УДК 004(075.8)

Informatics and Mathematical Methods in Simulation
Vol. 5 (2015), No. 3, pp. 289-297

МОДЕЛЬ ОЦІНКИ ЕФЕКТИВННОСТІ ЗАХИСТУ ПРОГРАМНОГО КОДУ ВІД НЕСАНКЦІОНОВАНИХ ЗМІН

А.Є. Кілін[1], В.Г. Кононович[1], І.В. Кононович[2], В.В. Беззубенко[3]

[1] Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна; e-mail: vl_kononovich@ukr.net
[2] Одеська національна академія харчових технологій,
вул. Канатна, 112, м. Одеса, 65039, Україна; e-mail: kononovich@mail.ru
[3] Одеська національна академія зв'язку,
ул. Кузнечная, 1, Одесса, 65021, Украина; e-mail: vladimirbezzubenko@gmail.com

В роботі пропонується, додатково до існуючих, механізм захисту програмного коду від несанкціонованого змінювання. На цьому прикладі вдосконалюється загальна модель оцінки ефективності системи захисту. Алгоритм захисту заснований на стеганографічних підходах. Оцінка ефективності захисту проводиться за допомогою моделі вибору оптимального рівня захищеності за принципом «витрати на захист – ефективність». При цьому формалізуються типові залежності відшкодування збитків від рівня захищеності та залежності витрат на побудову системи безпеки від того ж рівня захищеності. Доводиться, що в загальному випадку доцільно обирати функцію Ципфа для залежності відшкодування збитків від рівня захищеності та одну з гіперболічних функцій для залежності витрат на побудову системи безпеки від того ж рівня захищеності. Введення названих функцій в модель вибору оптимального рівня захищеності дозволила перейти від якісних оцінок витрат на організацію системи безпеки до конкретних обчислень при математичному експерименті. Вдосконалена модель захисту та загальної оцінки ефективності системи захисту дозволить обгрунтовувати доцільність підвищення рівня захищеності програмного коду.

Ключові слова: захист програмного коду, несанкціоновані зміни, оцінка ефективності, рівень захищеності, моделювання, математичний експеримент.

Вступ

Дана робота відноситься до сфери забезпечення авторських прав на корисні моделі – програмне забезпечення і розглядає проблеми застосування та оцінки ефективності алгоритмічних і стеганографічних методів у комплексах захисту програмного коду від несанкціонованих змін.

Загальні методи та принципи захисту програмного коду розглянуті у відомій монографії [1]. Питання захисту програм від несанкціонованого тиражування, застосування стеганографії, аналізу засобів захисту та інструментів, які застосовуються при дослідженнях, а також методи оцінки ефективності захисту, розглянуті у [2]. Спостерігається вал науково-технічних матеріалів та пропонованих застосувань захисту програмного коду. З останніх робіт відмітимо [3; 4], де розглядається комбінований захист програмного забезпечення від несанкціонованих впливів та методи захисту програмного коду. Методи аналізу програм, захисту від аналізу та інструментарії виявлення змін викладені у навчальному посібнику [5]. Навики дослідження коду зловмисного програмного забезпечення, необхідні для розробки протидії, розглядаються в [6].

Класичною роботою по управлінню інформаційними ризиками та знаходженню економічно виправданої безпеки є книга [7]. Але залежності витрат на побудову

системи безпеки та залежності відшкодування збитків від досягнутого рівня захищеності досліджені недостатньо. Наприклад, витрати на компенсацію порушень політики безпеки вважаються лінійно залежними від рівня захищеності. Тому формалізація вказаних залежностей є актуальною задачею.

Метою роботи є розроблення стеганографічного, додаткового до алгоритмічних, механізму захисту програмного коду від несанкціонованих змін і вдосконалення моделі оцінки його ефективності за принципом оптимізації витрат на захист шляхом формалізації типових залежностей витрат на запобіжні заходи захисту та залежності витрат на відновлення втрат від рівня захищеності.

