# НЕОБХІДНІСТЬ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ПІДПРИЄМСТВІ

**О.А. Журан**, *к.е.н., доцент*
**О.В. Бучка**

*Одеський національний політехнічний університет*

Підприємство – це інструмент задоволення потреб і досягнення певних цілей суспільства, соціальних груп та індивідів. Ефективна діяльність підприємства припускає, що вона забезпечує безпеку своїх членів, виступає засобом виживання людини, що діє в її рамках. У той же час саме підприємство піддається різноманітним небезпекам, що загрожували її існуванню і цілісності. Це обумовлює необхідність забезпечення діяльності по підвищенню захищеності життєво важливих інтересів підприємства та її членів.

Актуальність данної роботи полягає в тому, що в умовах економіки постіндустріального суспільства, інформація усіх напрямків діяльності підприємства, стає найбільш цінним і дорогим ресурсом.

Проблеми інформаційної безпеки у сучасному житті постають усе більш складними і практично значущими. Інформаційна безпека (ІБ) є однією із складових частин економічної безпеки, яка формує модель захищеності підприємства.

Необхідно відзначити роботи А. Баранова, К. Белякова, В. Брижко, І. Гаврилова, М. Гуцалюка, Л. Задорожної, О. Зінченко, Г. Лазарєва, Д. Ловцова, А. Марущака та ін., які розглядали питання забезпечення інформаційної безпеки.

ІБ підприємства включає сукупність напрямів, методів, засобів і заходів, що знижують вразливість інформації і перешкоджають несанкціонованому доступу до інформації, її розголошенню або витоку. Елементами цієї системи є: правовий, організаційний, інженерно-технічний захист інформації, а основною її характеристикою – комплексність. Структура системи, склад і зміст елементів, їх взаємозв'язок залежать від об'єму і цінності інформації, що захищається, характеру можливих загроз безпеки інформації, необхідної надійності захисту і вартості системи.

Необхідно підкреслити, що пріоритетним напрямком у 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 виконавець – працівник фірми). Як показує практика, переважна більшість таких правопорушень здійснюються самими працівниками підприємства.

Правопорушник отримує доступ до інформації, що охороняється, без дозволу її власника або з порушенням встановленого порядку доступу. Способи такого неправомірного доступу до комп'ютерної 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. Причому доступ може бути здійснений на території підприємства, де зберігаються носії, з комп'ютера на робочому місці, з локальної мережі, глобальної мережі [1]. Проблеми, пов'язані з інформаційною безпекою на підприємствах, можуть бути вирішені тільки за допомогою систематичного і комплексного підходу. З методологічної точки зору, підхід до проблем інформаційної безпеки починається з виявлення суб'єктів інформаційних відносин та інтересів цих суб'єктів.

Весь спектр інтересів суб'єктів, пов'язаних з використанням інформації, можна поділити на такі категорії: забезпечення доступності, цілісності і конфіденційності ресурсів інформаційного середовища.

Іноді в ряд основних складових інформаційної безпеки включають захист від несанкціонованого копіювання інформації, але як нам бачиться, це занадто специфічний аспект з сумнівними шансами на успіх, тому ми не станемо його виділяти.

Інформаційні системи створюються (купуються) для отримання певних інформаційних послуг. Якщо з тих чи інших причин надати ці послуги користувачам стає неможливо, це очевидно завдає шкоди всім суб'єктам інформаційних відносин. Тому, не протиставляючи доступність решті аспектам, прийнято виділяти її як найважливіший елемент інформаційної безпеки.

Значення кожної з складових інформаційної безпеки для різних категорій суб'єктів інформаційних відносин різному.

Для комерційних організацій провідну роль відіграє доступність інформації. Прикладом може бути і постачальник інтернет-послуг (безкоштовний поштовий сервер). Зазвичай для такої установи дуже важливо забезпечити можливість постійного доступу користувачів до сервісу (швидкість Інтернету для користувачів так само важлива).

Мета захисту інформації на об'єктах можуть бути досягнуті при проведенні робіт за такими напрямками:

– оцінка можливостей і ступеня небезпеки технічних засобів розвідки;

– виявлення можливих технічних каналів витоку інформації;

– аналіз можливостей і небезпеки несанкціонованого доступу до інформаційних об'єктів;

– розробка і реалізація організаційних, технічних, програмних та інших засобів і методів захисту інформації від усіх можливих загроз;

– створення комплексної системи захисту [2].

Можна зауважити, що підприємства розглядаються суб'єктами інформаційного права, а вивчення інформаційних правових відносин необхідно для правильного регулювання на підприємстві.

Захист інформаційних ресурсів підприємства є одним з ключових завданнях в умовах підвищення рівня внутрішніх за зовнішніх загроз. Щоб зберегти бізнес, розвіватися і буті конкурентоспроможними, підприємствам необхідно створити ефективну систему управління інформаційною безпеки.

**Список використаної літератури:**


1. Курушин В. Д. Компьютерные преступления и информационная безопасность / В.Д. Курушин, В.А. Минаев. - М.: Новый юрист. - 2012. - 256 с.
2. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи [Електронний ресурс] / Режим доступу: http: //nbuv.gov .ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf.