УДК 347.731:681.3

Бойченко О. В., к.т.н.; **Торошанко Я. І.,** к.т.н.

МОДЕЛЬ КОРПОРАТИВНОГО ІНФОРМАЦІЙНОГО ЗАХИСТУ ОБ'ЄКТУ ІНФОРМАТИЗАЦІЇ

Бойченко О. В., Торошанко Я. І. Модель корпоративного інформаційного захисту об'єкту інформатизації. Розглядаються питання захисту від несанкціонованого доступу інформаційних ресурсів організацій і установ. Запропонована модель корпоративної системи антивірусного захисту і системи управління доступом на об'єкті інформатизації.

Ключові слова: ЗАХИСТ ІНФОРМАЦІЇ, ВІРУС, УПРАВЛІННЯ ДОСТУПОМ, ІНФОРМАЦІЙНА БЕЗПЕКА

Бойченко О. В., Торошанко Я. И. Модель корпоративной информацийнной защиты объекта информатизации. Рассматриваются вопросы защиты от несанкционированного доступа информационных ресурсов организаций и учреждений. Предложена модель корпоративной системы антивирусной защиты и системы управления доступом на объекте информатизации.

Ключевые слова: ЗАЩИТА ИНФОРМАЦИИ, ВИРУСЫ, УПРАВЛЕНИЕ ДОСТУПОМ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Boichenko O. V., Toroshanko Ya. I. Model of corporate information protection of informatization object. Issues of fetch protection of information resources of organizations and enterprises are considered. The model is proposed for antivirus protection corporate system and access control system at the object of infromatization.

Keywords: INFORMATION PROTECTION, MODELLING, VIRUSES, ACCESS CONTROL, INFORMATION SECURITY

Вступ. Становлення та розвиток інформаційного суспільства, стрімке впровадження інформаційно-телекомунікаційних систем і технологій в усі сфери життєдіяльності суспільства, широке впровадження в практику діяльності організацій та установ цифрової технології обробки та обміну даними – характерна ознака сьогодення. Все це обумовлює актуальність задач забезпечення захисту інформаційного ресурсу цих закладів, а також потребує розробки новітніх підходів до функціонування системи інформаційної безпеки засобів обробки інформації підприємств.

Дослідженням проблематики застосування організаційних, програмно-технічних та інших заходів захисту інформаційних ресурсів організацій та установ свого часу займалися такі відомі фахівці, як Галатенко В. О., Кондратьєв Я. Ю., Романюк Б. В., Камлик М. І., Гавловський В. Д., Кечиєв Л. М. та інші [1].

Основні задачі та напрямки досліджень систем забезпечення інформаційної безпеки установ та організацій сформульовані в [2]. Це *накопичення* та захист від несанкціонованого доступу відомчих інформаційних ресурсів; *розробка*, впровадження та супроводження сучасних безпечних технологій; побудова захищеної відомчої інфраструктури; *формування* і розвиток інформаційних стосунків; *мінімізація* та, по можливості, усунення існуючих чи потенційних внутрішніх і зовнішніх загроз розвитку інформаційно-аналітичного забезпечення організації.

Необхідність подальших наукових досліджень обгрунтовується наявністю проблем надійного функціонування систем відомчого інформаційного забезпечення та відомчої системи інформаційної безпеки з урахуванням стрімкого поширення сучасних інформаційних технологій та широких можливостей доступу криміногенних елементів до конфіденційної інформації.

Модель системи антивірусного захисту. Для економічного обґрунтування сучасних систем захисту інформаційних ресурсів розглянемо модель модернізації корпоративної системи антивірусного захисту і системи управління доступом на об'єкті інформатизації (рис. 1). 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 [3, 4].

