Визначені основні параметри загроз інформаційним об'єктам систем передачі та обробки інформації, а також приведений загальний підхід до побудови формальної моделі загроз, що дозволяє здійснювати вибір функціональних послуг захисту

Ключові слова: інформація, профіль, захист, параметр, безпека

Определены основные параметры угроз информационным объектам систем передачи и обработки информации, а также приведен общий подход к построению формальной модели угроз, что позволяет осуществлять выбор функциональных услуг защиты

Ключевые слова: информация, профиль, защита, параметр, безопасность

УДК 681.14

ПРИНЦИПИ ВИБОРУ ФОРМАЛЬНИХ ПАРАМЕТРІВ ПРИ ПОБУДОВІ ПРОФІЛЕЙ ЗАХИСТУ ІНФОРЕСУРСІВ

Ю.В. Щербина
Кандидат технічних наук, доцент*
Контактний тел.: 096-519-46-01
E-mail: fleshka_04@ukr.net
С.Л. Волков
Кандидат технічних наук, завідувач кафедрою
Кафедра інформаційно-вимірювальних технологій
Одеська державна академія технічного регулювання та якості
ул. Ковальска, 15, м. Одеса, Україна, 65029
Контактний тел.: 050-316-71-14
E-mail: greyw@ukr.net
О.О. Скопа
Доктор технічних наук, доцент*
Контактний тел.: (048) 703-64-23, 050-504-17-81
E-mail: skopa2003@ukr.net
*Завідувач кафедри інформаційних систем в економіці
Одеський національний економічний університет
вул. Преображенська, 8, м. Одеса, Україна, 65082

Постановка проблеми у загальному вигляді та її зв'язок з важливими науковими та практичними завданнями

У останні десятиліття спостерігається тенденція повсюдного переходу до безпаперового документообігу, заснованого на використанні розподілених обчислювальних систем. Це пояснюється високим рівнем автоматизації технологічних процесів, які забезпечують доставку інформації до абонентів, широким розповсюдженням сучасних технологій накопичення, зберігання та обробки інформації, а також застосуванням цифрових методів обробки сигналів. У цих умовах вимоги до коректності інформаційних процесів, що протікають в системах передачі та обробки інформації, постійно ростуть і для їх задоволення доводиться створювати системи захисту інформації, здатні протистояти зовнішнім та внутрішнім загрозам. Враховуючи високу вартість такого роду систем, виникає необхідність щодо приймання спеціальних заходів для підвищення їх ефективності, яка, в першу чергу, визначається правильним врахуванням ризиків від реалізації загроз, що мають місце в умовах експлуатації. Це робить завдання створення методології оцінки загроз інформаційним ресурсам особливо актуальним.

Мета досліджень

Створення методології, яка позначена вище, є складним завданням. Ця складність пояснюється, по-перше, суб'єктивним підходом до оцінки вартості самих інформаційних об'єктів і, по-друге, постійною зміною середовища експлуатації систем, які підлягають захисту. Обидві ці обставини визначають необхідність постійного моніторингу стану безпеки системи та актуальності загроз, виявлених на момент введення її в експлуатацію.

Аналіз досліджень та публікацій

Останніми роками проблемі вироблення методології оцінки загроз інформаційним ресурсам було присвячено достатньо багато публікацій, проте більшість з них найчастіше відображає підхід до рішення часткових завдань.

Крім того, одні й ті ж терміни не завжди однаково розуміються різними авторами. Звідси витікає ще одна проблема, яка пов'язана з відсутністю строгого закріплення відповідних понять, пов'язаних з діяльністю з захисту інформації в нормативно-правових актах, регулюючих відносини між замовниками та розробниками засобів її захисту.

У зарубіжній нормативній базі досить добре прописана процедура аналізу ризиків, тобто приводиться послідовність обов'язкових етапів, які виконуються при оцінці загроз. До них найчастіше відносять:

– *визначення меж системи, яка підлягає захисту;*

– *визначення переліку інформаційних об'єктів, які необхідно захищати;*

– виявлення слабких місць в системі захисту та переліку загроз;

– оцінка ризиків від окремих типів загроз;

– визначення функціональних послуг захисту;

– визначення залишкових ризиків.

Невирішені проблеми

До поточного моменту в Україні відсутні точні нормативно закріплені методики оцінки захищеності автоматизованих систем, а також методики побудови формальних моделей загроз, на підставі яких може робитися висновок про дійсний рівень такої захищеності. Як наслідок, розробникам системи захисту надається достатня свобода дій.

