УДК 004.056.5

Б. І. Мороз, доктор технічних наук,
декан факультету інформаційних та транспортних систем і технологій Академії митної служби України
О. К. Ткачова, кандидат наук з державного управління, доцент кафедри вищої математики та інформатики Академії митної служби України
А. І. Кірюхіна, провідний фахівець лабораторії економіко-математичного моделювання в митній справі Академії митної служби України

ДО ПИТАННЯ МОДЕЛЮВАННЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Визначено сутність та основні складові загроз безпеці, розглянуто окремі аспекти проблеми моделювання загроз інформаційній безпеці та оцінки ризиків.

Определена сущность и основные составляющие угроз безопасности, рассмотрены отдельные аспекты проблемы моделирования угроз информационной безопасности и оценки рисков.

Essence and basic constituents of threats of security are in-process certain, the separate aspects of problem of threat modeling of information security and estimation of risks are considered.

Ключові слова. Загроза, інформаційна безпека, моделювання загроз.

Вступ. За умов глобальної інтеграції та міжнародної конкуренції головною ареною зіткнень національних інтересів багатьох держав стає інформаційний простір. Проте неефективне використання інформації може послабити або значно зашкодити як безпеці конкурентного підприємства, так і всієї країни. Проблема інформаційної безпеки набула особливого значення, коли в державних структурах та в суспільстві в цілому зрозуміли, що інформаційні ресурси є об'єктом власності й мають товарну цінність.

Слід зазначити, що вибір цілей і методів протидії конкретним загрозам інформаційній безпеці становить важливу проблему, що потребує проведення детального аналізу як різних рівнів загроз, так і різних рівнів захисту підприємства, держави, суспільства загалом.

Питання забезпечення інформаційної безпеки, встановлення загроз безпеці, подолання загроз інформаційному суверенітету держави розглянуто в працях В. Авер'янова, С. Гордієнко, Б. Кормича, В. Горбуліна, Г. Козаченко, І. Баймакової [1], О. Новікова та ін. Процес моделювання загроз уперше описано 1999 р. в Microsoft як методологію в документі "Threats to our software" ("Загрози нашим програмним продуктам"), складеному Дж. Гармс, П. Гарг і М. Говардом. Моделювання загроз висвітлено в працях А. Лукацького [2, 3], В. Миронової [4], Л. Остермана [5], А. Шостака [6], М. Говарда [7, 8], Ле Бланка, М. Снайдера та ін. Незважаючи на значну кількість досліджень у цій сфері, недостатньо висвітлено окремі аспекти питання моделювання загроз.

Постановка завдання. Метою статті є огляд останніх досліджень та аналіз методів моделювання загроз інформаційній безпеці.

Результати дослідження. Під загрозою розуміють:

- сукупність умов і чинників, що створюють потенційну або реальну небезпеку, пов'язану з незаконним отриманням інформації або ненавмисними діями з нею;
- потенційну причину, яка може завдати шкоди системі або організації;

• загрози безпеці персональних даних – сукупність умов і чинників, що створюють небезпеку несанкціонованого, зокрема випадкового, доступу до персональних даних результатом якого може стати знищення, зміна, блокування, копіювання, поширення персональних даних, а також інших несанкціонованих дій під час їх обробки в інформаційній системі персональних даних [*1*, 24].

Джерелом загроз, що реалізується шляхом несанкціонованого доступу до баз даних із використанням штатного чи спеціально розробленого програмного забезпечення, є суб'єкти, дії яких порушують регламентовані правила доступу до інформації. Цими суб'єктами можуть бути:

– порушник;

– носій програми;

– апаратна закладка.

Загрози класифікуються: за можливими джерелами; за середовищем поширення; за способами реалізації; за можливим об'єктом дії; за деструктивною дією на інформацію; за вразливістю, що використовується.

Під час характеристики загроз ураховуються: джерело – внутрішнє або зовнішнє; мотивація (наприклад, фінансова вигода, конкурентна перевага); частота виникнення; правдоподібність; шкідлива дія; тривалість дії загрози (разове незаконне отримання інформації).

Для ефективного забезпечення інформаційної безпеки важливі різноманітні моделі та методи оцінки загроз і небезпек. Їх варіативність занадто лабільна і залежить як від рівня розвитку тієї чи іншої цивілізації, так і від контексту оцінки, наявності всебічних даних про фактори загрози, алгоритму вирахування коефіцієнта ймовірності настання та розміру негативних наслідків. Наявність конкретних даних із цього питання дозволяє досить точно визначити ступінь впливу інформаційної зброї, рівень загроз та небезпек.