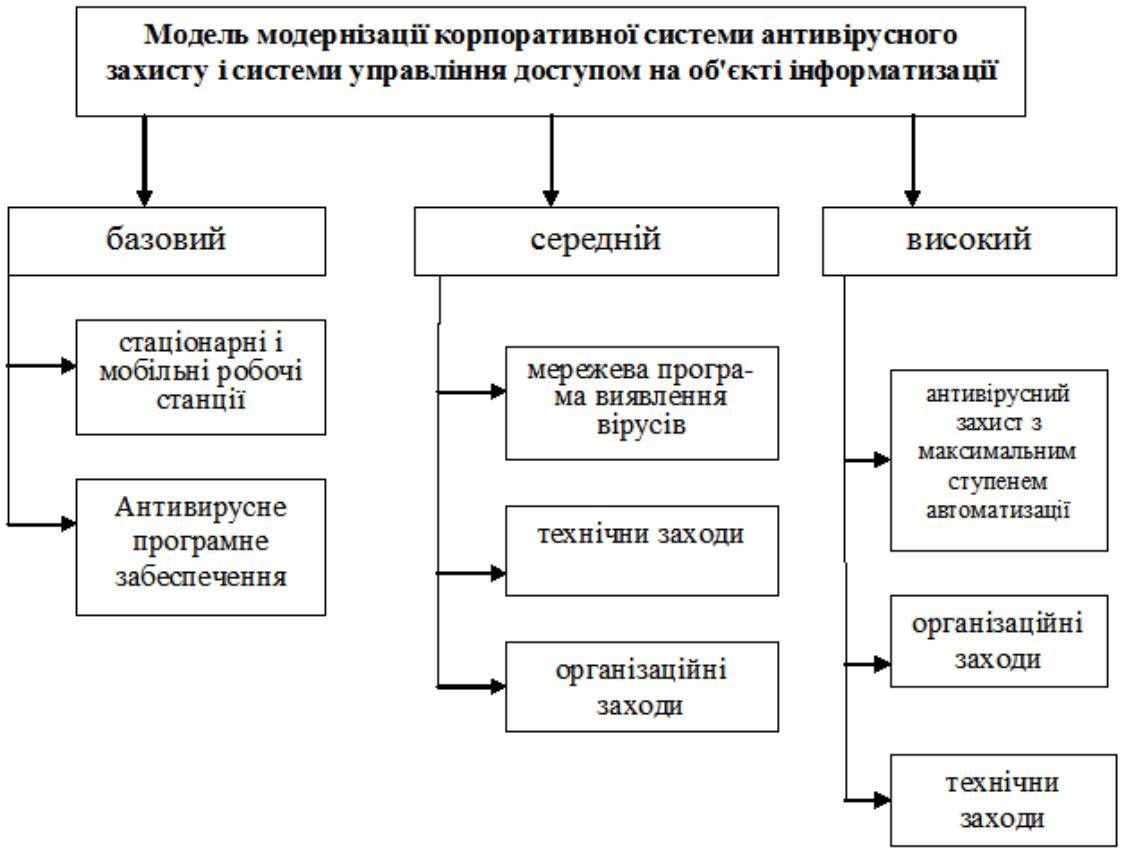

Рис. 1. Модель модернізації корпоративної системи антивірусного захисту

Базовий стан характеризується тим що, стаціонарні і мобільні робочі станції забезпечені локальним захистом від вірусів. Антивірусне програмне забезпечення станцій та бази регулярно оновлюються, встановлюються програми автоматичного знищення вірусів. Основна мета рівня – організація мінімального захисту від вірусів і шкідливого програмного забезпечення при невеликих витратах.

На середньому стані встановлюється мережева програма виявлення вірусів. Здійснюваний на сервері системний контроль програмних оновлювань відстежує появу вірусів в мережі, запобігаючи подальшому розповсюдженню вірусів.

Високий стан реалізується системою антивірусного захисту, яка тісно інтегрована в комплексну систему централізованого управління безпеки інформаційних ресурсів компанії і має максимальний ступінь автоматизації.

Також можна умовно виділити три аналогічні рівні системи контролю і управління доступом в інформаційній системі (забезпечення фізичної безпеки) [4, 5].

На базовому рівні ведеться інвентаризаційний облік робочих станцій, серверів та іншого апаратного устаткування. Постійно ведеться контроль переміщення апаратних засобів, особливо мобільних компонентів інформаційних систем. Сюди відносяться такі організаційні заходи, як періодичні інструктажі персоналу компанії.