Стеганографічний спосіб захисту програмного коду

Для підвищення рівня захищеності програмного коду в комплексі системи захисту від несанкціонованих змін, додатково до існуючих засобів захисту, пропонується механізм захисту, заснований на стеганографічних методах. Основною метою тут є як захист від несанкціонованих змінень, так і захист самого коду. Наприклад, ми винайшли певний алгоритм і хочемо випускати програму, яка його використовує. Але при цьому ми хочемо, щоб сам алгоритм залишився секретом. Для цього нам необхідно цей алгоритм приховати всередині нашої програми. Вирішення цієї проблеми, у свою чергу, також веде до захисту від несанкціонованих змінень. Цей наслідок витікає із факту, що сам доступ до коду та, відповідно, змінення утруднені. Суть методу полягає в наступному.

Ділянки коду, що становлять підвищену цінність, будемо вбудовувати у стеганоконтейнер. У ролі стеганоконтейнеру можуть виступати звичайні зображення, які у наш час є у багатьох програмних продуктах. Прихований код буде динамічно вийматися, компілюватися та виконуватися під час роботи програми. Таким чином, такий код буде існувати в його початковому вигляді лише під час виконання програми у динамічній пам’яті.

У якості стеганографічного метода добре підходить метод найменшого значущого біту, через його високу пропускну спроможність.

Модель оптимізації системи захисту за принципом «мінімізація витрат – ефективність»

Якісну модель оптимізації системи захисту інформаційного середовища підприємства за принципом «мінімізація витрат – ефективність» описав у своїй книзі Петренко [7]: «Взаємозв’язок між усіма витратами на безпеку, спільними витратами на безпеку та рівнем захищеності інформаційного середовища підприємства може бути представлена так, як це зображено на рис. 1.

Загальні витрати на безпеку складаються із витрат на запобіжні заходи, на контроль та відновлювання втрат (внутрішніх і зовнішніх). Із зміною рівня захищеності інформаційного середовища змінюються величини складових спільних витрат і, відповідно, їх сума – спільні витрати на безпеку».

Графіки побудовані із врахуванням наступних допущень: по-перше, при виконанні робіт по попередженню порушень політики безпеки (ППБ) у першу чергу виконуються роботи, які дають найбільший ефект по захисту інформаційного середовища; по-друге, залежності й активність атак не змінюються у часі, тоді економічний баланс не міняється.

Застосуємо дану якісну модель для оцінки ефективності механізму захисту програмного коду. Для цього проведемо і обґрунтуємо формалізацію складових залежностей для певних типових випадків. Крім того, необхідно дати відповідну

інтерпретацію моделі. «Будемо розглядати залежності витрат від відносного рівня захищеності x, який змінюється від 0 до 1. При цьому, $x=0$ відповідає незахищеній системі; $x=1$ відповідає високому рівню захищеності системи; $x<1$ означає, що абсолютно захищених систем у природі не існує.

Величина витрат – y також є відносною, що змінюється у інтервалі від 0 до 1. При визначенні відношення затрат на безпеку використовують яку-небудь базу вимірювань. Типовими базами вимірювання можуть бути: обсяг проданої продукції, якщо він не залежить від сезонних факторів або інших циклічних змін; обсяг виробництва; трудоємність, що представляється як величина оплати праці, безпосередньо витраченої на виробництво продукції, якщо вона має стабільний характер; обсяг ресурсів інформаційного середовища підприємства, тобто сукупна вартість власних ресурсів, які виділяються інформаційному середовищу підприємства, або величина витрат на заміну або відновлення працездатності тощо. База вимірювань не повинна залежати від поліпшення технологій, автоматизації виробничих процесів, зміни обслуговуючого персоналу. Порівнювані величини повинні братись у їх вартісному вираженні [7]».

