УДК 347.731:681.3
© О. Бойченко[1], 2011

МОДЕЛЮВАННЯ СУЧАСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Розглядається питання моделювання систем захисту інформаційних ресурсів для підвищення ефективності систем інформаційної безпеки в діяльності ОВС України. Запропонована система економічного обґрунтування застосування трьохрівневої системи інформаційної безпеки.

The question of design of informative resources defense 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.

1. ПОСТАНОВКА ЗАДАЧІ

Становлення та розвиток інформаційного суспільства, стрімке впровадження інформаційно-телекомунікаційних систем та технології в усі сфери життєдіяльності суспільства, широке впровадження в практику діяльності організацій та установ цифрової технології обробки та обміну даними, а також необхідність забезпечення захисту інформаційного ресурсу закладів, тягне за собою розробку новітніх підходів до функціонування системи інформаційної безпеки підприємств. Особливо нагально зазначене стосується діяльності органів внутрішніх справ, що обумовлено наявністю формування та використання значних обсягів конфіденційних даних. Тому науковий пошук у напрямку створення більш дієвих систем методів захисту інформаційних ресурсів є достатньо обґрунтованим.

Аналіз останніх наукових досліджень та публікацій. Дослідженням проблематики застосування організаційних, програмно-технічних та інших заходів захисту інформаційних ресурсів організацій та установ свого часу займалися такі видатні фахівці, як Галатенко В.О., Кондратьєв Я.Ю., Романюк Б.В., Камлик М.І., Гавловський В.Д., Кечиєв Л.М. та інші. Поряд з цим, зазначимо, що питанням моделювання та економічного обґрунтування застосування відповідних систем захисту даних у наукових розробках приділено не достатньо уваги.

Мета роботи полягає у проведенні аналізу наукових підходів до моделювання систем захисту інформаційних ресурсів організацій для

[1] Кримський юридичний інститут Одеського державного університету внутрішніх справ

оптимізації комплексу заходів інформаційної безпеки в діяльності ОВС України.

2. ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Для економічного обгрунтування 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 стани системи захисту інформаційних ресурсів і інформаційної системи від вірусів і шкідливого програмного забезпечення, а саме: базовий, середній та високий [1].

Базовий стан характеризується тим що, стаціонарні і мобільні робочі станції володіють локальним захистом від вірусів. Антивірусне програмне забезпечення і бази регулярно оновлюються для успішного розпізнавання і парирування 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 стані встановлюється мережева програма виявлення вірусів. Управління програмними оновленнями на сервері автоматизоване. Системний контроль над подіями оповіщає про випадки появи вірусів і надає інформацію по запобіганню подальшому розповсюдженню вірусів. Превентивний захист від вірусів припускає виробленя і проходження певної політики захисту інформації, передаваної по відкритих каналах зв'язку Інтернет. Додатково до технічних заходів використовуються організаційні заходи захисту інформації.

Високий стан характеризується тим, що антивірусний захист сприймається як один з основних компонентів корпоративної системи захисту. Система антивірусного захисту тісно інтегрована в комплексну систему централізованого управління безпеки інформаційних ресурсів компанії і володіє максимальним ступенем автоматизації. При цьому організаційні заходи по захисту інформації переважають над технічними заходами. Стратегія захисту інформації визначається виключно стратегією розвитку бізнесу компанії.

Також умовно виділимо три рівні розвитку системи контролю і управління доступом в інформаційній системі (забезпечення фізичної безпеки): базовий, середній та високий [2].

На базовому рівні ведеться облік як мінімум робочих станцій і серверів, інвентаризаційні таблички кріпляться на відповідне апаратне забезпечення. Введена процедура контролю переміщення апаратних засобів інформаційних систем. Проводяться постійні і періодичні ін-

структажі персоналу компанії. Особлива увага приділяється мобільним компонентам інформаційних систем.

На середньому рівні використовуються механічні і електронні замки, шлюзові кабіни і турнікети. Організовуються контрольно-пропускні пункти і прохідні. Здійснюється відеоспостереження на об'єкті інформатизації. Розробляються інструкції по дії в 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, затвердженій керівництвом компанії. Активно використовуються весь комплекс заходів захисту інформації, починаючи з організаційного і закінчуючи технічним рівнями.

Модель по модернізації корпоративної системи в частині безпеки інформаційних ресурсів припускає модернізацію двох елементів: антивірусного захисту і системи управління безпеки інформаційних ресурсів. Обґрунтовуючи перехід від базового рівня до підвищеного (середнього або високого) рівня захисту інформаційних ресурсів, на практиці розробляються вимоги до елементів захисту, сформульовані в завданні на модернізацію інформаційної системи [3,4].

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, які підрозділяються на наступні категорії:

1. Витрати на формування і підтримку ланки управління 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 необхідного 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 інфор-

маційної безпеки підприємства (організаційні витрати і витрати на придбання і установку засобів захисту).

