СЕКЦІЯ 10
СУЧАСНІ СИСТЕМИ ЕКОНОМІЧНОЇ, ІНФОРМАЦІЙНОЇ ТА ФІНАНСОВОЇ БЕЗПЕКИ В УМОВАХ ГЛОБАЛІЗАЦІЇ

Ю.І. Кошлань, студентка, НТУ «ХПІ»
Є. М. Строков, ст. викл., НТУ «ХПІ»

НАПРЯМИ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ФУНКЦІОНУВАННЯ ТА ЗАХИСТУ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Сучасні тенденції розвитку соціально-економічних систем характеризуються постійним підвищенням ролі інформації, збільшенням її обсягів та якісних характеристик. Обробка та обмін цифровою інформацією отримує усе більш вагоме значення як у житті кожної людини, так і у функціонуванні державних і суспільних інститутів. Інформатизація веде до створення єдиного світового інформаційного простору, до уніфікації інформаційних технологій різних країн. Можна стверджувати, що промислове суспільство трансформується в інформаційне. На сьогодні вже сформувався новий вид трудової діяльності, пов'язаний із здобуттям, поширенням і зберіганням інформації.

Нові технології обіцяють грандіозні перспективи, але у той же час катастрофічно зростає ціна втрат в разі нештатного функціонування або зниження надійності систем обробки і передачі інформації. Підвищення значущості і цінності інформації вимагає відповідних заходів, щодо забезпечення її захисту.

Розвиток засобів, методів і форм автоматизації процесів зберігання і обробки інформації, масове застосування персональних комп'ютерів та збільшення кількості користувачів значно підвищують уразливість даних та інформаційних систем в цілому. Данні, що використовуються та зберігаються

можуть бути несанкціоновано змінені, викрадені або знищені.

Це пояснює постійну актуальність проблеми забезпечення інформаційної безпеки.

Під інформаційною безпекою слід розуміти захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятний збиток суб'єктам інформаційних відносин, у тому числі власникам і користувачам інформації і підтримуючої інфраструктури.

Ключовими моментами в цьому визначенні є те, що інформаційна безпека залежить не тільки від комп'ютерів, але і від підтримуючої інфраструктури, до якої можна віднести системи електро-, водо- і теплопостачання, кондиціонери, засоби комунікацій і, обслуговуючий персонал, а також виділення поняття «неприйнятний збиток». Застрахуватись від усіх видів збитків неможливо, тим більше неможливо зробити це економічно доцільним способом, коли вартість захисних засобів і заходів не перевищує розмір очікуваного збитку. Значить, з чимось доводиться миритися і захищатися слід тільки від того, з чим змиритися ніяк не можна, тобто поріг неприйнятності має матеріальне вираження, а метою захисту інформації стає зменшення розмірів збитку до допустимих значень.

На сьогодні виділяють три напрямки забезпечення захисту даних у інформаційних системах: адміністративно-законодавчий, процедурний (управління доступом), програмно-технічний.

До адміністративно-законодавчих засобів забезпечення інформаційної безпеки відносять законодавчі акти, які регламентують правила використання і обробки інформації обмеженого доступу і встановлюють міри відповідальності за порушення цих правил.

До процедурних засобів відносяться заходи безпеки, що орієнтовані на персонал. Наприклад, обмеження доступу до апаратури, носіїв інформації, встановлення різних рівнів доступу.

Програмно-технічні засоби забезпечення інформаційної безпеки – це найбільший та найширший напрям. До його складу відносяться як системи

відеоспостереження, так і програмні продукти криптографічного закриття інформації від несанкціонованого доступу.

Ефективна комплексна реалізація визначених трьох напрямків забезпечення інформаційної безпеки повинна протистояти всім можливим загрозам та забезпечити мінімізацію втрат.

Таким чином, можна зробити висновок, що визначення комплексу засобів захисту даних в інформаційній системі – складна оптимізаційна задача, при розв'язанні якої потрібно враховувати як потенційні можливості різноманітних загроз та вартість реалізації відповідних засобів захисту.

Список літератури: **1.** *Левін В.К.* Захист інформації в інформаційно-обчислювальних системах і мережах. / Програмування, 2004 .- № 5 - 5-16 с.; **2.** *Титоренко Г.А.* Інформаційні технології управління. М., Юніті: 2002; **3.** *Галатенко В.А.* Основы информационной безопасности. – СПб. : Питер, 2006. – 204 с.; **4.** *Губенков А.А., Байбурин В.Б.* Информационная безопасность. – М. : Радио и связь, 2005. – 308 с.; **5.** *Кечиев Л.Н., Степанова П.В.* ЭМС и информационная безопасность в системах телекоммуникаций. – М. : Мысль, 2005. – 269 с.

О. Роман, студентка

ГЕНЕЗИС НАУКОВИХ ПОГЛЯДІВ ЩОДО ВИЗНАЧЕННЯ СУТНОСТІ ДЕФІНІЦІЇ «ФІНАНСОВА БЕЗПЕКА ПІДПРИЄМСТВА»

Відсутність єдиного науковообґрунтованого підходу до визначення сутності поняття «фінансова безпека» зумовлює необхідність дослідження та порівняння теоретичного базису, що зустрічаються у різних наукових працях. Найбільш загальне визначення дефініції «фінансова безпека» наступне: це такий стан фінансово-кредитної сфери підприємства, який характеризується збалансованістю і якістю системної сукупності фінансових інструментів, технологій і послуг, стійкістю до внутрішніх і зовнішніх негативних чинників (загроз), здатністю цієї сфери забезпечувати захист фінансових інтересів, достатні обсяги фінансових ресурсів для всіх його підсистем та процесів [1].

Український науковець Барановський О.І. у своїй монографії «Фінансова безпека в Україні (методологія оцінки та механізм забезпечення)» визначає