постановка проблеми. Питання забезпечення інформаційної безпеки сьогодні для України стоять на одному рівні із захистом суверенітету і територіальної цілісності, забезпеченням її економічної безпеки. Рівень інформаційної безпеки активно впливає на стан політичної, економічної, оборонної та інших складових національної безпеки України, бо найчастіше реалізація інформаційних загроз – це нанесення шкоди в політичній, військовій, економічній, соціальній, екологічній сферах тощо.

В сучасних ринкових умовах господарювання інформаційна безпека в умовах глобального інформаційного суспільства відіграє провідну роль. Широка інформатизація всіх сфер життя суспільства, зокрема сфери забезпечення безпеки особи, суспільства, економіки і фінансів, державної інфраструктури, ставить питання про комплексний підхід до проблеми інформаційної безпеки.

Отже, проблема організації захисту підприємства на сьогодні є важливою складової в діяльності будь-якого підприємства.

Аналіз основних досліджень і публікацій. Інформаційна безпека є складовою загальної проблеми інформаційного забезпечення функціонування системи органів виконавчої влади, підприємств, організацій та установ. В різних літературних

джерелах інформаційна безпека інтерпретується трохи по різному, але суть її залишається та сама. Наприклад, О. Г. Додонов визначає інформаційну безпеку як стан захищеності інформаційного простору, що забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави [1]. Б. М. Кормич та І. М. Панарін визначають інформаційну безпеку як це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства і держави [1–6].

У науковій літературі досліджені поняття інформаційного забезпечення безпеки підприємства, серед найбільш значущих розробок варто назвати праці Ю. А. Фісун, В. К. Гасеський, В. А. Авраменко, Р. Л. Калюжний [1–4] тощо.

Формулювання мети. Метою дослідження є вивчення сутності інформаційної безпеки підприємства, та визначення шляхів вдосконалення забезпечення захисту інформації.

Виклад основного матеріалу дослідження. Аналізові змісту поняття «інформаційна безпека» зазвичай дослідниками приділяється значна увага, у той час як такі поняття, як небезпека і загроза розглядаються дещо спрощено і здебільшого у звуженому плані, відірваному від контексту поняття «інформаційна безпека».

Необхідність у розробленні поняття «загроза» визначається:

1) відсутністю єдиного підходу до дослідження основних понять інформаційної безпеки;

2) недостатньою розробленістю родового поняття «загроза» і питань його відмежування від інших споріднених понять, таких, як «небезпека», «виклик», «ризик», і відповідно видового «інформаційна загроза» і його відмежування від таких понять, як «інформаційна війна», «інформаційне протиборство», «інформаційний тероризм»;

3) наявністю невирішеної проблеми формування категорійно-понятійного апарату теорії інформаційної безпеки;

4) можливістю на підставі теоретичних розробок даного апарату формувати адекватну систему моніторингу та управління загрозами та небезпеками в інформаційній сфері [6].

Найбільш широко загрози інформаційним ресурсам можна розглядати як потенційно можливі випадки природного, технічного або антропогенного характеру, які можуть спричинити

небажаний вплив на інформаційну систему, а також на інформацію, яка зберігається в ній. Виникнення загрози, тобто віднаходження джерела актуалізації певних подій у загрози характеризується таким елементом, як уразливість. Саме за наявності вразливості як певної характеристики системи і відбувається активізація загроз. Безперечно, що самі загрози за своєю суттю відповідно до теорії множин є не вичерпними, а отже і не можуть бути піддані повному описові.

Інтегруючи різноманітні підходи, а також пропозиції щодо розв'язання даного питання, вважаємо, що можна виділити такі види загроз інформаційній безпеці: розкриття інформаційних ресурсів; порушення їх цілісності; збій в роботі самого обладнання.

Розглянемо більш детально кожну загрозу інформаційній безпеці.

Загроза розкриття інформаційних ресурсів полягає утому, 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.

Захист інформації – сукупність засобів, методів, організаційних заходів щодо попередження можливих випадкових або навмисних впливів природного чи штучного характеру, наслідком яких може бути нанесення збитків чи шкоди власникам інформації або її користувачам, інформаційному простору. Суттю захисту інформації є її доступність при збереженні цілісності інформації та гарантованій конфіденційності.

Діяльність із забезпечення інформаційної безпеки здійснюється за допомогою різних способів, засобів і прийомів, які у сукупності й складають методи. Метод передбачає певну послідовність дій на підставі конкретного плану. Методи можуть значно змінюватися і варіюватися в залежності від типу діяль-

ності, в якій вони використовуються, а також сфери застосування.

Важливими методами аналізу стану забезпечення інформаційної безпеки є методи описи і класифікації. Для здійснення ефективного захисту системи управління НБ слід, по-перше, описати, а лише потім класифікувати різні види загроз та небезпек, ризиків та викликів і відповідно сформулювати систему заходів по здійсненню управління ними.

У якості розповсюджених методів аналізу рівня забезпечення інформаційної безпеки використовуються методи дослідження при чинних зв'язків. За допомогою даних методів виявляються причинні зв'язки між загрозами та небезпеками; здійснюється пошук причин, які стали джерелом і спричинили актуалізацію тих чи інших чинників небезпеки, а також розробляються заходи по їх нейтралізації. У числі даних методів причинних зв'язків можна назвати наступні: метод схожості, метод розбіжності, метод сполучення схожості і розбіжності, метод супроводжувальних змін, метод залишків.

