УДК 004.45:005.74
Таран Д. – ст. гр. ПТс-38, Носуля О. – ст. гр. ТЗ-18
Харківський державний університет харчування та торгівлі

ІНФОРМАЦІЙНА БЕЗПЕКА ДЛЯ ПІДПРИЄМСТВ В УМОВАХ СУЧАСНИХ ТЕХНОЛОГІЙ

Науковий керівник: канд. техн. наук., доцент Сорокіна С.В.

Taran D., Nosulia O.
Kharkiv state University of food technology and trade

INFORMATION SECURITY FOR ENTERPRISES IN CONDITIONS OF MODERN ENGAGEMENT TECHNOLOGIES

Supervisor: PhD in Technical Sciences, Sorokina S.V.

Ключові слова: прикладні програми, інформаційна безпека
Keywords: software, information security

Винахід комп'ютера і подальший бурхливий розвиток інформаційних технологій в другій половині XX століття зробили проблему захисту інформації актуальної для усього суспільства.

Будь-яке сучасне підприємство незалежно від виду діяльності і форми власності не в змозі успішно розвиватися і вести господарську діяльність без створення в ньому умов для надійного функціонування системи захисту власної інформації. Відсутність у багатьох керівників підприємств і компаній чіткого представлення з питань захисту інформації призводить до того, що їм складно повною мірою оцінити необхідність створення надійної системи захисту інформації на своєму підприємстві і тим більше складно буває визначити конкретні дії, необхідні для захисту тих або інших конфіденційних відомостей.

Сучасні комп'ютерні системи, що використовують операційні системи (ОС) Windows, Windows NT, різні версії UNIX відносяться до частково контрольованих систем. Неприємною особливістю таких ОС є те, що повний перелік усіх їх можливостей повністю не відомий користувачеві. Резонно допустити наявність в цих ОС прихованих можливостей здійснення несанкціонованого доступу до інформації, що обробляється під їх управлінням. Побудова надійного захисту включає оцінку інформації яка є в комп'ютерній системі з метою уточнення міри її конфіденційності, аналізу потенційних погроз її безпеки і встановлення необхідного режиму її захисту.

Ефективність захисту інформації досягається не кількістю грошей, витрачених на її організацію, а здатністю її адекватно реагувати на усі спроби несанкціонованого доступу до інформації; заходи щодо захисту інформації від несанкціонованого доступу повинні носити комплексний характер, тобто об'єднувати різнорідні заходи протидії погрозам (правові, організаційні, програмно-технічні); основна загроза інформаційної безпеки комп'ютерних систем виходить безпосередньо від співробітників.

З урахуванням цього необхідно максимально обмежувати як круг співробітників, що допускаються до конфіденційної інформації, так і круг інформації, до якої вони допускаються (у тому числі і до інформації за системою захисту). При цьому кожен співробітник повинен мати мінімум повноважень по доступу до конфіденційної інформації.