Мета статті

Відповідно до прийнятої в Україні термінології [1], поняття «Модель загроз» припускає формальний або неформальний опис методів її реалізації. Враховуючи, що при складанні профілю захисту функціональні послуги захисту вибираються з переліку, обумовленого нормативним документом [2], формальною моделлю загроз повинен бути такий набір параметрів, який дозволяв би розробникові оптимальним чином вибирати послуги захисту з пропонованого переліку.

Виклад основного матеріалу

До того як визначити модель загроз, важливо відмітити, що ж є інформаційним об'єктом, що вимагає захисту. Далі, під *інформаційними об'єктами* розумітимемо джерела/приймачі інформації, а також інформаційні потоки безвідносно до їх фізичних носіїв [3]. Це означає, що реальними об'єктами, які підлягають строгому обліку, є файли, які зберігаються в різних видах пам'яті, та дані, що зберігаються в апаратній частині інтерфейсів використовуваної обчислювальної системи. Останні можуть бути ідентифіковані своїми адресами портів. Всі вони повинні бути класифіковані, описані та строго враховані.

Із сказаного випливає, що роботи по формуванню моделі загроз повинні починатися з просторової та функціональної структуризації системи, що захищається. Модель повинна задавати багаторівневі координати будь-якого з об'єктів, що ідентифікується. Просторова структуризація системи припускає виділення локальних середовищ – окремих частин системи, які розташовані в окремих будівлях або приміщеннях і вимагають своїх особливих засобів захисту. Глибина такої структуризації визначається вибраним рівнем гарантій захищеності. Функціональна структуризація припускає розділення системи на функціональні підсистеми, які, у свою чергу, повинні бути структуровані до рівня конкретних засобів або програм, що виконують різноманітні функції.

Коротко оцінимо якість проведеної декомпозиції автоматизованої системи, що підлягає захисту.

Для того, щоб можна було вибрати засіб захисту від загрози, вона повинна бути оцінена кількісно. У якості такої оцінки, зазвичай, використовують показник ризику [1], що визначається як функція вірогідності реалізації конкретної загрози, а також вигляд та величина нанесеного збитку. У простому випадку, ризик можна представити як $W = P_y C_i$, де P_y – вірогідність вдалої атаки на і -й інформаційний об'єкт, C_i – вартість даного об'єкту у відносних одиницях, визначувана замовником.

Оскільки точної й об'єктивної процедури визначення вартості інформаційних об'єктів не існує навіть при кваліфікованій експертизі, пропонується вибирати за одиницю вартість найменш цінного об'єкту (з погляду власника системи), який вимагає захисту, а вартість решти об'єктів визначати по відношенню до нього.

Оцінка вартості кожного інформаційного об'єкту, що підлягає захисту, повинна бути комплексною. Це значить, що необхідно враховувати залежність між різними інформаційними об'єктами, оскільки доступ, отриманий зловмисником до деякого інформаційного об'єкту, може побічно впливати на безпеку інших, пов'язаних з ним об'єктів. Такий облік повинен виконуватися відповідно до наступного правила:

– комплексна вартість оцінюваного об'єкта дорівнює звичайній вартості, якщо пов'язані з ним об'єкти мають меншу вартість;

– комплексна вартість об'єкта рівна сумі його власної вартості та величині, яка характеризує ступінь залежності об'єктів, помноженої на вартість залежного об'єкту, якщо вартість залежного об'єкту більше вартості оцінюваного об'єкту.

Це правило може бути виражене таким чином:

$$C_k = C_0 + \sum_i^n \lambda_i C_{CB_i}, \text{ для всіх } C_{CB_i} > C_0;$$

$$C_k = C_0, \text{ для всіх } C_{CB_i} < C_0,$$

де C_k – комплексна оцінка об'єкту, предмета захисту, C_0 – звичайна оцінка об'єкту, предмета захисту, C_{CB_i} – звичайна оцінка об'єкту, пов'язаного з об'єктом, який розглядається в даний момент λ_i – коефіцієнт, що характеризує зв'язок між об'єктами.

Найчастіше загрози класифікуються по вигляду нанесеного збитку: *порушенню конфіденційності, цілісності* або *доступності*. З цього слідує, що одна й та ж загроза може бути реалізована різними сценаріями атак. Під атакою, зазвичай розуміють цілеспрямовану послідовність дій, що приводять до реалізації загрози. Сценарій атаки припускає використання слабкого місця (уразливості) в системі захисту. Наявність декількох слабких місць припускає можливість реалізації різних сценаріїв атак. Відповідно, при визначенні ризиків від реалізації загроз, необхідно враховувати їх загальну вірогідність реалізації. Якщо допустити, що в деякий момент часу реалізується лише один з можливих сценаріїв, то загальна вірогідність може бути визначена так:

$$P_y = \sum_{j=1}^{m} P_j^A (1-P_1^A)(1-P_2^A)...(1-P_{j-1}^A)(1-P_{j+1}^A)...(1-P_m^A),$$

де m – загальна кількість можливих атак на даний інформаційний об'єкт, P_j^A – вірогідність успішної реалізації j -ї атаки.