Вибір методів аналізу стану забезпечення інформаційної безпеки залежить від конкретного рівня і сфери організації захисту. В залежності від загрози уможливлюється завдання щодо диференціації як різних рівнів загроз, так і різних рівнів захисту. Що стосується сфери інформаційної безпеки, то у ній зазвичай виділяють:

1) фізичний;
2) програмно-технічний;
3) управлінський;
4) технологічний;
5) рівень користувача;
6) мережевий;
7) процедурний[7].

В нинішніх умовах для підприємств дуже важливим є захист електронної корпоративної інформації. Безпека електронної системи – це здатність її протидіяти спробам завдати збитків власникам і користувачам систем у разі появи різних збуджувальних (навмисних і ненавмисних) впливів на неї.

Ефективність захисту систем за допомогою будь-яких криптографічних алгоритмів значною мірою залежить від безпечного розподілу ключів. Тут можна виділити такі основні методи розподілу ключів між учасниками системи.

Метод базових/сеансових ключів – метод описаний у стандарті ISO 8532 і використовується для розподілу ключів симетричних алгоритмів шифрування; 2) метод відкритих ключів – метод описаний у стандарті і може бути використаний для розподілу ключів як для симетричного, так і для асиметричного шифрування. За його допомогою можна також забезпечити надійне функціонування центрів сертифікації ключів для електронного цифрового підпису на базі асиметричних алгоритмів та розподіл сертифікатів відкритих ключів учасників інформаційних систем. Використання методу відкритих ключів дає можливість кожне повідомлення шифрувати окремим ключем симетричного алгоритму та передавати цей ключ із самим повідомленням у зашифрованій асиметричним алгоритмом формі [6].

Висновки. Отже, захист інформації на підприємстві є доцільним здійснювати в наступних напрямах:

– комплексним застосуванням різних засобів і методів;

– створенням структури захисту й охорони з кількома рівнями;

– постійним їх удосконаленням.

Успіх справи залежить від збалансованої й налагодженої взаємодії захисту операційних систем і гарантування безпеки баз даних.

Список використаних джерел

1. Бибик С. Ділові документи та правові папери: листи, протоколи, заяви, договори угоди / Бибик С. – Харків : Фолио, 2005. – 491 с.
2. Зубок М. І. Інформаційна безпека / Зубок М. І. – Київ : КНТЕУ, 2005. – 93 с.
3. Зубок М. І. Правове регулювання безпеки підприємницької діяльності / Зубок М. І. – Київ : КНТЕУ, 2005. – 76 с.
4. Інформаційне законодавство : зб. законодавчих актів / ред. Ю. С. Шемшученко, К. С. Чиж. – Київ : Юридична думка, 2005. – Т. 5: Міжнародно-правові акти в інформаційній сфері. – 328 с.
5. Карпенко О. О. Сучасне діловодство : навч. посіб. / О. О. Карпенко, М. М. Матліна. – Харків : Нац. аерокосм. ун-т «Харк. авіац. ін-т», 2009. – 75 с.
6. Коваленко Ю. О. Забезпечення інформаційної безпеки на підприємстві [Електронний ресурс] / Ю. О. Коваленко. – Електронні дані. – Режим доступу:

http://www.econindustry.org/arhiv/html/2010/st_51_18.pdf. – Назва з екрана. – Дата звернення: 13.10.2018.
7. Коваленко Ю. О. Організація систем інформаційної безпеки підприємств [Електронний ресурс] / Ю. О. Коваленко. – Електронні дані. – Режим доступу: http://fullref.ru/job_05dc6b4cd1d240ca816e0bf9a1e0c2d4.html. – Назва з екрана. – Дата звернення: 15.10.2018.

Заочна форма навчання

УДК 023

ІНФОРМАЦІЙНА ПІДТРИМКА РЕКЛАМНИХ КОМПАНІЙ ТОВАРІВ ПІДПРИЄМСТВА

В. Р. Деркач, *магістр спеціальності Інформаційна, бібліотечна та архівна справа освітня програма «Документознавство та інформаційна діяльність»*
Л. М. Колєчкіна, *д. ф.-м. н., професор – науковий керівник*

Анотація. Сучасний етап розвитку нашої країни відрізняється динамізмом і змінами у всіх сферах громадського життя. Процес відновлення торкнув усі без винятку політичні, економічні та соціальні інститути. У період коли багато виробничих підприємств, об'єднань, концернів та інших організацій стали незалежними, нормальне їхнє функціонування в цих економічних умовах практично неможливе без добре організованої комплексної маркетингової діяльності. Реклама продукції і діяльності підприємства – це найважливіша складова частина комплексу маркетингових заходів, своєрідний вихід на споживача.

В роботі розглядаються основні аспекти визначення поняття реклами та її види, а також описано способи інформаційної підтримки реклами, та шляхи вдосконалення рекламних продуктів для підприємства.

Abstract. The present stage of development of our country is characterized by dynamism and changes in all spheres of public life. The process of restoration has touched all without exception political, economic and social institutions. During the period when many manufacturing enterprises, associations, concerns and other organizations became independent, their normal functioning under these economic conditions is practically impossible without a well-organized integrated marketing activity. Advertising of products and