Розвивається ідея аналітичного підходу в методології оцінювання та управління ризиками інформаційної безпеки. Робляться відповідні узагальнення щодо оцінки та управління ризиків інформаційної системи

Ключові слова: ризик, інформаційна безпека, оцінювання ризиків

Развивается идея аналитического подхода в методологии оценки и управления рисками информационной безопасности. Делаются соответствующие обобщения в оценке и управлению рисков информационной системы

Ключевые слова: риск, информационная безопасность, оценка рисков

Develops the idea of an analytical approach to the methodology of risk assessment and management of information security. Appropriate generalizations made in the evaluation and management of risk information system

Key words: risk, information security, risk assessment

УДК 681.323

АНАЛІТИЧНИЙ ПІДХІД В МЕТОДОЛГОІЇ ОЦІНЮВАННЯ ТА УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

О.А. Замула
Кандидат технічних наук, доцент, професор*
Контактний тел.:(057) 702-14-25
E-mail: bit@iit.com

Б.В. Волобуєв
Магістрант*
E-mail: bodog2008@narod.ru

В.І. Черниш
Магістрант*
E-mail: vlad.chernish@gmail.com

К.І. Іванов
Магістрант
*Кафедра безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
Пр. Леніна, 14, м. Харків, Україна, 61234
Контактний тел.:(057) 702-10-13
E-mail: kiivnv@gmail.com

1. Вступ

У сучасному світі поняття ризику широко вживається в різних сферах діяльності. Це поняття, як правило, застосовується для опису будь-якого потенційно небезпечного явища. Задовго до появи поки що недосконалою теорії ризику та методів ймовірнісної оцінки негативних явищ з терміном «ризик» зазвичай пов'язувалося значення (якісне або кількісне), яке характеризувало потенційну ступінь небезпеки однієї або декількох погроз. При цьому прийняття управлінського рішення в умовах дії негативних факторів пов'язане з мінімізацією негативних наслідків, які можуть виникнути при реалізації цих загроз. У даному контексті порівняно недавно було введено поняття управління ризиками, яке фактично відображає суть вибору такого рішення.

Управління інформаційними ризиками представляє собою досить широке поняття, яке використовується в літературі як вид діяльності, що включає визначення загроз безпеці інформаційної системи, оцінку рівня небезпеки загроз (тобто розміру можливого збитку), а також ймовірностей реалізації цих загроз - тобто проведення повного аналізу ризиків системи [1,2]. На основі цього аналізу приймається рішення про заходи щодо зниження загального рівня ризику для системи. Причому конкретний зміст цього поняття залежить від розв'язуваної задачі.

2. Концепції оцінювання ризиків

Ризик проявляється в різних сферах діяльності людини таких, як функціонування організацій, взаємодія з навколишнім середовищем. Ризик є проявом неповної визначеності, з якою доводиться стикатися в багатьох сферах життєдіяльності. З цього випливає, що його поява зумовлена випадковими процесами, що протікають у світі. Поняття ризику пов'язане з можливим проявом негативних наслідків, в результаті реалізації цих процесів. Однак у деяких випадках з точки зору управління має сенс допускати певну величину ризику для того, щоб мати можливість отримати певний позитивний результат, з будь-якою ймовірністю. Прикладом цього є комерційна діяльність, в якій особа, яка приймає рішення, може цілеспрямовано йти на ризик, щоб досягти матеріального виграшу. В інших випадках ризик є суто негативним явищем. Найбільш

очевидним прикладом цього є ризик порушення безпеки (техногенної, інформаційної тощо). Такий вид ризиків, проявляючись, має лише негативні наслідки. Крім вищезгаданої корисності, існує ще один вид, в якому передбачуваність розвитку подій є основною метою управління. Тобто сама невизначеність є джерелом ризику.

Невизначеність має місце і при отриманні користі систем, яка часто є випадковою величиною. Вищенаведений приклад комерційного ризику, очевидно, свідчить на користь оцінки, в даному випадку, шансів. Тобто невизначеність породжує не лише ризики, але і шанси, які також слід вимірювати і враховувати.

Для кожного з перерахованих випадків необхідно використовувати власну методику оцінки та управління. Однак на практиці [3,4] застосовують декілька концепцій.:

1. Концепція ризику як можливості. У рамках цієї концепції управління ведеться на основі взаємозв'язку між ризиком і користю. У даному випадку звичайно зі зростанням ризику зростає і потенційний дохід. Менеджмент в цьому випадку спрямований на максимізацію користі з одночасним обмеженням втрат.

