УДК 347.731:681.3

О.В. Бойченко, к. т. н.

МОДЕЛЮВАННЯ СУЧАСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Розглянуто питання моделювання систем захисту інформаційних ресурсів для підвищення ефективності систем інформаційної безпеки в діяльності органів внутрішніх справ України. Запропоновано систему економічного обґрунтування застосування трирівневої системи інформаційної безпеки.

The question of design of informative resources defence systems is examined for the increase of informative safety systems efficiency in activity of OIA of Ukraine. The system of economic ground of the three-level system of informative safety application is offered..

Постановка проблеми

Становлення та розвиток інформаційного суспільства, стрімке впровадження інформаційно-телекомунікаційних систем і технології в усі сфери життєдіяльності суспільства, широке впровадження у практику діяльності організацій та установ цифрової технології оброблення та обміну даними, а також необхідність забезпечення захисту інформаційного ресурсу закладів, зумовлює потребу у розробленні новітніх підходів до функціонування системи інформаційної безпеки підприємств.

Особливо нагально зазначене стосується діяльності органів внутрішніх справ, що зумовлено наявністю формування та використання значних обсягів конфіденційних даних. Тому науковий пошук створення більш дієвих систем методів захисту інформаційних ресурсів досить обґрунтований.

Аналіз останніх наукових досліджень та публікацій

Застосування організаційних, програмно-технічних та інших заходів захисту інформаційних ресурсів організацій та установ свого часу досліджували такі видатні фахівці, як В.О. Галатенко [1; 2], Я.Ю. Кондратьєв, Б.В. Романюк, М.І. Камлик, В.Д. Гавловський, Л.М. Кечиєв [3; 4]. Проте питанням моделювання та економічного обґрунтування застосування відповідних систем захисту даних у наукових розробках приділено недостатньо уваги.

Мета роботи полягає у проведенні аналізу наукових підходів до моделювання систем захисту інформаційних ресурсів організацій для оптимізації комплексу заходів інформаційної безпеки в діяльності органів внутрішніх справ України.

Системи захисту інформаційних ресурсів

Для економічного обґрунтування сучасних систем захисту інформаційних ресурсів розглянемо модель модернізації корпоративної системи антивірусного захисту і системи управління доступом на об’єкті інформатизації.

Для цього спочатку умовно визначимо три можливі рівні системи захисту інформаційних ресурсів та інформаційної системи від вірусів і шкідливого програмного забезпечення[1]:

− базовий;
− середній;
− високий.

Базовий рівень характеризується тим, що стаціонарні і мобільні робочі станції мають локальний захист від вірусів. Антивірусне програмне забезпечення і бази регулярно оновлюються для успішного розпізнавання і знищення нових вірусів, встановлюється програма автоматичного знищення найбільш небезпечних вірусів. Основна мета рівня – організація мінімального захисту від вірусів і шкідливого програмного забезпечення при невеликих витратах.

На середньому рівні встановлюється мережева програма виявлення вірусів. Керування програмним оновленням на сервері автоматизоване. Системний контроль над подіями оповіщає про випадки появи вірусів і надає інформацію щодо запобігання подальшому розповсюдженню вірусів. Превентивний захист від вірусів припускає вироблення і проходження певної політики захисту інформації, що передається відкритими каналами зв’язку Інтернет. Додатково до технічних заходів використовуються організаційні заходи захисту інформації.

Високий рівень характеризується тим, що антивірусний захист сприймається як один з основних компонентів корпоративної системи захисту. Система антивірусного захисту тісно інтегрована в комплексну систему централізованого керування безпеки інформаційних ресурсів компанії і має максимальний ступінь автоматизації. При цьому організаційні заходи із захисту інформації переважають над технічними заходами. Стратегія захисту інформації визначається виключно стратегією розвитку бізнесу компанії.