На середньому рівні використовуються механічні і електронні замки, шлюзові кабіни і турнікети, організовуються контрольно-пропускні пункти і прохідні, ведеться відеоспостереження. Розробляються та вдосконалюються інструкції по діях персоналу в штатних і позаштатних ситуаціях. Передбачаються заходи по залученню приватних і державних охоронних структур.

Високий рівень забезпечення фізичної безпеки апаратних засобів є частиною єдиної політики безпеки, затвердженій керівництвом компанії, використовується 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 [6, 7].

При цьому можливі декілька варіантів реалізації цих вимог, що характеризуються різними економічними показниками та можуть бути основою раціональної економічної моделі системи інформаційної безпеки об'єкту інформатизації.

Зокрема, модель типової структури витрат за вибраними елементами системи безпеки інформаційних ресурсів насамперед визначає такі позиції:

– *витрати на створення системи безпеки* інформаційних ресурсів у складі таких категорій, як витрати на формування і підтримку ланки управління системою захисту інформації (організаційні витрати);

– *витрати на контроль*, тобто на визначення і підтвердження досягнутого рівня захищеності ресурсів підприємства;

– *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);

– *зовнішні витрати* на ліквідацію наслідків порушення політики інформаційної безпеки. Це компенсація втрат у випадках, пов'язаних з просочуванням інформації, втратою іміджу компанії, втратою довіри партнерів і споживачів.

Економічні аспекти забезпечення інформаційної безпеки. При дотриманні політики інформаційної безпеки та проведенні профілактики порушень можна виключити або істотно зменшити витрати по відновленню системи інформаційної безпеки до відповідності вимогам політики безпеки; відновленню ресурсів інформаційного середовища підприємства; переобладнанню системи інформаційної безпеки; вирішенню юридичних спорів та виплат компенсацій, а також встановленню причин порушення політики інформаційної безпеки.

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

Неминучі витрати можуть включати обслуговування технічних засобів захисту; конфіденційне діловодство; функціонування і 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.

Повністю виключити витрати на інформаційну безпеку неможливо, проте вони можуть бути приведені до прийнятного рівня. Деякі витрати є абсолютно необхідними, деякі можуть бути істотно зменшені або виключені внаслідок скорочення або зникнення загроз порушення інформаційної безпеки системи.

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

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 [8].

Основні напрямки досліджень. 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.

Підводячи підсумок, слід зазначити, що ефективність попереджувальної діяльності у напрямку зниження ризику інформаційній безпеці, яка зазначена в даній моделі, не велика.

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 елементом моделі є визначення цінності інформаційних ресурсів як сукупної вартості власних ресурсів, що виділяються в інформаційному середовищі підприємства. Ресурси зазвичай підрозділяються на декілька класів, наприклад, фізичні, програмні та інформаційні.

Важливим етапом моделювання корпоративної системи інформаційної безпеки об’єкту інформатизації є проведення повного аналізу ризиків, при якому необхідно визначити цінність ресурсів; до стандартного набору додати список загроз, актуальних для досліджуваної системи; оцінити ймовірність загроз; визначити уразливість ресурсів; запропонувати систему захисту інформації, що забезпечує необхідний рівень інформаційної безпеки ресурсів (рис.2).