Дослідження загроз за моделями, під якими розуміються ті або інші аналоги (схеми, структури тощо) – дійова форма оцінки їхньої небезпеки. Моделі можуть бути конкретними або концептуальними, а також: статичними, такими, що відображають структуру, зв'язки й стани небезпек і загроз; простими динамічними, такими, що характеризують кількісні зміни; складними динамічними, такими, що відбивають кількісні зміни в їхньому розвитку.

Загрози моделюються для: систематичної ідентифікації потенційних небезпек; систематичної ідентифікації можливих видів відмов; кількісної оцінки або ранжування ризиків; виявлення чинників, що призводять до ризику, і слабких ланок у системі; глибшого розуміння функціонування системи; зіставлення ризиків досліджуваної системи з ризиками альтернативних систем або технологій; ідентифікації та зіставлення ризиків і невизначеностей; можливості вибору засобів і прийомів для зниження ризику.

Основне завдання моделювання загроз – обґрунтування рішень, що стосуються ризиків.

Початкові дані для моделювання – це:

– перелік джерел загроз;

– перелік вразливостей, через які можлива реалізація загроз; перелік загроз безпеці інформації;

– перелік деструктивних дій, що виконуються в результаті реалізації загроз;

– значення коефіцієнтів небезпеки виконання деструктивних дій;

– значення вірогідності наявності сприятливих умов для використання вразливості для реалізації загроз безпеці інформації;

– сукупність взаємозв'язків між джерелами загроз, загрозами і вразливими ланками;

– сукупність взаємозв'язків між загрозами і деструктивними діями.

Модель загроз повинна відповісти на такі питання:

▪ Які загрози можуть бути реалізовані? Ким?

▪ З якою вірогідністю можуть бути реалізовані ці загрози? Який потенційний збиток від цих загроз? Яким чином можуть бути реалізовані ці загрози?

▪ Засоби й канали реалізації. Чому ці загрози можуть бути реалізовані?

▪ Уразливості і мотивація. На що може бути спрямовано ці загрози? Як можна їх відбити? [3].

Модель загроз має систематизувати всі наявні відомості і припущення про можливі вектори атак, мотивацію зловмисників, вірогідність несанкціонованих дій і потенційний розмір збитку від їх реалізації.

Моделювання загроз включає множину різних процедур з виявлення вимог до безпеки системи та аналізу різних схем захисту. Не існує єдиного "кращого" або "правильнішого" методу моделювання загроз, навпаки, слід поєднувати й комбінувати різні альтернативи для того, щоб досягти явно заданих або прихованих цілей.

Загрози визначають політику безпеки, а вона, відповідно, процес розробки. Зокрема:

▪ потрібно зрозуміти, що реально загрожує системі, і провести оцінку ризиків;

▪ визначити політику безпеки для запобігання цим загрозам. Це повинні бути положення на зразок: "тільки вповноважені банки мають право змінювати баланс на платіжних картках" або "всі рухи грошових коштів у системі мають бути доступні контролю";

▪ розробити запобіжні заходи, які втілюють у життя політику безпеки. Ці контрзаходи повинні поєднувати механізми захисту, виявлення і реагування.

Правову базу регулювання інформаційної безпеки в Україні становить ряд документів: Закон України "Про доступ до публічної інформації" [9], Закон "Про інформацію" [10], Проект Закону "Про інформаційний суверенітет та інформаційну безпеку України" [11], Указ Президента "Про доктрину інформаційної безпеки України" [12]. На жаль, в Україні нормативні документи не дають відповіді на запитання "як оформити модель загроз?".

Орієнтовна модель загроз А. Шостака [6] відображає загальні риси базового процесу моделювання загроз (рис. 1).

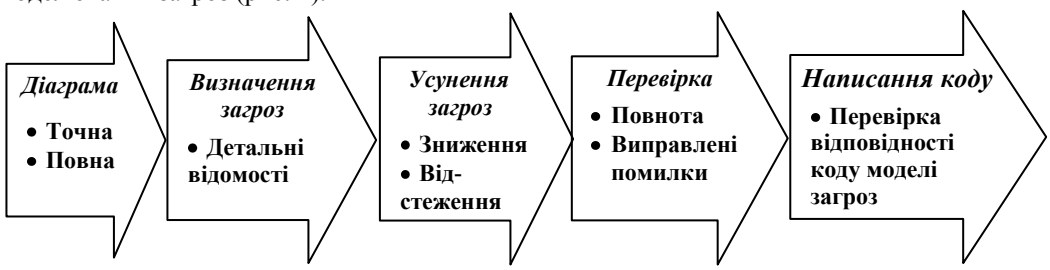

Рис. 1. Процес моделювання загроз

Створення схеми додатка (рис. 2) та застосування мозкового штурму істотно допоможе в моделюванні загроз [6].