2. Концепція ризику як небезпеки. Ця концепція передбачає розгляд негативних подій, що заподіюють шкоду. Ризик характеризує можливість настання такої події, а також його наслідки. Управління ризиками в цьому випадку є мінімізація ймовірності настання негативних подій, а також величин збитку.

3. Концепція невизначеності. Дана концепція передбачає збільшення рівня ризику по мірі зростання кількості різних варіантів розвитку подій. Тобто, якщо система знаходиться в єдино можливому стані, то ризик для неї мінімальний і, відповідно, рівень ризику зростає у разі збільшення ймовірності реалізації інших альтернатив.

Керуючі впливи в рамках концепції невизначеності спрямовані на збільшення ймовірності появи очікуваних результатів, тобто зниження дисперсії для даної випадкової величини.

У рамках дослідження проблеми оцінки та управління ризиками систем кожна з цих стратегій представляє певний інтерес, оскільки застосування першої концепції пов'язано з отриманням певної вигоди від функціонування системи, другої - з мінімізацією наслідків негативних впливів та максимізацією позитивних, а третьої - з поліпшенням передбачуваності поведінки системи.

3. Узагальнена модель оцінювання ризиків

Розглянемо запропоновану модель оцінки ризиків для довільної системи. Для початку введемо загальне поняття ризику.

Розглянемо множину загроз для системи. Загроза – сукупність умов та факторів, при реалізації якої буде пошкоджено систему. Ризик є величиною, яка дозволяє оцінити апріорну ступінь небезпеки загрози. Для оцінки ступеня небезпеки необхідно ввести міру ризику як числову характеристику, що дозволяє визначити його рівень. Ризик можна визначити як відображення множини негативних факторів (загроз) U на деяку числову множину значень міри ризику R:

В окремому випадку ризик можна розглянути як функціонал загрози:

$$\text{Risk: } U \to R \qquad (1)$$

$$\text{Risk} = \varphi(U). \qquad (2)$$

У загальному випадку не важко визначити, яким чином проводиться відображення. Розглянемо загрозу як абстрактний об'єкт, що має певний набір характеристик, виходячи з яких визначається значення міри ризику для загрози. Вид відображення залежить від класу задач, які вирішуються системою.

Ймовірність можна визначити як відображення множини позитивних факторів V на множину значень міри C:

$$\text{Ch: } V \to C \qquad (3)$$

$$\text{Ch} = \varphi(V). \qquad (4)$$

4. Ймовірнісна природа ризику

Будь-яка система не є повністю детермінованою, хоча б виходячи з того, що надзвичайно складно врахувати різноманітні умови і фактори, які мають на неї вплив. Зазвичай у особи, яка приймає рішення з управління системою, недостатньо інформації для точного прогнозування її поведінки.

Тому при розрахунку міри ризику повинна враховуватися невизначеність, пов'язана з системою. Виникнення ризику в загальному випадку є наслідком невизначеностей у системі. В іншому випадку можливо було б існування повністю детермінованих систем з нульовим ризиком і максимальною користю.

Тому при розгляданні ризику, як апріорного ступеня небезпеки загрози, очевидна доцільність застосування методів теорії ймовірностей для розрахунку значення міри ризику. Найбільш поширене уявлення загрози Ui полягає у поєднанні кількісної оцінки збитку при реалізації загрози - ui та ймовірності реалізації загрози (зазвичай протягом певного періоду часу) - pi. У цьому випадку мірою ризику є такий вираз:

$$\text{Risk}(Ui) = uipi \qquad (5)$$

Вираз (5) прийнятний для вирішення багатьох практичних завдань, тому що являє собою вирішення проблеми оцінки ризику у спрощеній формі, а також є ефективним для оцінки ризику кожної загрози.

Такий підхід має ряд переваг. Поряд з простотою використання варто врахувати, що в результаті міра ризику оцінюється тією ж фізичною величиною, що і значення збитку. Це говорить про те, що її досить зручно використовувати при розрахунках у наглядній формі.

На практиці, якщо є статистика величини збитків та ймовірність її появи часто представлені не конкретними значеннями, а законами розподілу збитків для конкретної системи в цілому. Це дозволяє більш реалістично оцінити ймовірність виникнення збитку певної величини. У цьому випадку доцільно розгля-

нути два основні класи опису виникнення збитків або доходу:

Перший клас: закони розподілу, що представляють дискретну випадкову величину.