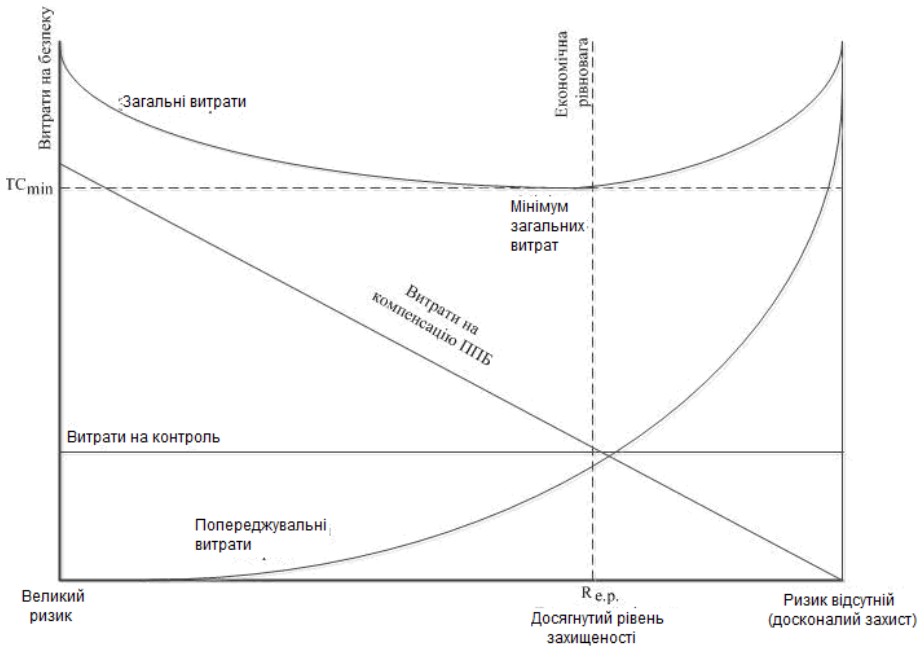

Рис.1. Модель оптимальних витрат на захист інформаційного середовища підприємства (модель запозичена із [7, рис. П7.4]

Витрати на компенсацію наслідків несанкціонованої зміни програмного коду. По суті ці витрати можна оцінювати величиною збитків від несанкціонованої зміни програмного коду. На рис. 1 ця залежність (витрати на компенсацію ППБ від рівня захищеності) лінійна. Це досить грубе наближення. В нашому випадку в реалізації загроз найбільше значення має людський фактор. Взаємодія людини з навколишнім середовищем має нелінійний характер. Реакція людини (її зору, слуху, нюху тощо) пропорційна логарифму подразнення. Скоріше за все, сприймання людиною рівня загроз або рівня витрат теж є нелінійним. Тому математичні формули для типових залежностей необхідно шукати серед стійких статистичних розподілів і залежностей. Такі розподіли дозволяють передбачати результати майбутніх випробувань у масових випадкових явищах.

Класичним є «нормальний розподіл», що випливає із закону великих чисел. У теорії ймовірностей існує центральна гранична теорема (теорема Ляпунова), що стосується граничних законів розподілу суми випадкових величин. Згідно цієї теореми

сума незалежних випадкових величин x_i $(i=1,2,\ldots,n)$, які мають будь-який розподіл, наближаються до нормального при необмеженому збільшенні величини n, якщо виконуються наступні умови: 1) всі величини мають скінчені математичні очікування m_i та дисперсії $M((x_i-m_i)^2)=D_i=\sigma_i^2$; 2) ні одна з величин по значенню різко не відрізняється від інших. Останнє породжує правило обробки статистичних даних, за якого найбільше та найменше значення відкидаються. Сказане означає, що кандидатом для формалізації залежності між нормованою величиною збитків при несанкціонованій зміні програмного коду та рівнем захищеності може служити нормальний (гаусів) розподіл при $m=0$:

$$y_1=\varphi(x)=\frac{k}{\sigma\sqrt{2\pi}}\exp\left(-x^2/2\sigma^2\right),\ x=\overline{0,1}, \qquad (1)$$

де k – нормуючий коефіцієнт; σ – середньоквадратичне відхилення.