Під час розробки системи безпеки потрібно моделювання загроз та оцінка ризиків.

Якщо частота події на рік становить >1, то це часта подія, якщо $1–10^{-1}$ – ймовірна, $10^{-1}–10^{-2}$ – випадкова, $10^{-2}–10^{-4}$ – малоймовірна, $10^{-4}–10^{-6}$ – неправдоподібна, 10^{-6} – неймовірна.

Класифікація ризику: *B* – висока величина ризику, *C* – середня величина ризику, *M* – мала величина ризику, *H* – незначна величина ризику [3].

Досить непросто скласти перелік загроз, потрібно знати, як реагувати на кожну з них. Слід оцінити можливий збиток від реалізації загрози і можливу кількість таких випадків протягом року, а потім обчислити очікувані втрати за рік. Наприклад, "заплановані" збитки від хакерського вторгнення в мережу становлять 10 000 дол. у кожному випадку, а такі події можуть траплятися тричі на день, або тисячу разів за рік. У такому разі очікувані збитки за рік

не перевищать 10 млн дол. Якщо очікувані збитки за рік дорівнюють 10 млн дол., то придбання установки і підтримка брандмауера за 25 000 дол. на рік – вельми вигідна справа.

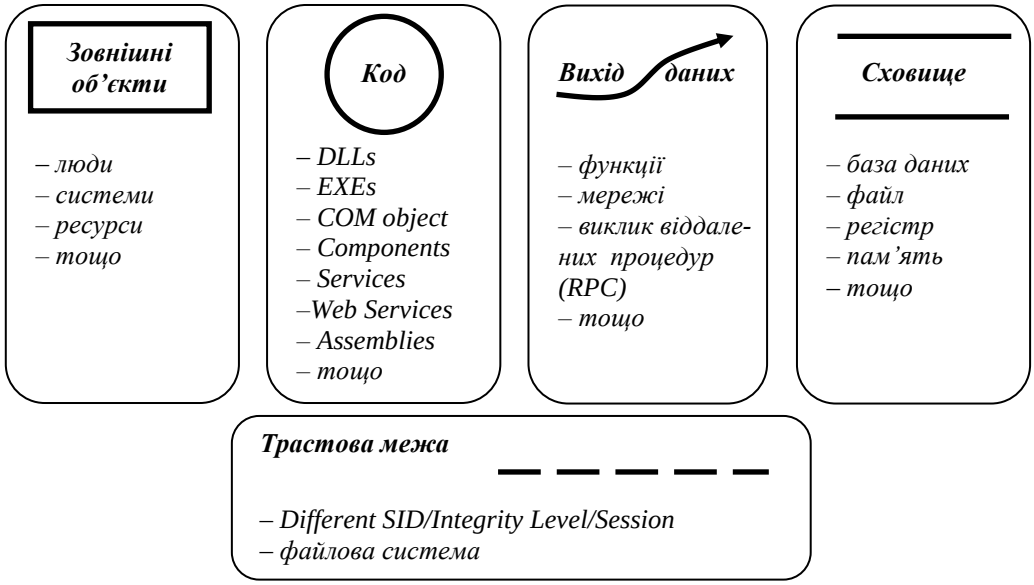

Рис. 2. Орієнтовна схема додатка моделювання загроз

Іноді ймовірність реалізації загрози дуже мала. Якщо йдеться про вторгнення в систему конкурента з метою отримання відомостей про нові розробки, втрати можуть досягти, наприклад, 10 млн дол. у кожному випадку. Але якщо ймовірність таких вторгнень становить 0,001 або 0,1 % на рік, то очікувані збитки за рік перетворюються на 10 000 дол., і заходи протидії, які обходяться в 25 000 дол., стають абсолютно не вигідними [13].

Існує велика кількість формул для визначення ймовірності загроз, коефіцієнтів небезпек. Вірогідність реалізації загрози – показник, що характеризує наскільки вірогідна реалізація конкретної загрози для безпеки для даної системи в умовах обстановки, що склалася.

