Вступ

Незважаючи на те, що сучасний прогрес у галузі глобальних комп'ютерних мереж і засобів мультимедіа привів до розроблення численних методів, призначених для гарантування безпечного передавання даних каналами телекомунікацій і використання їх у неоголошених цілях, алгоритмів синтезу інформаційних систем, ці методи часто не мають потрібного теоретичного обґрунтування, опис їхніх властивостей, переваг і недоліків опирається лише на практичний досвід їх використання, що не гарантує їхньої успішної роботи у разі застосування в позаштатних ситуаціях (такими часто є стеганографічні методи, методи розпізнавання фальсифікацій цифрових контентів тощо).

Масове створення, впровадження і експлуатація інформаційних систем призвели до виникнення спектра нових проблем у сфері безпеки інформації. І це закономірно. Коли комерційна організація допускає витік більш ніж 20 % важливої внутрішньої інформації, вона в 60 випадках зі 100 банкрутує. Стверджують також, що 93 % компаній, які втратили доступ до особистої інформації на термін 10 днів, залишили свій бізнес, причому половина з них заявила про свою неспроможність негайно.

Потреби в гарантуванні безпеки пов'язані з тим, що існує множина суб'єктів і структур, які зацікавлені в чужій інформацій і готові платити за це високу ціну. Так, вартість пристроїв підслуховування, які продаються у США, становить у середньому приблизно 900 тис. дол. на рік. Сумарна шкода, яку завдають організаціям, проти яких виконують підслуховування, становить кожен рік у США приблизно 8 млрд дол. А придбати пристрої для несанкціонованого доступу до інформації можливо і за іншими каналами: проникнення в інформаційні системи, перехоплення і дешифрування повідомлень тощо. В результаті, за даними SANS Institute, середній розмір збитку від однієї атаки в США на корпоративну систему для банківського й IT-секторів становить приблизно півмільйона доларів. Приблизно структура наслідків неефективного гарантування інформаційної безпеки в американських організаціях є такою: крадіжка конфіденційної інформації – 20–25 % від загального річного збитку; фальсифікування фінансової інформації – 21–25 %; забруднення шкідливими програмами – 11–12 %; порушення доступу до Web-сторінок – 1–11 %; зрив роботи інформаційної системи – 4–10 %; незаконний доступ працівників до інформації – 4–9 %; інші види шкоди – 14–33 %.

У таких умовах все більше поширюється аксіома, що захист інформації повинен за всіма характеристикам відповідати масштабам загроз. Відхилення від цього правила призведе до додаткових збитків. Для кожної інформаційної системи є оптимальний рівень захищеності, який необхідно постійно підтримувати. Немає сумнівів, що захист критично важливих для інформаційних систем масивів повинен відповідати міжнародним, корпоративним нормативним і методичним документам. Застосовуються високовартісні технічні засоби і впроваджуються суворо регламентовані організаційні заходи. Однак немає відповіді на найважливіше питання – наскільки рішення, яке запропоновується або реалізовується, справді вдале, яка його запланована і реальна ефективність. Такому положенню, яке наявне в інформаційній системі, але є неможливим у галузі гарантування інформаційної безпеки, відповідає низка причин:

• ігнорування системного підходу до методології аналізу і синтезу систем захисту інформації (СЗІ);

• відсутність механізмів повного і достовірного підтвердження якості СЗІ;

• недоліки нормативно-методичного гарантування інформаційної безпеки, насамперед у галузі показників і критеріїв.

Усім фахівцям у галузі захисту інформації відомі основні постулати, які не втратили актуальність досі: абсолютний захист створити неможливо; СЗІ повинна бути комплексною; СЗІ повинна бути адаптованою до змін обстановки; СЗІ повинна бути системою, а не простим набором хаотичних деяких технічних засобів і організаційних заходів, як це частіше буває на практиці; системний підхід до захисту інформації повинен застосовуватися, починаючи від підготовки технічного завдання і закінчуючи оцінкою ефективності та якості СЗІ в процесі її експлуатації – життєвий цикл КСЗІ.

Успіх у сфері інформаційної безпеки може принести тільки комплексний підхід, що уособлює в собі заходи чотирьох рівнів:

• законодавчого;

• адміністративного;

• процедурного;

• програмно-технічного.

Проблема ІБ – не тільки (і не стільки) технічна; без законодавчої бази, без постійної уваги керівництва організації й виділення необхідних ресурсів, без заходів керування персоналом і фізичного захисту вирішити її неможливо. Комплексність також ускладнює проблематику ІБ; необхідна взаємодія фахівців із різних галузей.