Але, незважаючи на широке розповсюдження нормального розподілу у науці й техніці, цей розподіл не підходить до опису згаданих залежностей. По-перше, пряма лінія на рис.1 більше підходить до опису залежності між нормованою величиною збитків та рівнем захищеності, ніж крива Гауса. По-друге, ця крива не може описувати соціальні явища в силу їх «негаусовості». Цей феномен пояснюється далі.

Другим кандидатом для формалізації залежності між нормованою величиною збитків та рівнем захищеності може служити експоненціальна функція

$$y_2(a,x)=\exp(-ax),\ x=\overline{0,1}, \qquad (2)$$

де a – параметр.

Експоненціальна функція має важливу властивість. Швидкість зміни експоненціальної функції пропорціональна значенню функції у цій точці. Завдяки цьому, вона застосовна для опису багатьох природних процесів. У даному разі експоненціальна функція показує, що зі збільшенням рівня захищеності втрати зменшуються. При $x=1$, $y(x)>0$. Це певною мірою відповідає реальній ситуації. Абсолютно захищених систем не буває. І при високому рівні захищеності можливі втрати.

Теоретично можливі ситуації, коли подія наступає, але це відбувається рідко, потенційна шкода невелика і тоді приймається рішення не захищатись від такої загрози. Можливі також загрози непереборної сили – стихійні лиха, теракти тощо. Експоненціальну функцію відбираємо для подальшого експериментального дослідження.

Останнім часом розвинуті теорії негаусових процесів, які можуть бути кращими кандидатами для формалізації залежностей. Стаціонарні розподіли значень змінних, у своїй масі, є не гаусовими, тобто не можуть бути описані розподілом Гауса та іншими гаусовими розподілами, що підпорядковуються центральною граничною теоремою теорії ймовірностей. За великих значеннях змінної воно має гіперболічну форму розподілу Ципфа, а в логарифмічних координатах розподіл Ципфа має вид прямої лінії. Ципфовими називають всякі розподіли, які мають при великих значеннях змінної вид розподілу Ципфа [9].

Негаусовість є загальною властивістю просторових та непросторових фрактальних структур. Негаусовими є часові структури, які утворюються відносно рідкими подіями, необмеженими у часі. Події, обмежені у часі, навпаки, розподілені більш гаусово. Там, де не існує обмежень значень змінної, розподіл виявляється негаусовим. Негаусові розподіли є більш поширеними, ніж гаусові. Наведемо деякі теоретичні відомості [10].

«Кількісні шкали поділяють на відкриті та закриті у залежності від того, чи обмежені зверху відносні значення вимірюваної величини. У випадку обмежених шкал, згідно центральної граничної теореми Ляпунова, отримують гаусові (нормальні) розподіли. Обмеження може бути із-за процедури вимірювання, наприклад, при визначенні тестових балів. Гранична теорема Гнеденко – Дебліна визначає умови для наближення розподілу нормованих сум однакового розподілених незалежних випадкових величин до стійких негаусових розподілів. Статистичні стаціонарні розподіли, які отримані за допомогою відкритих (необмежених) шкал, здебільшого мають довгі хвости, що описуються розподілом Ципфа (Парето):

$$y_3(\alpha, x) = \frac{C}{x^{1+\alpha}},\ 0 < x_0 \le x \le J,\ 0 < \alpha < \infty, \tag{3}$$

де $y_3(x)$ – частість; α – показник розподілу Ципфа, який визначає його форму: чим α менше, тим більш довгохвостий даний розподіл; C – параметр, який забезпечує нормування відносно обсягу вибірки; x_0 та J – мінімальне та максимальне вибіркове значення x. Значення параметра α, як правило, невеликі».

