

2. Податковий кодекс України: Закон України № 609-VIII від 15.07.2015. Відомості Верховної Ради України. 2020.

3. Податковий кодекс України: Закон України № 466-IX від 16.01.2020. Відомості Верховної Ради України. 2020.

**Ольга Микитишин**

*студентка магістратури юридичного факультету  
Західноукраїнського національного університету*

**Роман Мельник**

*викладач кафедри кримінального права і процесу,  
економічної безпеки та правоохоронної діяльності  
Західноукраїнського національного університету*

## **ОСНОВИ ФОРМУВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА**

Визначення сучасного розуміння інформаційної безпеки, її значення для реалізації основних бізнес-процесів. Аналіз напрацювань вітчизняних та зарубіжних науковців надав змогу визначити, що найбільш розповсюдженим є визначення інформаційної безпеки як певного рівня захищеності інформації від незаконного ознайомлення, перетворення і знищення, а також захищеність інформаційних ресурсів від впливів, спрямованих на порушення їх працездатності. Природа цих впливів може бути найрізноманітнішою. Це і спроби проникнення зловмисників, і помилки персоналу, і вихід з ладу апаратних і програмних засобів, стихійні лиха тощо [2, с.165]. Інша група науковців, з точки зору бізнесу, під інформаційною безпекою підприємства розуміють стан захищеності інтересів (цілей) організації в умовах загроз в інформаційній сфері. На їх думку, інформаційна сфера є сукупністю інформації, інформаційної інфраструктури, суб'єктів, які здійснюють збір, формування, розповсюдження, зберігання і використання інформації, а також системи регулювання виникаючих при цьому відносин. Відповідно до вищезазначених підходів, відповідь на питання про роль інформаційної безпеки в бізнесі сучасної організації є очевидною, оскільки підприємства розглядали її як «звичайну страховку» від проблем і неприємностей: «...заплатив гроші, впровадив рішення і можеш спокійно зосередитися на основній

діяльності...» [З., с. 31]. Однак розвиток ринку, інформатизація сфер діяльності суб'єктів господарювання, зростання кількості загроз і засобів забезпечення безпеки призводить до принципово іншого розуміння ролі інформаційної безпеки. В умовах глобальної інформатизації її не можна сприймати виключно як захист або «страховку» – вона переростає в більше, а саме – в один з ключових бізнес-активів сучасної організації.

З одного боку, необхідність підвищення ефективності системи інформаційної безпеки пов'язана із загостренням проблем захисту інформації. Тут можна згадати, по-перше, зростаючу потребу забезпечення конфіденційності даних. Вітчизняні підприємства, слідом за своїми західними колегами, приходять до необхідності враховувати так звані репутаційні ризики, відповідальність за забезпечення конфіденційності даних своїх клієнтів, субпідрядників, партнерів. Разом з тим, на більшості підприємств організаційна складова системи інформаційної безпеки опрацьована слабо.

Наприклад, дані як такі часто не класифіковані, тобто компанія не має чіткого уявлення про те, які у неї є типи даних з позицій їх конфіденційності, критичності для бізнесу. А це тягне за собою цілий ряд проблем, починаючи від складнощів в обґрунтуванні адекватності заходів щодо захисту інформації та закінчуючи неможливістю при виникненні інциденту використовувати правові методи їх розслідування.

Створення реально, а не формально діючої системи інформаційної безпеки можливо лише при забезпеченні узгодженості між правовими, організаційними, технологічними, технічними та економічними факторами забезпечення необхідного рівня інформаційної безпеки.

Висока ефективність системи інформаційної безпеки може бути досягнута, якщо всі її компоненти представлені якісними рішеннями, функціонують як єдиний комплекс і мають централізоване управління. Система безпеки повинна будуватися на основі аналізу ризиків, і вартість її впровадження і підтримки повинна бути адекватною існуючим загрозам, тобто економічно обґрунтованою.

Розглянуті підходи до визначення інформаційної безпеки, визначені драйвери формування системи інформаційної безпеки підприємства та модель інформаційного протидіючого обумовлюють доцільність формування системи менеджменту інформаційної безпеки на основі ризик-орієнтованого підходу, який ґрунтується на припущенні того, що оцінка ризику робить можливим вирішення питань, пов'язаних з інформаційними активами організації: актуальні

загрози і їх джерела – фактори ризику; можливість і періодичність виникнення загроз; визначення інформаційних активів (їх кількісний аналіз), які можуть підлягати впливу при виникненні загрози [1, с. 133]. Аналіз напрацювань в даній сфері дозволив визначити, що стандартній системі управління інформаційною безпекою підприємства притаманні всі загальні для систем менеджменту елементи.

Таким чином управління інформаційною безпекою є невід’ємною частиною корпоративного управління підприємством, що мають як загальні фактори: об’єкти, предмети, зв’язки, так і відмінності. Досвід, накопичений в останні десятиліття, переконує в необхідності застосування міжнародних модельних стандартів формування системи менеджменту інформаційної безпеки вітчизняного підприємства, що має базуватися на ризик-орієнтованому підході управління інформаційними технологіями. Проте, на практиці реалізація політики інформаційної безпеки суб’єктів господарювання ускладнюється пошуком компромісу між відповідністю, зручністю і безпекою. Тому наступним напрямом дослідження стане аналіз методичних підходів до визначення рівня інформаційної безпеки підприємства.

### **Перелік використаних джерел**

1. Андрианов В. В. Обеспечение информационной безопасности бизнеса / В. В. Андрианов, С. Л. Зефирова, В. Б. Голованов, Н. А. Голдуев. – М. : ООО «Альпина», 2010 – 265 с.
2. Аникин И.В. Теория информационной безопасности и методология защиты информации [Текст] / И.В. Аникин, В.И. Глова, Л.И. Нейман, А.Н. Нигматуллина. — Казань: Изд-во Казан. гос. техн. ун-та, 2008. — 358 с.
3. Тарасова О.В. Корпоративна культура як інструмент ефективного менеджменту підприємства. *Економіка харчової промисловості*. — 2013. — № 3(19). — С. 28–32.
4. Романова Ю.Д. Інформаційні технології в менеджменті (управлінні): підручник і практикум для академічного бакалаврату / під заг. ред. Д.Ю. Романової. — М: Видавництво Юрайт, 2015. — 478 с.