Класифікація витрат умовна, оскільки збір, класифікація і аналіз витрат на інформаційну безпеку – внутрішня діяльність підприємств, і детальна розробка переліку втрат залежить від особливостей конкретної організації. Найголовніше при визначенні витрат на систему інформаційної безпеки – взаєморозуміння та згода за статтями витрат усередині підприємства. Крім того, категорії витрат повинні бути постійними і не повинні дублювати один одного.

Неможливо повністю виключити витрати на інформаційну безпеку, проте вони можуть бути приведені 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 за відсутності порушень політики інформаційної безпеки або скоротяться у випадку зменшення кількості порушень та їх руйнуючої дії.

При дотриманні політики інформаційної безпеки та проведенні профілактики порушень можна виключити або істотно зменшити наступні витрати:

1. Відновлення системи інформаційної безпеки до відповідності вимогам політики безпеки;
2. Відновлення ресурсів інформаційного середовища підприємства;
3. Переобладнання системи інформаційної безпеки;
4. Юридичні спори та виплати компенсацій;
5. 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 підтримку досягнутого рівня захищеності інформаційного середовища підприємства.

Неминучі витрати можуть включати:

1. Обслуговування технічних засобів захисту;
2. Конфіденційне діловодство;
3. Функціонування і аудит системи інформаційної безпеки;
4. Мінімальний рівень перевірок і контролю із залученням спеціалізованих організацій;
5. 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). Із зміною рівня захищеності інформаційного середовища змінюються величини загальних витрат і 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.

При стійкому зниженні витрат на компенсацію порушень політики інформаційної безпеки витрати на попереджувальні заходи все більше зростають. Таким чином для зниження рівня ризику безпеці інформації, необхідно заощадити значну кількість витрат з урахуванням відсоткового вкладу від загальної кількості витрат організації на забезпечення необхідного рівня захисту інформаційних ресурсів [5].

Проведений аналіз з використанням класичних методів математичного моделювання та прогнозу стосується тільки загальний випадок, оскільки заснований 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 у відповідності з правилом пріоритету, згідно з яким першочерговим є розгляд проблем, вирішення яких дає найбільший ефект по зниженню інформаційного ризику.

Друге допущення визначається незмінністю в часі точки економічної рівноваги. Однак слід зазначити, що на практиці таке припущення часто не виконується.

3. ОСНОВНІ РЕЗУЛЬТАТИ

Підводячи підсумок, слід зазначити, що ефективність попереджувальної діяльності у напрямку зниження ризику інформаційній безпеці, яка зазначена в даній моделі, не велика. Але такий підхід дозволяє не повторювати допущені раніше помилки, що у свою чергу підвищує ефективність системи інформаційного захисту взагалі.

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

Крім того, розробники засобів захисту не встигають за активністю зловмисників, які знаходять все нові і нові проломи в системах захисту. Поряд із цим, інформатизація підприємства може породити нові проблеми, вирішення яких зажадає додаткових попереджувальних витрат.

Наступним важливим етапом економічного обґрунтування є збір і аналіз даних, складання звіту за витратами на безпеку інформаційних ресурсів і узгодження з 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 доволі мінливий показник. У такому випадку обсяги виробництва й витрати на інформаційну безпеку можуть залишатися відносно постійними.

Важливим також є урахування того, 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 співпадати з обсягом реально проданої або поставленої продукції.

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

Важливим елементом моделі є визначення цінності інформаційних ресурсів, що обов’язково повинно враховуватись при проведенні економічного обґрунтування.

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

Оцінка цінності ресурсів проводиться спеціалізованими організаціями під час виконання роботи по аналізу ризиків інформаційної безпеки підприємства. Як правило, оцінка фізичних ресурсів проводиться з урахуванням вартості їх заміни або відновлення працездатності.

Програмні ресурси оцінюються 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 оцінка цього ресурсу проводиться за такою ж схемою (у вартісному виразі).

Завершальним етапом моделі є ухвалення рішень. Усі встановлені причини нанесення збитку інформаційному ресурсу тягнуть за собою проведення необхідних заходів коректування та здійснення пошуку областей, які дадуть найбільшу віддачу у відповідь на витрачені зусилля.

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

4. ВИСНОВКИ

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

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

1. Галатенко В.А. Основы информационной безопасности.– С-Пб.: «Питер», 2006. – 204 с. 2. Организация и современные методы защиты информации / Под общ. ред. С.А. Диева, А.Г. Шаваева. – М.: Концерн "Банковский Деловой Центр", 2008. – 472 с. 3. Губенков А.А., Байбурин В.Б. Информационная безопасность. - М.: «Радио и связь», 2005. – 308 с. 4. Кечиев Л.Н., Степанов П.В. ЭМС и информационная безопасность в системах телекоммуникаций. – М.: «Мысль», 2005. – 269 с. 5. С.Л. Емельянов. Основы информационной безопасности. – Одесса: Изд-во "Юридична література", 2008 г. - 196 с. 6. Скотт В. Разработка правил информационной безопасности. - М.: «АйТи-Пресс», 2002. – 109 с.