державної політики у сфері природних монополій" від 19.08.1997 р., № 853/97 // Урядовий кур'єр. -28.08.1997.

**ВИШНЬОВСЬКИЙ Сергій**
слухач магістратури за спеціальністю
«Адміністративний менеджмент»
(науковий керівник: к.е.н., доцент кафедри державного і муніципального управління Богач Ю. А.)

## УДОСКОНАЛЕННЯ МОДЕРНІЗАЦІЇ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПІДПРИЄМСТВА

Впровадження сучасних інформаційно-комунікативних технологій в процеси модернізації інформаційного забезпечення підприємства передбачає розробку системи заходів, спрямованих на підготовку до модернізації інформаційної інфраструктури, удосконалення різних сегментів інформаційної інфраструктури, створення інтегрованої інформаційної інфраструктури.

Головними функціональними компонентами інтегрованої інформаційної інфраструктури мають стати:

- інтегроване телекомунікаційне середовище (усі види й типи мереж);
- правова й економічна інфраструктура, що забезпечує стійкий розвиток інформаційних технологій та інформаційних ресурсів;
- система інформаційної безпеки.

Важливим функціональним компонентом інформаційної інфраструктури підприємства э інформаційна безпека. Це пов'язано з тим, що багато найважливіших інтересів підприємства в даний час значною мірою визначається станом навколишнього інформаційного середовища. Цілеспрямовані або ненавмисні впливи на інформаційну сферу з боку зовнішніх або внутрішніх джерел можуть завдавати серйозної шкоди цим інтересам і становлять загрози та ризики для безпеки. Тому інформаційна безпека в сучасних умовах є однією з необхідних умов нормального функціонування підприємства.

Поняття інформаційної безпеки можна розглядати у декількох

ракурсах. По-перше, це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання й розвиток в інтересах громадян, організацій, держави. По-друге, це стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їх існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз. Стан інформованості визначає ступінь адекватності сприйняття суб'єктами дійсності і, як наслідок – обґрунтованість подальших рішень і дій [1].

Погіршення на підприємстві таких параметрів інформації, як конфіденційність, цілісність, доступність, вірогідність тощо, може призвести до таких негативних наслідків: збоїв у функціонуванні систем управління технологічними процесами й іншими критичними системами; розголошення відомостей, що становлять комерційну й інші види таємниць; порушення вірогідності фінансової документації; несанкціонованого доступу до персональних даних фізичних осіб тощо.

Результатом усього наведеного вище може стати: погіршення ділових відносин із партнерами; зриви переговорів, втрата вигідних контрактів; невиконання договірних зобов'язань; необхідність проведення додаткових ринкових досліджень; відмова від рішень, що стали неефективними через розповсюдження інформації, і, як наслідок, – фінансові втрати, пов'язані з новими розробками; втрата можливості запатентувати результат науково-технічної діяльності або продати ліцензію; зниження цін або обсягів реалізації; втрати ділової репутації; більш жорсткі умови одержання кредитів; труднощі в постачанні і придбанні устаткування тощо.

Формування сучасної ефективної системи інформаційної безпеки підприємства вимагає створення відповідних структурних підрозділів інформаційної безпеки і покладення на них системи функцій і завдань.

Функціональне навантаження служби інформаційної безпеки підприємства повинно охоплювати такі напрями:

– розробка методології та методик аналізу загроз, оцінки рівня інформаційної безпеки підприємства і системи її забезпечення;

– організація і здійснення конкретних видів діяльності із захисту інформації;

– експлуатація технічних засобів захисту інформації;

– аудит і контроль функціонування системи інформаційної безпеки підприємства.

З огляду на складний характер питань, що входять у блок інформаційної безпеки підприємства, деякі з зазначених функцій можуть виконуватися тільки разом з іншими структурними підрозділами і службами підприємства (службою по роботі з персоналом, юридичною, господарською службою тощо). Вітчизняна і зарубіжна практика використання різних організаційних схем функціонування підрозділів, що відповідають за інформаційну безпеку підприємства (функції такого підрозділу можуть покладатися на системних адміністраторів; цей підрозділ може знаходитися у структурі служби інформаційної безпеки, що підпорядковується вищому керівництву), свідчить, що найкращим є варіант, при якому підрозділ інформаційної безпеки входить до складу служби економічної безпеки підприємства. Підтримуючи цей варіант, акцентуємо, що саме в цьому випадку створюються найкращі можливості розв'язання проблем інформаційної безпеки в контексті загальних завдань безпеки бізнесу підприємства.

*Література:*

1. Коваленко Ю.О. Забезпечення інформаційної безпеки на підприємстві [Електронний ресурс] Режим доступу: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/econpr_2010_3_20.pdf

**ГАНУСЕВИЧ Андрій**
слухач магістратури за спеціальністю
«Адміністративний менеджмент»
(науковий керівник: к.е.н., доцент кафедри державного і муніципального управління Богач Ю. А.)

## ОРГАНІЗАЦІЯ АНАЛІТИЧНОЇ РОБОТИ В БАНКІВСЬКІЙ УСТАНОВІ

Ефективність функціонування банківської установи багато в чому залежить від обґрунтованості, своєчасності і доцільності прийнятих управлінських рішень. Останні, в свою чергу, приймаються на базі отриманої аналітичної інформації, яка максимально повинна відповідати