Умовно виділимо три рівні розвитку системи контролю й керування доступом в інформаційній системі (забезпечення фізичної безпеки) [5]:
− базовий;
− середній;
− високий.
На базовому рівні ведеться облік робочих станцій і серверів, інвентарні таблички кріпляться на відповідне апаратне забезпечення, уведено процедуру контролю переміщення апаратних засобів інформаційних систем, періодично проводяться інструктажі персоналу компанії. Особлива увага приділяється мобільним компонентам інформаційних систем.
На середньому рівні використовуються механічні й електронні замки, шлюзові кабіни і турнікети; організовуються контрольно-пропускні і прохідні пункти; здійснюється відеоспостереження на об'єкті інформатизації; розробляються інструкції щодо дії у штатних і позаштатних ситуаціях; залучаються приватні і державні охоронні підприємства і структури.
Високий рівень характеризується тим, що забезпечення фізичної безпеки апаратних засобів є частиною єдиної політики безпеки, затвердженої керівництвом компанії. Активно використовується весь комплекс заходів захисту інформації, починаючи з організаційного і закінчуючи технічним рівнями.
Модель з модернізації корпоративної системи щодо безпеки інформаційних ресурсів передбачає модернізацію двох елементів:
− антивірусного захисту;
− системи керування безпекою інформаційних ресурсів.
Обгрунтовуючи перехід від базового до підвищеного (середнього або високого) рівня захисту інформаційних ресурсів, на практиці розробляються вимоги до елементів захисту, сформульовані в завданні на модернізацію інформаційної системи [3; 5].
При цьому можливі декілька варіантів реалізації цих вимог, що характеризуються різними економічними показниками.
Розглядаючи типову структуру витрат за вибраними елементами системи безпеки інформаційних ресурсів, необхідно насамперед визначитись з витратами на створення системи безпеки інформаційних ресурсів, які включають витрати, що включають такі категорії:
1) витрати на формування і підтримання ланки керування системою захисту інформації (організаційні витрати);
2) витрати на контроль, тобто на визначення і підтвердження досягнутого рівня захищеності ресурсів підприємства;
3) внутрішні витрати на ліквідацію наслідків порушення політики інформаційної безпеки – витрати, пов'язані з компенсацією наслідків негативного результату застосування системи інформаційної безпеки (недостатність потрібного рівня захищеності);
4) зовнішні витрати на ліквідацію наслідків порушення політики інформаційної безпеки – компенсація втрат у випадках, пов'язаних з просочуванням інформації, втратою іміджу компанії, втратою довіри партнерів і споживачів.
При цьому зазвичай виділяють одноразові і систематичні витрати. До одноразових відносяться витрати на формування політики інформаційної безпеки підприємства (організаційні витрати і витрати на придбання і установку засобів захисту).
Класифікація витрат умовна, оскільки збирання, класифікація і аналіз витрат на інформаційну безпеку – внутрішня діяльність підприємств, і детальна розробка переліку втрат залежить від особливостей конкретної організації. Найголовніше у визначенні витрат на систему інформаційної безпеки – взаєморозуміння та згода за статтями витрат усередині підприємства. Крім того, категорії витрат мають бути постійними і не повинні дублювати один одного.
Неможливо повністю виключити витрати на інформаційну безпеку, проте вони можуть бути зведені до прийнятного рівня. Деякі види витрат на інформаційну безпеку є абсолютно необхідними, а деякі можуть бути істотно зменшені або виключені. Останні – це ті, які можуть зникнути, коли немає порушень політики інформаційної безпеки, або скоротяться у випадку зменшення кількості порушень та їх руйнівної дії.
У разі дотримання політики інформаційної безпеки та проведення профілактики порушень можна виключити або істотно зменшити такі витрати:
− відновлення системи інформаційної безпеки відповідно до вимог політики безпеки;
− відновлення ресурсів інформаційного середовища підприємства;
− переобладнання системи інформаційної безпеки;
− юридичні спори та виплати компенсацій;
− встановлення причин порушення політики інформаційної безпеки.

Необхідні витрати не залежать від рівня погроз безпеці інформації, тобто вони є обов'язковими в умовах навіть досить низького рівня погроз безпеці інформації, а саме вони визначаються витратами на підтримання досягнутого рівня захищеності інформаційного середовища підприємства.

Неминучі витрати можуть включати:

− обслуговування технічних засобів захисту;

− конфіденційне діловодство;

− функціонування та аудит системи інформаційної безпеки;

− мінімальний рівень перевірок і контролю із залученням спеціалізованих організацій;

− навчання персоналу методам інформаційної безпеки.

Важливим елементом ефективного функціонування системи інформаційного захисту є визначення залежності між витратами на безпеку інформаційних ресурсів і рівнем захищеності інформаційної системи.

Сума всіх витрат на підвищення рівня захищеності підприємства від погроз інформаційній безпеці складає загальні витрати на безпеку.

У свою чергу, загальні витрати на безпеку складаються з витрат на попереджувальні заходи, витрат на контроль і відновлення втрат (зовнішніх і внутрішніх). Зі зміною рівня захищеності інформаційного середовища змінюються загальні витрати на інформаційну безпеку.

Це відбувається за рахунок збільшення обсягів попереджувальних заходів, пов'язаних з обслуговуванням системи захисту. Витрати на компенсацію зменшуються в результаті попереджувальних дій, що приводить до зменшення загальних витрат на інформаційну безпеку. Зміни ж обсягів витрат на контроль незначні.

У разі стійкого зниження витрат на компенсацію порушень політики інформаційної безпеки витрати на попереджувальні заходи все більше зростають. Таким чином, щоб знизити рівень ризику безпеці інформації потрібно заощадити значну кількість витрат з урахуванням відсоткового внеску від загальної кількості витрат організації на забезпечення потрібного рівня захисту інформаційних ресурсів [5].

Проведений аналіз із використанням класичних методів математичного моделювання та прогнозування стосується тільки загального випадку, оскільки оснований на відповідних припущеннях, які не завжди відповідають реальним ситуаціям.