Визначення вірогідності реалізації атак – одне з найбільш відповідальних завдань. Окремо повин-

ні бути оцінені умисні та ненавмисні загрози, а також загрози, здійснювані із зовнішнього середовища, та внутрішні загрози. В кожному випадку повинне бути передбачене застосування окремої методики з залученням фахівців в цій області. Таку методику розробник системи захисту може мати свою або може скористатися готовим пакетом прикладних програм на власний вибір. Початкові дані для визначення вірогідності загроз отримуються від власника системи або від організацій, що професійно займаються діяльністю в даній області.

Коли ризик від всіх окремих загроз визначений, загрози для однотипних об'єктів ранжирують, тобто складають ряд в порядку зростання ризиків. Це дає можливість, враховуючи думку замовника системи, виділити ті з них, що не є істотними, тобто ті, які можна не враховувати при вибиранні засобів захисту.

Загальний ризик від реалізації загроз, визнаних істотними, може бути визначений за правилом:

$$W = \sum_{i=1}^{n} P_{y_i} C_i ,$$

де n – загальне число істотних загроз.

Таким чином, виходячи зі сказаного, формальну модель загроз можна визначити як перелік обов'язкових параметрів, що визначаються на етапі аналізу ризиків, яких достатньо для вибору адекватних функціональних послуг захисту. До їх числа відносять:

– код, однозначно ідентифікуючий інформаційний об'єкт в досліджуваній інформаційній системі;

– вартість інформаційного об'єкта у відносних одиницях;

– перелік об'єктів, доступ до яких відкривається у разі несанкціонованого доступу до об'єкта, який захищається; їх вартості та коефіцієнтів зв'язку з оцінюваним об'єктом;

– опис уразливостей та сценаріїв атак з їх використанням, а також обчислена вірогідність їх успішної реалізації;

– обчислене значення ризику від реалізації даної загрози та висновки щодо її істотності.

Сумарний ризик є узагальненим показником, який характеризує можливі втрати у разі порушення прийнятої в системі політики безпеки. З урахуванням думки замовника, необхідно вибирати засоби захисту від кожної загрози по критерію «ефективність – вартість». Після цього слід визначити залишкову загальну величину ризику і, якщо, на думку замовника, ця величина достатньо велика, підсилити засоби захисту.

Приведений список параметрів може бути розширений за бажанням розробника, але їх мінімальна кількість повинна бути закріплена нормативним документом.

Висновок

Формальна модель загроз повинна бути сукупністю записів в базі даних загроз, поля якої містять інформацію про всі їх параметри для кожного інформаційного об'єкта, який підлягає захисту. При такому способі організації модель зручно підтримувати в актуальному стані, тобто доповнювати новими записами та видаляти відомості про ті загрози, які втратили свою актуальність.

Література

1. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу [Текст]. – Введ. 1999-04-28. – К. : Видавн. Департ. спец. телеком. систем та захисту інформації СБ України. – 30 с.
2. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу [Текст]. – Введ. 1999-04-28. – К. : Видавн. Департ. спец. телеком. систем та захисту інформації СБ України. – 59 с.
3. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу [Текст]. – Введ. 1999-04-28. – К. : Видавн. Департ. спец. телеком. систем та захисту інформації СБ України. – 21 с.

Abstract

The article outlines the key parameters of hazards to information objects of information transmission and processing systems. The general approach to the construction of a formal model of hazards is given. This approach allows the selection of functional protection services. It was indicated that the formal hazard model could be defined as a list of required parameters. The attention is focused on the fact that the parameters are determined at the stage of risk analysis. It should be noted that parameters are usually sufficient to select appropriate functional protection services. It was concluded that the total risk, concerning the information security, is an overall index. Mentioned index characterizes the possible losses in case of violation of security in the accepted system. It was determined that the means of protection should be chosen according to the "efficiency-cost" criterion, taking into consideration the opinion of information safety system customer. It was shown that it is necessary to determine the total residual of risk, and then, if necessary, to enhance the protective devices

Keywords: information, profile, protection, parameter, security