**Кирилюк Х. А.**, магістр гр. ФЕБ-11
*Науковий керівник*:
Карковська В. Я., к.е.н.
Національний університет
«Львівська політехніка»

# Сучасні заходи забезпечення безпеки інформаційних систем на базі міжнародних стандартів ISO

Розвиток інформаційних систем в сучасних умовах супроводжується все більшою кількістю загроз інформаційній безпеці підприємства. Взаємодія суспільних і приватних мереж, а також спільне використання інформаційних ресурсів збільшує труднощі управління доступом та забезпечення гарантій безпеки інформаційно-комунікаційних систем та мереж (ІКСМ).

Міжнародні стандарти ISO/IEC 17799, ISO 27001 є основоположними в сфері управління інформаційною безпекою. Вони представляють собою модель системи менеджменту, яка визначає загальну організацію процесів, класифікацію даних, системи доступу, напрямки планування, відповідальність співробітників, використання оцінки ризику і т. ін. в контексті інформаційної безпеки.

Під забезпеченням безпеки інформаційних мереж розуміють запобігання ушкодженню інформаційних активів і переривання дій, пов'язаних з реалізацією безперервного процесу бізнесу. Інформаційні ресурси та засоби обробки, поширення інформації повинні бути керовані й фізично захищені.

Важливим є на періодичній основі виконувати перегляд ризиків безпеки й реалізованих засобів управління з метою оцінки та введення змін, що стосуються вимог і пріоритетів бізнесу, урахування нових видів загроз й вразливостей системі та послугам, підтвердження, того, що засоби управління залишаються ефективними й відповідними.

Перегляд політики безпеки варто виконувати на різних рівнях управління підприємством залежно від результатів попередніх оцінок. Оцінки ризику спочатку виконують на загальному рівні для того, щоб визначити пріоритети вкладення ресурсів в області високого ризику, і потім на більше детальному рівні, щоб розглянути специфічні ризики самої системи та її послуг.

Після ідентифікації вимог безпеки, варто вибирати й застосовувати заходи управління, таким чином, щоб забезпечувати впевненість у зменшені ризиків. Засоби управління можуть бути обрані із стандартів або з інших документів та заходів управління визначених для даного класу систем, або можуть бути розроблені підприємством.

Заходи управління варто вибирати, ґрунтуючись на відношенні вартості реалізації послуг та впровадження систем безпеки й зниження ризиків та можливих втрат, якщо відбудеться порушення. Також варто брати до уваги не грошові фактори (втрата репутації, соціальні тощо).

Деякі із заходів управління в стандартах та нормативних документах, можуть розглядатися, як керівні принципи для управління інформаційною безпекою й бути застосовними для більшості організацій.

Заходи управління із законодавчої точки зору, які включають: захист даних і таємність особистої інформації; охорону інформаційних ресурсів організації; права на інтелектуальну власність.

Всі заходи управління в стандартах та нормативних документах є важливими та застосування яких повинно визначатися з врахуванням ризиків (рис. 1).

Критичними факторами, для успішної реалізації інформаційної безпеки в межах підприємства є політика безпеки (цілі й дії, якої враховують мету діяльності підприємства), підхід реалізації безпеки (відповідність культурі та внутрішній етиці підприємства), під-

тримка й зобов'язання з боку керівництва, правильне розуміння вимог безпеки, оцінки ризику й управління ризиком, ефективний маркетинг безпеки для всіх адміністраторів і службовців, розподіл повноважень керівництва між всіма службовцями й підрядниками, забезпечення відповідного стажування й навчання, всебічна й збалансована система виміру, що використається для оцінки ефективності управління інформаційною безпекою й пропозиції на покращення діяльності підприємства, в рамках зворотного зв'язку, спрямовані на поліпшення бізнесу, оцінка загроз інформації, а також імовірності їхнього виникнення, процес визначення управління ризиками.


*Рис.1 Заходи управління інформаційною безпекою*

Одними із головних напрямів забезпечення інформаційної безпеки ІКСМ повинна бути система правил управління доступом (рис.2). Права кожного користувача або групи користувачів, які повинні бути чітко визначені у політиці безпеки.

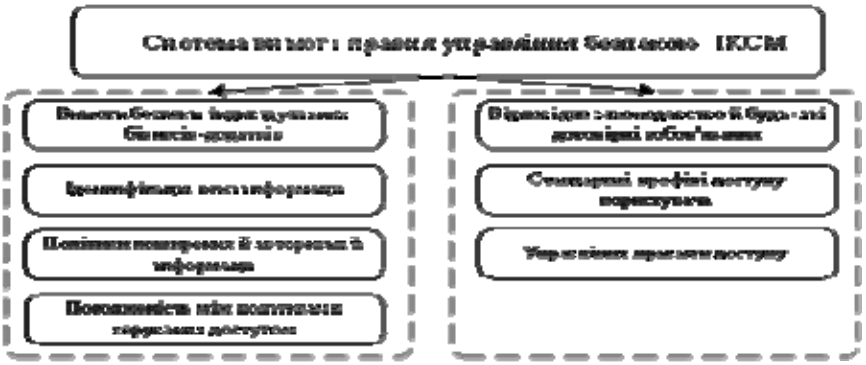

*Рис.2. Заходи управління безпекою ІКСМ*

Основна особливість заходів забезпечення та управління безпекою ІКСМ полягають у їх відповідності міжнародним стандартам та вимогам ISO.

Формулювання вимог для нових ІКСМ або вдосконалення існуючих повинні бути специфікованими в залежності від заходів забезпечення та системи управління безпекою. Застосування цих заходів полягає у комерційній цінності інформаційних ресурсів, а також з мінімізацією можливостей потенційних збитків бізнесу щодо відмови систем безпеки або її відсутності.

1. Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий: Учеб. пособие. — М.: МИФИ, 1995. — 252 с.
2. Галатенко В.С. Стандарты информационной безопасности. — М.: НИИСИ РАН, 2006. — 262 с.
3. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. — М.: Горячая линия — Телеком, 2000. — 452 с.
4. Петров В.А., Пискарев А.С., Шеин А.В. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах: Учеб. пособие. — М.: МИФИ, 1995. — 396 с.