3. Бебик В. Інформаційно-комунікаційний менеджмент у глобальному суспільстві: психологія, технології, техніка паблікрилейшнз : моногр. / В. Бебик. – Київ : МАУП, 2015. – 440 с.
4. Круковський М. Ю. Критерії ефективності системного електронного документообороту [Електронний ресурс] / М. Ю. Круковський. – Режим доступу: http://conf.atsukr.org.ua/conf_files/conf_dir_1/krukovskyi_sppr05.pdf (дата звернення: 01.10.19). – Назва з екрана.
5. Мокра М. Інформаційно-комунікаційне середовище в освітній системі США [Електронний ресурс] / М. Мокра. – Режим доступу: http://ena.lp.edu.ua/bitstream/ntb/23849/1/28-213 (дата звернення: 01.10.19). Назва з екрана.
6. Солдаткін В. І. Інформаційно-освітнє середовище відкритої освіти [Електронний ресурс] / В. І. Солдаткін. – Режим доступу: http://www.ict.edu.ru/vconf/php?avconf&cgetFormrthesis Desc&d=light&id_thesis1929 (дата звернення: 01.10.19). – Назва з екрана.

УДК 023

ОРГАНІЗАЦІЯ ТА УПРАВЛІННЯ СЛУЖБОЮ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

А. В. Бурдун, *магістр спеціальності 029 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 системи захисту є пріоритетним напрямом в загальній стратегії розвитку будь-якого підприємства. 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.

Ключові слова: інформація, інформаційна безпека, забезпечення безпеки підприємства

Abstract. It should be noted that today the establishment of an effective protection system is a priority in the overall strategy of development of any enterprise. The analysis of the specialized literature, as well as the arrays of practical information, makes it possible to speak about the lack of a unified concept of approach to information support of the enterprise system. Often, cases of inefficient use of forces and security of the enterprise in the process of ensuring their information security.

The paper deals with the main aspects of defining the concept of information security and information security of the enterprise, as well as describes methods and means of ensuring information security of the enterprise, and ways to improve it.

Keywords: information, information security, enterprise security

Постановка проблеми. Питання забезпечення інформаційної безпеки на підприємствах сьогодні є досить актуальним і наболівшим. 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 дже-

релах інформаційна безпека інтерпретується трохи по різному, але суть її залишається та сама.

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

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 [1–5].

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 [5].

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.

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.

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.

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 [5].

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; 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 [5].

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 інформаційних джерел

1. Бибик С. Ділові документи та правові папери: Листи, протоколи, заяви, договори угоди / С. Бибик. – Харків : Фолио, 2005. – 491 с.
2. Зубок М. І. Правове регулювання безпеки підприємницької діяльності / М. І. Зубок. – Київ : КНТЕУ, 2005. – 76 с.
3. Інформаційне законодавство: збірник законодавчих актів / ред. Ю. С. Шемшученко, К. С. Чиж. – Т. 5: Міжнародно-правові акти в інформаційній сфері. – Київ : Юридична думка, 2005. – 328 с.

4. 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.
5. Коваленко Ю. О. Забезпечення інформаційної безпеки на підприємстві [Електронний ресурс] / Ю. О. Коваленко. – Режим доступу: http://www.econindustry.org/arhiv/html/2010/st_51_18.pdf (дата звернення: 10.10.2019). – Назва з екрана.

УДК 023

ІНФОРМАЦІЙНІ МОДЕЛІ ДІЯЛЬНОСТІ КОМЕРЦІЙНОГО ПІДПРИЄМСТВА

Н. В. Зубань, *магістр спеціальності 029 Інформаційна, бібліотечна та архівна справа освітня програма «Документознавство та інформаційна діяльність»*
Л. М. Колєчкіна, *д. ф.-м. н., професор – науковий керівник*

Анотація. Комерція – це діяльність по забезпеченню купівлі-продажу товарів, що супроводжується проведенням відповідних розрахунків, з метою здобуття максимально можливого прибутку в умовах існуючих правових норм. Комерційне підприємство – це підприємство, яке здійснює операції та угоди з купівлі-продажу або перепродажу товарів. Основна функція – доведення товару до споживача. Інформаційна модель комерційного підприємства є схемою потоків інформації, використовуваної в процесі управління,відображає різні процедури виконання функції управління підприємством і представляє за кожним завданням зв'язок вхідних і вихідних документів і показників. Комерційне підприємництво отримало найбільший розвиток в Україні в перші роки переходу до ринку. Воно стало стрімко розвиватися, в основному як приватне, індивідуальне підприємництво. Даний вид діяльності приваблює доволі швидкою віддачею і відносно високою прибутковістю, яка досягає 20–30 %, а іноді й більше.

Ключові слова: комерція, комерційне підприємство, інформаційна модель комерційного підприємства.

Abstract. Commerce is the activity of ensuring the sale and purchase of goods, which is accompanied by the carrying out of