## Підсекція «Управління фінансово-економічною безпекою»

УДК 004.056.5

# ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА

Студ. О. Батечко, гр. МгУФБ-1-15
Наук. керівник доц. Н.В. Цимбаленко
Київський національний університет технологій та дизайну

В системі забезпечення безпеки все більшого значення набуває інформаційна безпека підприємства. Це пов'язано зі зростанням обсягу інформації, з необхідністю її зберігання, передачі і обробки. Обіг значної частини інформації в електронній формі, використання локальних і глобальних мереж створюють якісно нові загрози інформаційній безпеці підприємств.

Так, А. Сороковський визначає інформаційну безпеку підприємства як суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності. М. Танцюра характеризує інформаційну безпеку підприємства як збереження конфіденційності, цілісності та доступності інформації (доступність - це властивість бути досяжним і придатним до використання в інформаційному середовищі; цілісність - властивість захищеності точності і повноти даних; конфіденційність - властивість захищеності інформації від несанкціонованого використання). А. Марущак зазначає, що інформаційна безпека підприємства - це цілеспрямована діяльність його органів і посадових осіб з використанням дозволених методів і засобів по досягненню стану захищеності інформаційного середовища підприємства та забезпечення його нормального функціонування і динамічного розвитку. В цілому, можна зробити висновок, що пріоритетним напрямком в процесі забезпечення інформаційної безпеки підприємства є збереження в таємниці комерційно важливої інформації, що дозволяє успішно конкурувати на ринку товарів і послуг.

Досвід показує, що для боротьби з правопорушеннями у сфері обігу інформації на підприємстві необхідна цілеспрямована організація процесу захисту інформаційних ресурсів. Джерело цього виду загроз може бути внутрішнім (власні працівники), зовнішнім (наприклад, конкуренти) і змішаним (замовники - зовнішні, а виконавці – працівники).

Переважна більшість правопорушень у сфері обігу інформації здійснюються самими працівниками підприємства. Безпосереднім об'єктом таких правопорушень є інформація. Правопорушник отримує доступ до інформації, яка охороняється, без дозволу її власника або з порушенням встановленого порядку доступу. Способи неправомірного доступу до інформації можуть бути різними - крадіжка носія інформації, порушення засобів захисту інформації, використання чужого імені, зміна коду або адреси технічного пристрою, надання фіктивних документів на право доступу до інформації, установлення апаратури запису, що підключається до каналів передачі даних.

Всі загрози об'єктам інформаційної безпеки за способом впливу можуть бути об'єднані в п'ять груп: інформаційні, фізичні, організаційно-правові, програмно-математичні, радіоелектронні. Наслідки скоєних протиправних дій можуть бути різними: а) копіювання інформації; б) зміна змісту інформації; в) блокування інформації; г) знищення інформації без можливості її відновлення; д) порушення роботи комп'ютерної техніки, системи або мережі.

В цілому, різноманітність загроз інформаційній безпеці підприємства обумовлює необхідність застосування комплексного підходу до її забезпечення.