УДК 023

# УПРАВЛІННЯ ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОСТІ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

***І. А. Пухай,*** *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.** В процесі своєї діяльності будь-яке підприємство оперує інформацією як специфічним товаром високої цінності. Володіння інформацією, її оптимальне використання забезпечує ефективне функціонування суб'єкта господарювання як цілісного комплексу. Тому проблема забезпечення інформаційної безпеки є надзвичайно актуальною на сучасному етапі розвитку інформаційних технологій, який супроводжується введенням інформаційних систем у всі сфери діяльності людини, постійною взаємодією підприємств на теренах саме інформаційного простору.

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.** In the course of its activity, any enterprise operates information as a specific high value commodity. Possession of information, its optimal use ensures the effective functioning of the entity as a whole complex. Therefore, the problem of information security is extremely relevant at the current stage of information technology development, which is accompanied by the introduction of information systems in all spheres of human activity, constant interaction of enterprises in the territory of the information space itself.

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.** Захист інформації – є практичною реалізацією комплексної програми (концепції) інформаційної безпеки установи і являє собою жорстко регламентований і динамічний технологічний процес, що попереджає порушення доступності, цілісності, достовірності та конфіденційності цінних інформаційних ресурсів і в кінцевому рахунку забезпечує досить надійну безпеку інформації в процесі управлінської та виробничої діяльності установи. В даному випадку безпека розцінюється як реального результат, досягнутий за рахунок функціонування обраної системи захисту інформації. Передбачається, що захист конфіденціальної інформації здійснюється від різного виду загроз безпеки інформації, і насамперед несанкціонованого доступу до неї зловмисника [1]. Захисту підлягає будь документована інформація, неправомірне поводження з якою може завдати шкоди її власнику, власнику, користувачеві або іншій особі. Захисту потребує не тільки конфіденційний документ. Часто звичайний відкритий правовий акт важливо зберегти в цілісності та безпеці від викрадача чи стихійного лиха.

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 [1–4].

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.

**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».

Аналіз наукової думки та емпіричного матеріалу дає змогу визначити такі принципові положення організації захисту інформації в умовах інформатизації у контексті інформаційної безпеки (рис. 1.)

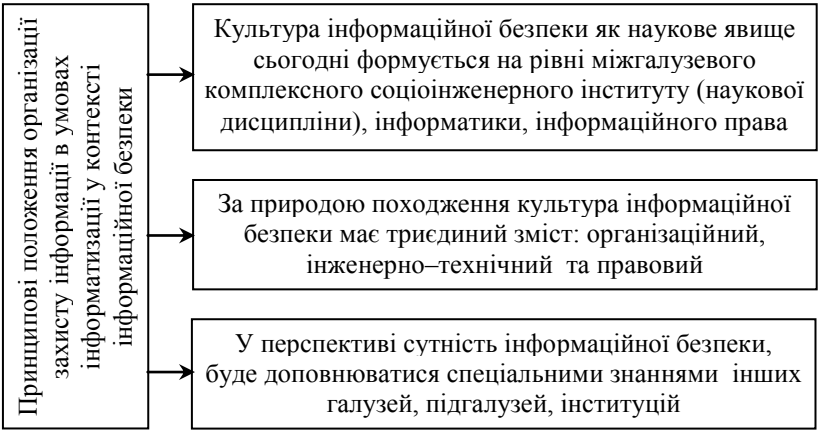


Рисунок 1 – Принципові положення організації захисту інформації в умовах інформатизації у контексті інформаційної безпеки [складено автором]

З погляду теорії організації і теорії систем, у науковому синтезі їх – теорії організації систем управління – формування цілеспрямованих, керованих систем (у тому числі будь-яких

практичних заходів) передбачає визначення елементів системи та осмислення проблематики предметної галузі (її природу) в цілому.

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: 1) метод базових 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 [4].

**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. Зубок М. І. Правове регулювання безпеки підприємницької діяльності / М. І. Зубок. – Київ : КНТЕУ, 2005. – 76 с.
2. 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.
3. 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.
4. 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: 05.10.2019). – Назва з екрана.



УДК 351.746:007


## БЕЗПЕКА ДОКУМЕНТНО-ІНФОРМАЦІЙНОЇ СИСТЕМИ УСТАНОВИ


***І. О. Славко,*** *магістр спеціальності 029 Інформаційна, бібліотечна та архівна справа освітня програма «Документознавство та інформаційна діяльність»*
***М. В. Макарова,*** *д. е. н., професор – науковий керівник*



**Анотація.** Розглянуто поняття інформаційної безпеки, її базові рівні. Зазначено відповідність завдань інформаційної безпеки установи Доктрині інформаційної безпеки України. Означено