Другий клас: закони розподілу, що представляють безперервну випадкову величину.

Для кожного з даних класів розподілу необхідно визначити міру, що дозволяє адекватно оцінювати рівень ризику.

5. Аналіз методів оцінювання ризиків інформаційної системи

Як показує огляд інформаційних джерел у галузі оцінки та управління інформаційними ризиками на даний момент переважають експертні методи їх оцінки [5,6]. Це обумовлено, перш за все, відсутністю узагальнених статистичних даних по реалізації загроз в інформаційній сфері для систем. Часто доводиться використовувати достовірну статистику спільно з експертними оцінками.

Експертні оцінки зазвичай є оцінки ймовірності настання подій, а також приблизні значення збитку відповідні цим подіям. На основі цих даних проводиться розрахунок ризику системи. Таким чином, для управління ризиками оцінка суб'єктивної ймовірності є ключовим моментом [6,7].

Застосування методів експертної оцінки має очевидні недоліки такі, як їх суб'єктивність, великі похибки при використанні їх в аналітичних розрахунках.

Необхідно відзначити також існуючі кількісні методи, що існують для оцінок ризику. Вони зазвичай використовують накопичену статистику і оперують з ймовірностями, отриманими в результаті статистичних розрахунків [6]. Недоліком таких методів є необхідність накопичення досить великих обсягів статистичних даних для отримання точних прогнозів щодо рівня ризику.

Оцінка ризику експертними методами має перевагу у вигляді достатньої простоти застосування в умовах відсутності об'єктивних даних про величини ймовірностей виникнення подій, і величинах збитку. Ефективністю такого способу оцінки інформаційних ризиків можна керувати шляхом зміни складу експертної групи, а також підвищенням рівня підготовки її учасників.

6. Аналітичні методи аналізу та управління інформаційними ризиками

Аналітичний спосіб отримання результатів здійснюється безпосередньо на основі значень екзогенних змінних. До його переваг відноситься швидкість знаходження рішення, а до недоліків - необхідність адаптації поставленої задачі до наявного в розпорядженні математичного апарату і відносно невелика його "прозорість" .

Під управлінням ризиками розуміється [3] розробка та обгрунтування оптимальних програм діяльності, покликаних ефективно реалізувати рішення в галузі забезпечення безпеки (корисності).

Звідки управління ризиками (шансами) системи являє собою циклічний багатоетапний процес, який, по суті, утворює безліч взаємопов'язаних процесів [2,3]. Схематично його можна зобразити, як це показано на рис. 1.

Опишемо докладніше кожний з етапів, представлених на даній схемі.

Аналіз ризиків спрямований на виявлення негативних (позитивних) факторів і кількісне визначення рівня ризиків, що виникають у процесі функціонування системи [3].

Ідентифікація - діяльність, спрямована на виявлення ризиків (шансів), характерних для даної системи, причин їх виникнення, форм прояву та негативних (позитивних) факторів. Ідентифікація сприяє формуванню у особи, яка приймає рішення, цілісної картини ризиків системи [3,4].

Оцінка ризиків - отримання (обчислення) кількісних значень ступеня прояву ризиків, характерних для даної системи [3].

Моніторинг результатів управління ризиків є оцінка ефективності прийнятих рішень з управління ризиками системи в процесі її функціонування.

Вибір управлінського рішення - це зіставлення оцінок ефективності всіх управлінських рішень з безлічі й вибір найбільш підходящого на основі критерію вибору оптимальних рішень.

Визначення множини управлінських рішень - побудова певної множини рішень, які можна вжити відповідно за даним станом системи.

Оцінка ефективності кожного елемента з множини управлінських рішень - отримання якісної або кількісної оцінки ефективності управлінського рішення на основі зіставлення збитків, витрат і позитивного економічного ефекту від його прийняття.

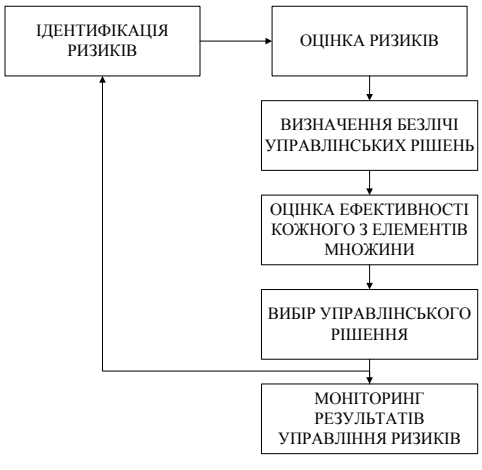

Рис. 1. Загальна схема управління ризиками

Висновки

Запропоновано принцип аналітичного підходу в методології оцінювання та управління ризиками інформаційної безпеки та були зроблені відповідні узагальнення щодо оцінки та управління ризиків інформаційної системи.