Для розподілу Ципфа характерно відсутність математичного очікування; m наближається до нескінченності. Критерієм гаусовості чи негаусовості цих розподілів служить зміна величини дисперсії. Якщо на даній генеральній сукупності дисперсія (та моменти вищих порядків) суттєво зростає з об'ємом вибірки, то таку сукупність називають негаусівською, у іншому випадку – гаусівською.

На основі теореми Гнеденко-Дебліна можна говорити, що ймовірнісні негаусові розподіли є ципфовими розподілами з $\alpha < 2$, тоді як ципфовий розподіл з $\alpha > 2$ є гаусовим. Використання ципфового розподілу для формалізації залежності між нормованою величиною збитків та рівнем захищеності доцільно по таким причинам. Ципфовий розподіл характеризується різким спадом (більш крутим ніж у експоненти) і довгим хвостом. Крутий спад відповідає реальним даним по величині збитків. Невеликий початковий приріст захищеності викликає знаний спад активності зловмисників. Авторами доведено, що лише об'ява про забезпеченість захисту об'єкта зменшує число зловмисників на 80% [8]. Відомості щодо наявності захисту відсікає значну частину законослухняних споживачів від спроб незаконного використання продукту.

Витрати на запобіжні заходи захисту від несанкціонованої зміни програмного коду. Аналогічним способом розглянемо застосування показникової та параболічної функції. Для формалізації залежності між нормованою величиною витрат на запобіжні заходи та рівнем захищеності може служити експонента

$$y_4(b, x) = \exp(b(x-1)),\ x = \overline{0,1}, \tag{4}$$

де b – параметр.

Ряд процесів у природі (радіоактивний розпад, зростання кількості бактерій за певний проміжок часу тощо) описуються експонентою. Функція (4) зручна для формалізації тому, що при $x = 0$ вона: $y_4(b,0) > 0$. Рівень захищеності починає зростати при певних початкових витратах, коли задіяна певна мінімальна функціонально повна множина заходів захисту. Наприклад тоді, коли повністю змонтовані всі елементи огорожі об'єкта.

Другим кандидатом для формалізації залежності між нормованою величиною витрат на запобіжні заходи та рівнем захищеності може служити параболічна функція

$$y_5(b,x) = bx^2,\ x = \overline{0,1}, \tag{5}$$

де b – параметр.

Парабола представляє собою найпростішу нелінійну функцію і має широке застосування у різних сферах, зокрема, у синергетиці. Для остаточного вибору типових функцій розподілу витрат на безпеку необхідні статистичні дані щодо цих витрат. Що стосується вибору таких функцій стосовно до конкретних об'єктів інформаційної діяльності, то вони можуть мати вельми специфічний характер.

Математичні експерименти із розподілами

Виявлення причин нанесення втрат, прийняття попередніх запобіжних заходів захисту, заходи підвищення рівня захищеності інформаційної системи повинні переслідувати мету – з найменшими витратами досягти найбільших результатів. Має сенс дослідити, як виглядають оптимальні витрати на оптимальну систему захисту у випадку, коли розглянуті розподіли матимуть місце у реальності. Постановка задачі формулюється так. Треба побудувати у трьохмірному просторі залежність

$$Y(a,b) = \min\left(y_i(a,x) + y_j(b,x)\right). \tag{6}$$

Із цієї побудови можна судити про можливий мінімум витрат на інформаційну безпеку. Інтервали змін параметрів a і b підбираються експериментально.

На рис. 2 представлені результати математичного експерименту, відповідно, для функцій $y_2(a,x)$ та $y_4(b,x)$. По осі z відкладається значення функції (6), по осям a і b відкладені, відповідно, параметри функцій (2) і (4).