Перше припущення стосується визначення попереджувальної діяльності з технічного обслуговування комплексу програмно-технічних засобів захисту інформації, а також попередження порушень політики інформаційної безпеки підприємства відповідно до правила пріоритету, згідно з яким першочерговим є розгляд проблем, вирішення яких дає найбільший ефект зі зниження інформаційного ризику.

Друге допущення визначається незмінністю в часі точки економічної рівноваги.

Однак на практиці таке припущення часто не виконується.

Ефективність попереджувальної діяльності щодо зниження ризику інформаційної безпеки, яка зазначена в цій моделі, невелика.

Але такий підхід дає змогу не повторювати допущені раніше помилки, що, у свою чергу, підвищує ефективність системи інформаційного захисту взагалі.

Практика вказує на потребу в залученні набагато більших витрат для досягнення належного ефекту застосування системи інформаційного захисту, що в результаті призводить до зрушення точки економічної рівноваги.

Крім того, розробники засобів захисту не встигають за активністю зловмисників, які знаходять все нові і нові недоліки в системах захисту. Разом з цим, інформатизація підприємства може породити нові проблеми, для вирішення яких потрібні будуть додаткові попереджувальні витрати.

Наступним важливим етапом економічного обґрунтування є збирання і аналіз даних, складання звіту за витратами на безпеку інформаційних ресурсів і узгодження із загальними фінансовими розрахунками.

Важливим також є проведення та складання типових баз вимірювань, що для багатьох організацій визначається співвідношенням витрати на безпеку з обсягами проданої продукції.

Проте, якщо обсяги продажу залежать від сезонних чинників (циклічних змін), вони не можуть бути достовірною базою як досить непевний показник.

У такому випадку обсяги виробництва й витрати на інформаційну безпеку можуть залишатися відносно постійними.

Важливо також є ураховувати те, що обсяг проданої продукції відрізняється від обсягу поставленої продукції, оскільки поставлена споживачеві продукція може бути ще не сплачена. Зазначене стосується також і обсягу проведеної продукції, який може не збігатися з обсягом реально проданої або поставленої продукції.

Отже, модельний вибір бази вимірювань для співвідношення витрат на безпеку (вартість проведеної продукції, кількість проведених одиниць продукту, обсяг проданої продукції, вартість поставленої продукції) залежить від технологічних обставин, які характеризують діяльність відповідного підприємства та відповідності рівня інформаційного захисту витратам на інформаційну безпеку.

Важливим елементом моделі є визначення цінності інформаційних ресурсів, що обов'язково повинно враховуватись під час проведення економічного обґрунтування.

Цінність інформаційних ресурсів підприємства з економічного погляду – це сукупна вартість власних ресурсів, що виділяються в інформаційному середовищі підприємства. Ресурси зазвичай підрозділяються на декілька класів, наприклад, фізичні, програмні та інформаційні.

Цінність ресурсів оцінюють спеціалізовані організації під час виконання роботи з аналізу ризиків інформаційної безпеки підприємства. Зазвичай, фізичні ресурси оцінюють з урахуванням вартості їх заміни або відновлення працездатності.

Програмні ресурси оцінюють тим же способом, що і фізичні – на основі визначення витрат на їх придбання або відновлення. Якщо для інформаційного ресурсу існують особливі вимоги до конфіденційності або цілісності, то оцінювання цього ресурсу проводиться за такою ж схемою (у вартісному виразі).

Завершальний етап моделі – ухвалення рішень. Після установлення причини завдання збитків інформаційному ресурсу потрібне проведення заходів щодо коректування та здійснення пошуку областей, які дадуть найбільшу віддачу у відповідь на витрачені зусилля.

Отже, проведення ретельного аналізу функціонування системи захисту інформації дозволить більш ретельно та ефективно застосовувати попереджувальні заходи для механізмів інформаційного захисту з оптимальною витратною частиною [6].

Висновки

Витрати на безпеку інформаційних ресурсів можуть бути понижені значною мірою за рахунок виявлення специфічних причин втрат і запропонованих програм зниження рівня ризику.

Крім того, всі рекомендації з удосконалення системи інформаційного захисту повинні містити дані про вартість застосування запропонованих програм. А заходи зниження рівня інформаційного ризику мають відповідати досягненню основного завдання – з найменшими витратами отримати якнайкращі результати.

Література

1. *Галатенко В.А.* Основы информационной безопасности. – С.Пб.: Питер, 2006. – 204 с.
2. *Галатенко В.А.* Стандарты информационной безопасности. – С.Пб.: Питер, 2006. – 236 с.
3. *Кечиев Л.Н., Степанов П.В.* ЭМС и информационная безопасность в системах телекоммуникаций. – М.: Мысль, 2005. – 269 с.
4. *Скотт В.* Разработка правил информационной безопасности. – М.: АйТи-Пресс, 2002. – 109 с.
5. *Губенков А.А., Байбурин В.Б.* Информационная безопасность. – М.: Радио и связь, 2005. – 308 с.
6. *Мельников В.В.* Безопасность информации в автоматизированных системах. – М.: Лучшие книги, 2003. – 264 с.

Стаття надійшла до редакції 19.12.08.