Розглянуто три основні концепції оцінювання ризиків, що найбільш розповсюджені на практиці. Концепція ризику як можливості. Концепція ризику як небезпеки. Концепція невизначеності. Кожна з цих стратегій представляє певний інтерес, оскільки застосування першої концепції пов'язано з отриманням певної вигоди від функціонування системи, другої - з мінімізацією наслідків негативних впливів та максимізацією позитивних, а третьої - з поліпшенням передбачуваності поведінки системи.

Розглянуто узагальнену модель оцінювання ризиків, ймовірнісу природу ризику.

Особливу увагу приділено аналітичним методам аналізу та управлінню інформаційними ризиками, що здійснюються безпосередньо на основі значень екзогенних змінних.

Література

1. Балдин К.В. Управление рисками и выбор стратегии [Текст] / К.В. Балдин // Высшее образование сегодня. - Реферируемое издание ВАК России. - Б.м. - 2005.- № 11. - С. 36-38.
2. Риски систем: оценка и управление [Текст] / В.Н. Асеев, Д.Е. Морев, В.Б. Щербаков. – под. ред. Ю.Н. Лаврухина - Воронеж: Междунар. ин-т компьют. технологий, 2007. - 261 с.
3. Вишняков Я.Д. Общая теория рисков: учеб. пособие для студ. высш. учеб. Заведений [Текст] / Я.Д. Вишняков, Н.Н. Радаев. - М.: Издательский центр «Академия», 2007. - 368 с.
4. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность [Текст] / С.А. Петренко. - М.: Компания АйТи; ДМК Пресс, 2004. – 384 с.
5. Черныш В.И. Методы оценивания информационных рисков компании [Текст] / В.И.Черныш // Материалы XV Международного юбилейного молодёжного форума «Радиоэлектроника и молодежь в XXI веке»: Сб. тезисов, 18–20 апреля 2011 р., Т.5. - Харьков: ХНУРЭ. 2011. – С. 195.
6. Замула О.А. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки [Текст] / О.А. Замула, В.І. Черниш // Системи обробки інформації . – Харків: ХУ ПС, 2011. – Вип.2(92). – С.53-56.
7. Замула А.А. Оценивание рисков информационной безопасности в современных информационных системах [Текст] / А.А. Замула, В.И. Черныш, К.И. Иванов // XIV Международная научно-практическая конференция «Безопасность информации в информационно – телекоммуникационных системах», тезисы докладов. – К.: ЧП «ЕКМО», НИЦ «ТЕЗИС» НТУУ «КПИ», 2011. - С. 31.

Запропоновано сформулювати багатокритеріальну задачу досягнення заданого рівня зрілості процесу розробки програмного забезпечення на основі вибору серед альтернативних варіантів реалізації цього процесу з урахуванням ресурсних обмежень організації

Ключові слова: поліпшення якості, модель зрілості

В работе предложено сформулировать многокритериальную задачу достижения заданного уровня зрелости процесса разработки программного обеспечения на основе выбора среди альтернативных вариантов реализации данного процесса с учетом ресурсных ограничений организации

Ключевые слова: улучшение качества, модель зрелости

We propose to formulate the problem of achieving the necessary level of maturity for the software process based on the selection among alternate variants of the process steps implementation under the resource constraints of the organiza-tion

Key words: quality improvement, maturity model

УДК 681.518

ОЦЕНКА И УПРАВЛЕНИЕ КАЧЕСТВОМ ПРОЦЕССА РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ОСНОВЕ МОДЕЛЕЙ ЗРЕЛОСТИ

В.А. Шеховцов
кандидат технических наук, доцент*
Контактный тел.: (050) 9653427
E-mail: shekvl@yahoo.com

М.Д.Годлевский
Доктор технических наук, професор, заведующий кафедрой*

И.Л.Брагинский
Аспирант
*Кафедра автоматизированных систем управления НТУ «ХПИ»
ул. Фрунзе 21 Харьков, Украина, 61002