УДК 681.528.54

Домарєв В.В., Климчук Р.В.

ТЕНДЕНЦІЇ РОЗВИТКУ МЕТОДОЛОГІЧНИХ, ТЕХНОЛОГІЧНИХ ТА ОРГАНІЗАЦІЙНИХ ОСНОВ СТВОРЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

Викладено питання розвитку методологічних, технологічних та організаційних основ створення систем безпеки інформаційних технологій з метою підвищення ефективності організаційно-технічних заходів на етапах проектування, впровадження та експлуатації систем безпеки інформаційних технологій.

Ключові слова: система безпеки, інформаційні технології, інформатизація, інформаційно-телекомунікаційна система.

Інформатизація як сукупність специфічних правових, науково-технічних та виробничих процесів з використанням ІТ, сприяє поліпшенню управління економікою, розвитку наукоємних виробництв, вдосконаленню соціально-економічних відносин та водночас стимулюють появу і розвиток невідомих раніше видів загроз безпеці комп'ютерної інформації.

Тенденція проникнення інформаційних технологій (ІТ) в усі сфери суспільних відносин супроводжується поширенням рівня загроз безпеці громадян і держави. Безпека національних інформаційних ресурсів та інформаційних технологій є одними з найбільш вагомих чинників національної безпеки України.

Практика показує, що проблема безпеки інформаційних технологій (БІТ) складна, різнопланова і пов'язана з вирішенням широкого спектра завдань, таких як: побудова раціональних методів і моделей оцінки рівня безпеки інформаційних ресурсів в системах управління органів державної влади, особливо силових структур, проведення аудита та експертиз стану безпеки інформаційно-телекомунікаційних систем (ІТС) з метою оцінки ефективності заходів щодо захисту інформації, розроблення ефективних апаратних і програмних засобів для реалізації алгоритмів методів і моделей систем безпеки інформаційних технологій.

Відомо, що захисні заходи забезпечують конфіденційність, цілісність і доступність інформації, однак якщо для режимних державних організацій на першому місці конфіденційність то для комерційних структур важливіше за все цілісність (актуальність) і доступність даних. У порівнянні з державними, комерційні організації більш відкриті й динамічні, тому ймовірні загрози для ІТС, які вони використовують, відрізняються й кількісно, і якісно. До того ж, оцінки важливості різних аспектів безпеки в державних і комерційних структурах досить різні.

Наприклад ІТС банківських систем відповідно до характеру завдань, що вирішуються ними, вимагають застосування нестандартних заходів забезпечення безпеки даних і висувають підвищені вимоги до безпеки процедур обробки інформації. До того ж безпеку інформації доводиться постійно підтримувати, взаємодіючи при цьому не тільки й не стільки з комп'ютерами, скільки з людьми.

Існуючи методичні рекомендації щодо захисту інформації в ІТС орієнтовані в першу чергу на розроблювачів інформаційних систем, а не на користувачів чи системних адміністраторів або менеджерів безпеки. Водночас з практичної точки зору більш важливі рекомендації, які дають не строго оптимальне, але досить ефективне рішення щодо захисту інформації.

Сучасні методики не враховують постійної перебудови структури ІТС, що захищаються, та не містять практичних рекомендацій з формування режиму безпеки. Іншими словами, ці рекомендації не дають відповідей на два головних із практичної точки зору питання:

- Як створювати корпоративну інформаційну систему, щоб вона відповідала вимогам безпеки інформації?
- Як практично сформувати політику безпеки й підтримувати її в умовах постійної зміни конфігурації програмно-апаратних засобів й структури самої системи?

У якості основних тенденцій розвитку сучасних методичних підходів до захисту інформації можна зазначити:

- розвиток методик оцінки, які дозволяють простежити прямування від єдиної шкали ранжирування вимог і критеріїв безпеки до множини незалежних приватних показників і введенню частково упорядкованих шкал;
- зростання ролі вимог адекватності реалізації засобів захисту і політики безпеки що свідчить про переваження «якості» забезпечення захисту над її «кількістю»;
- визначення функцій учасників процесу створення й експлуатації захищених систем, застосування відповідних механізмів і технологій оптимального розподілу відповідальності між всіма учасниками цього процесу.

На даному етапі в інформаційно-телекомунікаційних системах органів державної влади та місцевого самоврядування України багато уваги приділяється створенню комплексних систем захисту інформації. Але процес проектування та впровадження зазначених систем захисту базується на застарілих методичних підходах технічного захисту інформації, коли особлива увага приділяється збереженню конфіденційності інформації з обмеженим доступом на окремих об’єктах інформаційної діяльності.