Як основний інструмент боротьби зі складністю запропоновано об’єктно-орієнтований підхід. Інкапсуляція, успадкування, поліморфізм, виділення гра-

ней об'єктів, варіювання рівня деталізації – все це універсальні поняття, знати які необхідно всім фахівцям з інформаційної безпеки.

Законодавчий рівень є найважливішим для гарантування інформаційної безпеки. Необхідно всіляко підкреслювати важливість проблеми ІБ; сконцентрувати ресурси на найважливіших напрямах досліджень; скоординувати освітню діяльність; створити й підтримувати негативне ставлення до порушників ІБ – все це функції законодавчого рівня.

На законодавчому рівні особливої уваги заслуговують правові акти й стандарти.

Головне завдання засобів адміністративного рівня – сформувати програму робіт у сфері інформаційної безпеки й забезпечити її виконання, виділяючи необхідні ресурси й контролюючи стан справ.

Основою програми є політика безпеки, що уособлює підхід організації до захисту своїх інформаційних активів. Розроблення політики й програми безпеки починається від аналізу ризиків, першим етапом якого, насамперед, є ознайомлення з найпоширенішими загрозами.

Головні загрози – внутрішня складність ІС, ненавмисні помилки штатних користувачів, операторів, системних адміністраторів й інших осіб, що обслуговують інформаційні системи.

На другому місці за розміром збитку стоять крадіжки й підробки. Реальною небезпекою є: пожежі й інші аварії підтримувальної інфраструктури.

У загальній кількості порушень зростає частка зовнішніх атак, але основний збиток, як і раніше, завдають "свої". Для переважної більшості організацій доволі загального знайомства з ризиками; орієнтація на типові, апробовані рішення дасть змогу гарантувати базовий рівень безпеки за мінімальних інтелектуальних і поміркованих матеріальних витрат. Розробка програми й політики безпеки може бути прикладом використання поняття рівня деталізації. Все це повинно підрозділятися на кілька рівнів, що трактують питання різного ступеня специфічності.

Важливим елементом програми є розроблення й підтримання в актуальному стані карти ІС.

Безпеку неможливо додати до системи, її потрібно закладати з самого початку й підтримувати до кінця.

Заходи процедурного рівня орієнтовані на людей (а не на технічні засоби) підрозділяються на такі види:

- керування персоналом;
- фізичний захист;

• підтримка працездатності;
• реагування на порушення режиму безпеки;
• планування відновлювальних робіт.

На цьому рівні застосовуються важливі принципи безпеки:
• безперервність захисту в просторі й часі;
• поділ обов'язків;
• мінімізація привілеїв.

Поняття життєвого циклу корисно застосовувати не тільки до інформаційних систем, але й до співробітників. На етапі ініціації повинен бути розроблений опис посади з вимогами до кваліфікації й виділених комп'ютерних привілеїв; на етапі встановлення необхідно провести навчання, зокрема з питань безпеки; на етапі виведення з експлуатації потрібно діяти акуратно, не допускаючи завдання збитків скривдженими співробітниками.

Результативне виконання завдань аналізу і синтезу СЗІ не може бути забезпечено одними лише способами простого опису їх поведінки в різних умовах – системотехніка висуває проблеми, які потребують кількісної оцінки характеристик. Такі дані, які отримані експериментально або за допомогою математичного моделювання, повинні розкривати властивості СЗІ. Основним із них є ефективність, під якою розуміють ступінь відповідності результатів захисту інформації поставленій меті. Остання, залежно від наявних ресурсів, знань розробників та інших факторів, може бути досягнута тією або іншою мірою, тоді можливі альтернативні способи її реалізації. Ефективність має безпосередній зв'язок з іншими системними властивостями, зокрема надійністю, живучістю, завадозахищеністю – а загалом стійкістю. Тому кількісна оцінка ефективності дає змогу вимірювати і об'єктивно аналізувати основні властивості систем на всіх стадіях їх життєвого циклу, починаючи з етапу формування вимог і ескізного проєктування.

Частіше замовник СЗІ погано уявляє значення того або іншого засобу і його необхідність у загальному рівні безпеки, і в результаті збільшуються витрати у разі практичної невизначеності досягнутого ефекту. Надалі замовник СЗІ не отримує те, що йому реально потрібно, і не може об'єктивно перевірити і оцінити якість і ефективність запропонованого рішення.

Тому на першому плані проблема – як створити таку систему захисту інформації, яка б спроможна була за мінімальних витрат виконувати максимальні завдання захисту інформації. Цю проблему необхідно вирішувати поступово, починаючи з головного етапу життєвого циклу – проєктування систем захисту інформації в комплексі з особливостями об'єкта захисту.