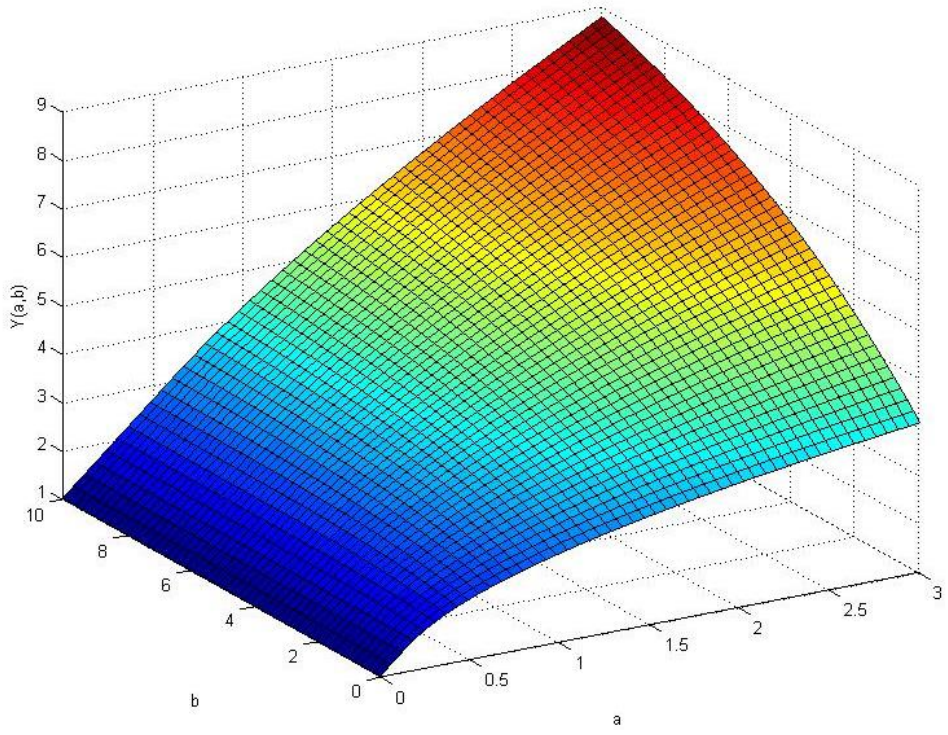

Рис.2. Розподіл оптимальних витрат на захист при експоненціальних функціях залежностей ризиків від витрат та затрат на захист