Натомість сучасний рівень розвитку інформаційних технологій передбачає сумісне використання ІТС різноманітних за структурою, призначенням та власністю. Ускладнення технологій обробки інформації призвело до появи нових видів загроз для процесів функціонування комп’ютерних систем. Збитки та руйнації, що є наслідком реалізація загроз інформаційним технологіям, набагато більші ніж наслідки загроз витоку інформації технічними каналами.

На відміну від методик технічного захисту інформації на окремих об’єктах інформаційної діяльності, виникає потреба дослідження та впровадження сучасних підходів та методичного апарату для створення систем безпеки інформаційних технологій (СБІТ) які б враховували питання захисту складних процесів обробки інформації в корпоративних ІТС.

Незважаючи на існування великої кількості праць, у яких розглядаються конкретні вузькі питання технічного або криптографічного захисту інформації в державних ІТС, практично не досліджені теоретичні підходи до вирішення проблем безпеки інформаційних технологій під час сумісного використання різноманітних ІТС різної форми власності.

Таким чином, складність й різнорідність сучасних ІТС потребує наукового дослідження та розробки системного підходу до вирішення проблем безпеки інформації шляхом розвитку методологічних, технологічних та організаційних основ створення відповідних систем безпеки інформаційних технологій (СБІТ).

СБІТ являють собою складні організаційно-технічні системи, що мають велику вимірність і багаторівневість. У роботах по створенню таких систем безпеки, як правило, беруть участь десятки організацій та підприємств, що накладає специфічні вимоги стосовно узгодження їхніх дій.

При переході від методів проектування засобів технічного захисту інформації до складних систем безпеки виникає необхідність створення єдиної комплексної методології проектування та впровадження СБІТ, яка об'єднує в собі методи розробки підсистем, елементів та програмних механізмів захисту інформації.

У цьому зв'язку в розробці СБІТ, на відміну від розробки засобів технічного захисту інформації, більшу частину складають задачі системного проектування та аналізу. Це задачі декомпозиції, системного проектування різних властивостей систем безпеки, побудови математичних та системних моделей різного класу, комплексування проектних рішень, розробки технічних вимог до елементів систем, аналізу коректності проектних рішень і т.п.

Оскільки СБІТ має велику вимірність і багаторівневість, то провести об'єктивний та достовірний аналіз проектних рішень на етапах системного проектування без сучасних комп'ютерних технологій неможливо. Тому методологія та методи розробки системних етапів СБІТ повинні створюватись з урахуванням їхньої подальшої реалізації

комп'ютерними засобами, що, в свою чергу, потребує їхньої формалізації та розробки нової інформаційної технології проектування.

Таким чином, нові види загроз інформаційним технологіям, складність й різнорідність сучасних ІТС потребує наукового дослідження та розробки системного підходу до вирішення проблем захисту інформаційних ресурсів шляхом розвитку методологічних, технологічних та організаційних основ створення відповідних систем безпеки інформаційних технологій.

Отже, розвиток методологічних, технологічних та організаційних основ створення систем безпеки інформаційних технологій з метою підвищення ефективності організаційно-технічних заходів на етапах проектування, впровадження та експлуатації СБІТ є актуальною і важливою проблемою. Дослідження цієї проблеми дозволить визначити методичні шляхи створення ефективних систем безпеки ІТ, що раціонально об'єднують різноманітні за властивостями засоби, заходи і методи захисту інформації.

ЛІТЕРАТУРА

1. Концепція технічного захисту інформації в Україні: Постанова КМ України від 8 жовтня 1997 р. №1126. // Урядовий кур'єр. -1997. - 12 листопада.

2. Положення про технічний захист інформації в Україні: Постанова КМ України від 9 вересня 1994 р. №632. // Запорізька правда України. -1994. -№12.

3. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.

4. Домарев В.В. Безопасность информационных технологий. Системный подход / В.В. Домарев. - К.: ООО ТИД Диа Софт, 2004. - 992 с.

5. Домарєв В.В. Управління інформаційною безпекою в банківських установах. Теорія і практика впровадження стандартів серії ISO 27k / В.В. Домарєв, Д.В. Домарєв. - Д.: Велстар,2012.-143с.

6. Конеев И.Р., Беляев А. В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 203.-752с :ил.

7. Уфимцев Ю.С., Буянов В.П., Ерофеев Е.А., Жогла Н.Л., Зайцев О. А., Курбатов Г.Л, Петренко А. И., Федотов Н. В. Методика информационной безопасности. – М.: Издательство «Экзамен», 2004. – 544с.

Надійшла: 16.12.2012

Рецензент: д.т.н., проф. Дудикевич В.Б.