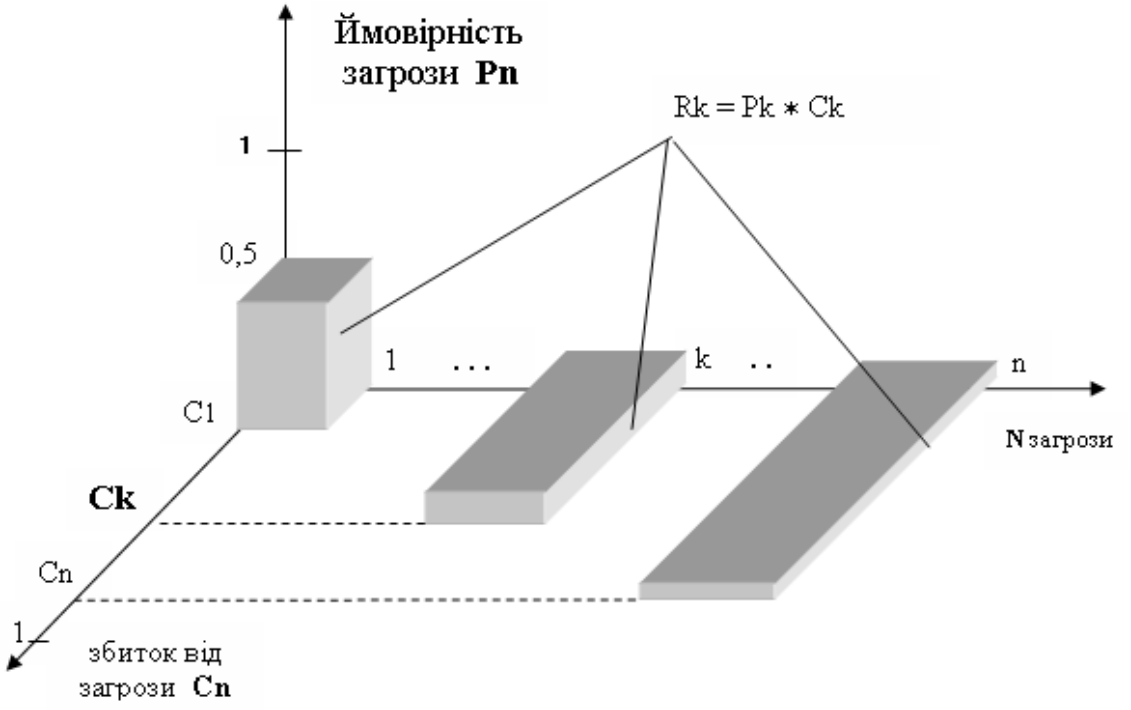

Рис. 2. Визначення збитку в залежності від загрози інформаційній безпеці

У простому випадку, якщо відома ймовірність *Pn* кожної *N*-ої загрози і очікуваний збиток від її реалізації *Cn*, чисельні значення ризиків можуть бути знайдені шляхом перемножування вказаних величин (рис. 2). Звідси видно, що в загальному випадку загроза, що має максимальну ймовірність появи або максимальний збиток від її реалізації, необов'язково має максимальний ризик.

На підставі результатів аналізу виявляються найбільш високі ризики, що переводять потенційну загрозу в розряд реально небезпечних і визначають застосування системи додаткових заходів захисту для зменшення ризику.

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.

Висновки. Таким чином, проведення ретельного аналізу функціонування системи захисту інформації, дозволить більш ефективно застосовувати попереджувальні заходи для механізмів інформаційного захисту з оптимальною витратною частиною [7 9].

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.

Література

1. Бойченко О. В. Моделювання сучасних систем захисту інформаційних ресурсів / О. В. Бойченко // Вісник Національного авіаційного університету. – Київ, 2009. – Вип. 1. – С. 201-204.

2. Бойченко О. В. Інформаційна безпека в органах внутрішніх справ України (організаційо-правові засади) / О. В. Бойченко. – Сімферополь: ВАТ «Сімферопольська міська друкарня» (СГТ), 2009. – 288 с.

3. Галатенко В. А. Основы информационной безопасности: учебник / В. А. Галатенко. – С-Пб.: Питер, 2006. – 204 с.

4. Бойченко О. В. Обмін даними в автоматизованій системі управління органів внутрішніх справ / О. В. Бойченко. – Сімферополь: «ДІАЙПІ», 2010. – 186 с.

5. Галатенко В. А. Стандарты информационной безопасности: монография / В. А. Галатенко. – С-Пб.: Питер, 2006. – 236 с.

6. Губенков А. А. Информационная безопасность: монографія / А. А. Губенков, В. Б. Байбурин. – М.: Радио и связь, 2005. – 308 с.

7. Кечиев Л. Н. ЭМС и информационная безопасность в системах телекоммуникаций: монография / Л. Н. Кечиев, П. В. Степанов. – М.: Мысль, 2005. – 269 с.

8. Мельников В. В. Безопасность информации в автоматизированных системах: монография / В. В. Мельников. – М.: Лучшие книги, 2003. – 264 с.

9. Скотт В. Разработка правил информационной безопасности: монография / Скотт В. – М.: АйТи-Пресс, 2002. – 109 с.