Коефіцієнт небезпеки загрози ($K_{нз}$) не залежить від виду і визначається формулою:

$$K_{нз} = \frac{q_з}{Q_{max}}, \qquad (1)$$

де $q_з$ – величина збитку, $Q_{\max}$ – максимальний збиток.

Величина збитку визначається експертним методом.

За російською методикою "Визначення актуальних загроз безпеки персональних даних під час їх обробки в інформаційних системах" можна розрахувати коефіцієнт загрози й оцінити ступінь її реалізації [4, 14].

Коефіцієнт загрози, що реалізується: $Y = (Y_1 + Y_2) / 20$, де Y_1 – показник захищеності, Y_2 – ймовірність реалізації.

Можливість реалізації загрози оцінюється так: $0 < Y < 0{,}3$ – низька; $0{,}3 < Y < 0{,}6$ – середня; $0{,}6 < Y < 0{,}8$ – висока; $Y > 0{,}8$ – дуже висока.

Під час складання переліку актуальних загроз безпеці кожній градації ймовірності виникнення загрози відповідає числовий коефіцієнт Y_2 – вірогідність реалізації: 0 – для маловірогідної загрози (об'єктивні передумови для реалізації загрози відсутні); 2 – для низької вірогідності

загрози (об'єктивні передумови для реалізації загрози існують, але вжиті заходи суттєво ускладнюють її реалізацію); 5 – для середньої вірогідності загрози (вжиті заходи забезпечення безпеки недостатні); 10 – для високої вірогідності загрози (заходів із забезпечення безпеки не вжито).

Числовий коефіцієнт Y_1 – показник захищеності: 0 – для високого ступеня початкової захищеності, 5 – для середнього, 10 – для низького. Захищеність оцінюється на основі опитування експертів.

Якщо подивитися на моделювання загроз із позиції цифр, то цікавим є дослідження компанії Forrester, згідно з яким чим раніше ми почнемо боротися з загрозами, усувати їх або знижувати їхню дію, тим краще буде з різних поглядів. При цьому Forrester врахувала різні етапи життєвого циклу системи і перевела поняття "тим краще" в деякі ресурси в умовних одиницях. Такими ресурсами можуть бути гроші, час, люди тощо. Наприклад, якщо на етапі дизайну або проектування системи на боротьбу з загрозами ми витратимо X ресурсів, то вже на етапі промислової експлуатації масштаб витрат збільшиться в 30 разів [*2*, 67].

Моделювання загроз дозволяє визначити найуразливіші місця в системі і вжити відповідних заходів для посилення її безпеки та мінімізації матеріального збитку.

Для забезпечення комп'ютерної безпеки моделювання загроз стає все більш актуальною проблемою, особливо, якщо розглядати останню у світлі збереження комерційної таємниці.

Так, за даними компанії ESET у 2013 р. збільшиться кількість шкідливих програм, спрямованих на мобільні пристрої, та їх модифікацій, популярнішим стане поширення загроз за допомогою різних веб-ресурсів, зросте кількість ботнетів ("зомбі") і "хмарних" атак, здійснюваних з метою крадіжки конфіденційної інформації.

Голова ради директорів Google Ерік Шмідт у своїй книзі "Новий цифровий вік" заявив, що вважає КНР країною, яка становить "ІТ-загрозу" і є "найбільш хитромудрим та успішним" хакером іноземних компаній [15]. У 2013 р. значно збільшиться кількість загроз під мобільні платформи. Основними видами шкідливої діяльності загроз під Android залишається крадіжка інформації (шпигунське ПЗ), відправлення дорогих SMS – повідомлень та перетворення мобільних пристроїв у "зомбі". У 2013 р. очікується значне зменшення кількості загроз, що поширюються за допомогою змінних пристроїв. При цьому, за прогнозами спеціалістів ESET, кіберзлочинці все частіше використовуватимуть для зараження так звані "посередники" – спеціальні веб-сервери для завантаження та виконання різних шкідливих програм. Отримавши несанкціонований доступ до серверів, зловмисники розсилатимуть гіперпосилання, що спрямовуватимуть користувачів на шкідливі веб-ресурси [15]. Однією з основних проблем залишаться добре відомі користувачам ботнети – мережі комп'ютерів, інфіковані шкідливими програмами, які дозволяють дистанційно управляти інфікованими машинами.