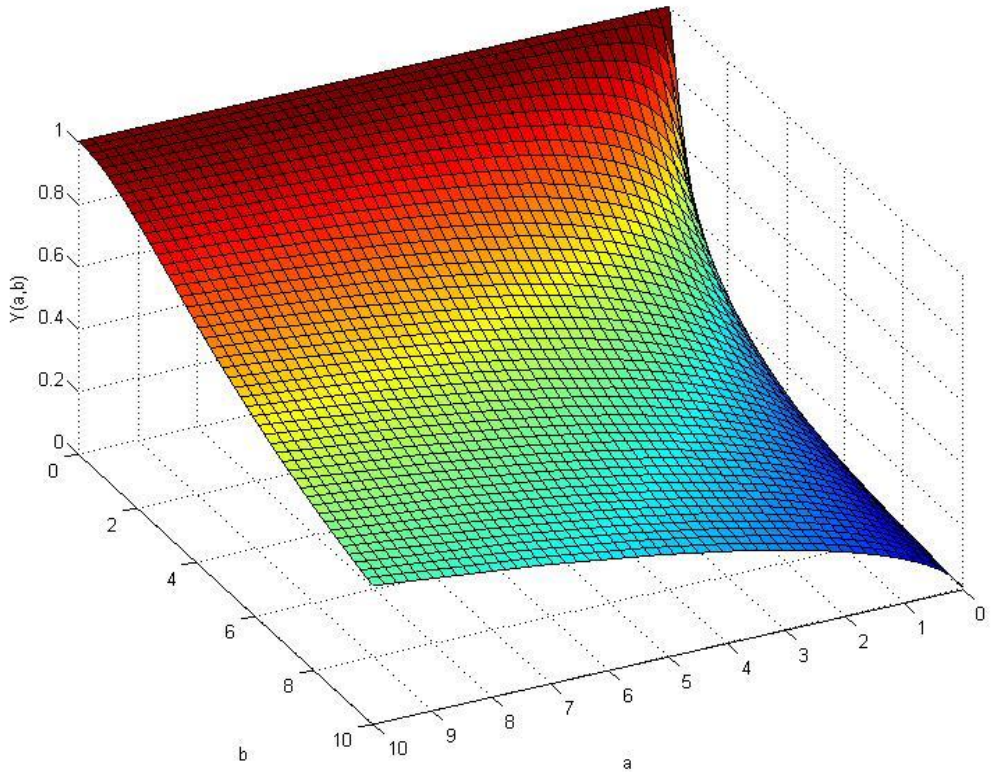

Рис. 3. Розподіл оптимальних витрат на захист при цапфових та експоненціальних функціях залежностей ризиків, відповідно, від витрат та затрат на захист

На рис. 3 представлені результати математичного експерименту, відповідно, для функцій $y_3(a,x)$ –ципфовий розподіл та $y_4(b,x)$ – експоненціальний розподіл. По осі z відкладається значення функції (6), по осям a і b відкладені, відповідно, параметри функцій (3) і (4).

Критерієм вибору функцій, придатних для формалізації залежності між нормованою величиною збитків (або витрат на систему захисту) та рівнем захищеності може служити наступний достовірний факт. Практикою доведено, що раціональна доля витрат на інформаційну безпеку можуть складати від 2% до 20% від обсягу продаж (або обороту). Більша доля витрат неефективна, бо знижує продуктивність основних виробничих функцій.

Висновки

В даній роботі розроблено стеганографічний, додатковий до алгоритмічних, механізм захисту програмного коду від несанкціонованих змін. Вдосконалена загальна модель оцінки ефективності системи захисту за принципом оптимізації витрат на захист. Проведена формалізація типових залежностей витрат на запобіжні заходи захисту та залежності витрат на відновлення втрат від рівня захищеності. Напрямком подальших досліджень повинні бути експериментальні дослідження статистики реальних витрат на інформаційну безпеку.

Список літератури

1. Казарин, О.В. Безопасность программного обеспечения компьютерных систем. Монография / О.В. Казарин. – М.: МГУЛ, 2003. – 212 с.
2. Скляров, Д.В. Искуство защиты и взлома информации / Д.В. Скляров. – СПб.: БХВ-Петербург, 2004. – 288 с. .
3. Десницкий, Д.А. Комбинирванная защита программного обеспечения от незанкционированных воздействий / Д.А. Десницкий, И.В. Котенко // Изв. вузов. Приборостроение. – 2010. – Т.53. – №11. – С. 36-41.
4. Петров, А.С. Методы защиты програмного кода / А.С. Петров, А.А. Петров // Системи обробки інформації. – 2010. – № 3 (84). – С. 68-71.
5. Проскурин, В.Г. Защита программ и данных: уч. пособие / В.Г. Проскурин. – М.: Издательский центр «Академия», 2012. – 208 с.
6. Федоров, Д.Ю. Основы исследования безопасности программного обеспечения / Д.Ю. Федоров. – СПб.: СПГИЭУ, 2012. – 68 с.
7. Петренко, С. А. Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. – М.: Компания АйТи; ДМК Пресс, 2004. – 384 с.
8. Кононович, В.Г. Визначення ідентичності об'єктів у системі соціальної та інформаційної безпеки / В.Г. Кононович, І.В. Кононович, С.В. Стайкуца, О.О. Цвілій // Сучасний захист інформації. – 2015. – №1. – С. 19-27.
9. Яблонский, А.И. Математические модели в исследованиях науки / А. И. Яблонский. – М.: Наука, 1986. – 352 с.
10. Хайтун, С.Д. Феномен человека на фоне универсальной эволюции / С. Д. Хайтун. – М.: Книжный дом «ЛИБРОКОМ», 2009. – 536 с.