На жаль, в Україні практично немає єдиного документа або стандарту, який би описував увесь процес моделювання загроз інформаційній безпеці. Слід зазначити, що існує ДСТУ 3396.1-96 "Захист інформації. Технічний захист інформації. Порядок проведення робіт". Цей стандарт установлює вимоги до порядку проведення робіт із технічного захисту інформації, але сам механізм створення моделі загроз не наводиться. Існують також інші ДСТУ щодо технічного захисту, а саме: ДСТУ 3396.0-96 "Захист інформації. Технічний захист інформації. Основні положення"; ДСТУ 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни та визначення"; ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння"; ДСТУ ГОСТ 31078:2004 "Захист інформації. Випробування програмних засобів на наявність комп'ютерних вірусів". Типова настанова (ДСТУ 31078-2002, IDT).

Актуальна ратифікація Європейської конвенції про кіберзлочинність, підписана Україною 23.11.2008 р. в Будапешті разом із тридцятьма іншими державами. Конвенція містить важливі положення, спрямовані на боротьбу з кіберзлочинністю шляхом уніфікації законодавства й вирішення низки процедурних питань щодо співпраці правоохоронних органів.

Висновки. У сучасному світі, в якому людина стає все більш і більш залежною від інформаційних технологій, застарілі методи моделювання загроз вже не працюють. Вони дуже сконцентровані на загрозах порушення цілісності, доступності й конфіденційності на шкоду іншим, навіть важливішим проблемам. Проблему інформаційної безпеки не можна розв'язати без розробки збалансованої політики безпеки, моніторингу інформаційного середовища, аналізу наслідків небезпечних інформаційних впливів.

Нині не можна говорити про правильний або неправильний метод аналізу ризику (моделювання загроз). Важливо, щоб організація користувалася найбільш зручним і доцільним методом, що дає вагомі результати.

Література

1. Баймакова И. Обеспечение защиты персональных данных : методическое пособие / Баймакова И. – 3-е изд. – М. : 1С-Паблишинг, 2011. – 268 с.

2. Лукацкий А. Какой должна быть модель угроз / А. Лукацкий // IT-Manager. – 2011. – октябрь. – С. 67.

3. Лукацкий А. Построение модели угроз [Электронный ресурс] // Шестой ежегодный IT & Security Forum в Казани, 2012 г. – Режим доступа : http://www.itsecurityforum.ru/2012/reports.

4. Миронова В. Анализ этапа определения актуальных угроз безопасности персональных данных / В. Миронова, А. Шелупанова // Технологии Microsoft в теории и практике программирования. VII Всероссийская научно-практическая конференция. – ТПУ, 23–24 марта 2010. – С. 207.

5. Остерман Л. О моделировании угроз [Электронный ресурс] / Остерман Л. – Режим доступа : http://blogs.msdn.com.

6. Шостак А. Возобновление процесса моделирования угроз [Электронный ресурс] / А. Шостак // MSDN Magazine. – 2008. – June. – Режим доступа : http://msdn.microsoft.com.

7. Howard M. Security Briefs : Threat Models Improve Your Security Process [Електронний ресурс] / M. Howard // MSDN Magazine. – 2008. – November. – Режим доступу : http://msdn.microsoft.com.

8. Howard M. Security Briefs : A Follow on Conversation about Threat Modeling [Електронний ресурс] / M. Howard // MSDN Magazine. – 2009. – September. – Режим доступу : http://msdn.microsoft.com.

9. Про доступ до публічної інформації [Електронний ресурс] : Закон України від 13.01.2011 р. № 2939-VI. – Режим доступу : http://zakon. rada.gov.ua.

10. Про інформацію [Електронний ресурс] : Закон України від 02.10.1992 р. № 2657-XII. – Режим доступу : http://zakon. rada.gov.ua.

11. Про інформаційний суверенітет та інформаційну безпеку України [Електронний ресурс] : проект Закону від 15.04.1999 р. № 1072-XIV. – Режим доступу : http://zakon. rada.gov.ua.

12. Про Доктрину інформаційної безпеки України [Електронний ресурс] : Указ Президента України від 08.07.2009 р. № 514/2009. – Режим доступу : http://zakon.rada.gov.ua.

13. Моделирование угроз и оценки риска [Електронний ресурс]. – Режим доступу : http://deviceinform.ru.

14. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена ФСТЭК от 14.02.2008 года.

15. Тенденції розвитку загроз у 2013 році [Електронний ресурс]. – Режим доступу : http://www.licasoft.com.ua.