МОДЕЛЬ ОЦЕНКИ ЭФФЕКТИВННОСТИ ЗАЩИТЫ ПРОГРАММНОГО КОДА ОТ НЕСАНКЦИОНИРОВАННЫХ ИЗМЕНЕНИЙ

А.Е. Килин[1], В.Г. Кононович[1], И.В. Кононович[2], В.В. Беззубенко[3]

[1] Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: vl_kononovich@ukr.net
[2] Одесская национальная академия пищевых технологий,
ул. Канатная, 112, м. Одесса, 65039, Украина; e-mail: kononovich@mail.ru
[3] Одесская национальная академия связи,
ул. Кузнечная, 1, Одесса, 65021, Украина; e-mail:vladimirbezzubenko@gmail.com

В данной работе предлагается, дополнительно к существующим, механизм защиты программного кода от несанкционированного изменения та. На этом примере, усовершенствуется общая модель оценки эффективности системы защиты. Алгоритм защиты основан на стеганографических подходах. Оценка эффективности защиты проводится с помощью модели выбора оптимального уровня защищенности за принципом «затраты на защиту – эффективность». При этом формализуются типовые зависимости компенсации убытков от уровня защищенности и зависимости затрат на построение системы безопасности от того же уровня защищенности. Доказывается, что в общем случае целесообразно выбирать функцию Ципфа для зависимости компенсации убытков от уровня защищенности и экспоненциальную либо гиперболическую функцию для зависимости затрат на построение системы безопасности от того же уровня защищенности. Введение названых функций в модель выбора оптимального уровня защищенности позволила перейти от качественных оценок затрат на организацию системы безопасности к конкретным вычислениям при математическом экспериментировании. Усовершенствованная модель защиты и общей оценки эффективности системы защиты позволит обосновывать целесообразность повышения уровня защищенности программного кода.

Ключевые слова: защита програмного кода, несанкционированные изменения, оценка эффективности, уровень защищенности, моделирование, математический эксперимент.

MODEL EVALUATION OF THE EFFECTIVENESS OF PROTECTION CODE FROM UNAUTHORIZED CHANGES

A.E. Kilin[1], V.G. Kononovich[1], I.V. Kononovich[2], V.V. Bezzubenko[3]

[1] Odessa National Politechnic University
1, Shevchenko Ave, Odessa, 65044, Ukraine; e-mail: vl_kononovich@ukr.net
[2] Odessa National Academy Food Technologies
112, Kanatnaja str., Odessa, 65039, Ukraine; e-mail: kononovich@mail.ru
[3] Odessa National Academy telecommunikation,
1, Kuznechnaja str., Odessa, 65021, Ukraine; e-mail: vladimirbezzubenko@gmail.com

The additional mechanism of protection of programmatic code from the unauthorized change is offered in this work. The algorithm is based on steganographic techniques. Improving overall model of evaluation efficiency of the system protection. A model of choice of an optimum level of protection for the principle of "protection costs – efficiency." This formalized depending on the level of compensation for losses and security costs depending on the construction of the security system on the level of security. It proved the expediency of the function according to Cypf for compensation of losses from the level of protection and an exponential or hyperbolic function for the dependence of the cost of protection. Using these functions allowed to pass from qualitative assessments of the cost of protection to computing in mathematical experimentation. Advanced security model and an overall assessment of the effectiveness of the protection system allows you to substantiate the expediency of improving the security code.

Keywords: protection of software code, unauthorized modifications, performance evaluation, the level of security, modeling, mathematical experiment.