Механика Транспорт Комуникации

Научно списание

ISSN 1312-3823

том 11, брой 3, 2013 г.

статия № 0863

http://www.mtc-aj.com

АНАЛИЗ И ОЦЕНКА НА РИСКА ПРИ ЗАЩИТА НА ИНФОРМАЦИЯТА В АНАЛИТИЧНИ СИСТЕМИ ЗА УПРАВЛЕНИЕ

Христина Спиридонова, Антонио Андонов, Мариана Михова

hristinaspiridonova@abv.bg, andonov@vtu.bg

Висше транспортно училище „Тодор Каблешков”
бул. Гео Милев 158, София
БЪЛГАРИЯ

Ключови думи: *информационна сигурност, риск, конфиденциална информация*

Резюме: *В съвременните бизнес-процеси защитата на конфиденциалната информация е важна компонента на дейността, свързана с разработването, съпровождането и управлението на информационните технологии. В настоящата статия са предложени мерки за прогнозиране на количествени характеристики на риска, свързан със защитата на конфиденциалната информация в аналитични системи с различно предназначение.*

Централно място в тази проблематика заемат задачите за избор на варианти при сценарийно планирани алтернативи, стратегии, планове и т.н., оптимални по отношение на един или друг критерий. В научната литература по тези проблеми съществуват забележими разлики между работите с теоретичен и приложен характер. В теорията се разглеждат логическите основи на избора, аксиоматиката, общите принципи на съгласуваност и рационалност, а повечето приложими работи са посветени на построяването на конкретни модели и процедури, в значителна част евристични. В тази ситуация от изключителна актуалност са въпросите за разработване и систематизация на теоретично обосновани методи, способни да служат като методологична основа за решаване на приложни задачи. В този смисъл целта на предложената работа е да предложи подход при прогнозиране на качествени характеристики на риска при приемане на решения, свързани със защитата на конфиденциална информация в аналитични системи. Получени са оценки на прогнозирани нива на риска при въздействие върху конфиденциална информация с цел нейното обезценяване, както и на ефективността на защитата ѝ, позволяващи да се проследят стратегическите закономерности на поведението на участвалите субекти, преследващи противоположни цели.

1. Увод

В настоящата действителност на съвременния етап на развитие на обществото, когато протича коренна промяна на ценностите, много традиционни ресурси на човешкия прогрес губят своето първостепенно значение и роля. Но информацията е била и остава оновен ресурс на научно-техническото и социално-икономическото развитие на обществото. Колкото повече обемът и достъпността на информацията е по-голям, толкова по-висока е отговорността на решенията, които се вземат.

Съвременните технологични достижения и тяхното бързо развитие в такива

области като космически изследвания, радиоелектронна, компютърна и рентгенова техника постоянно изменят ситуацията в областта на защита на конфиденциалната информация, като позволяваг създаването на високоефективни средства за несанкциониран достъп до нея. Защитата от тях е възможна само на същото технологично ниво. Създаването на глобални мрежи от системи с различно предназначение: военни, банкови, за електронно банкиране и търговия, ведомствени за специални задачи и други, изискват все по-бързи темпове за обмен и достъпност на информацията в условия на мобилност. Обменяната в тях информация е в основната си част класифицирана, затова основен фактор при тях е защитата и сигурността на информационния обмен. Най-уязвими елементи на информационите системи са оборудването и апаратурата, предназначени за обработка, съхранение и предаване на конфиденциалната информация. Разработването обаче на комплексен подход към проблема, включващ технологични, правни, систематични и организационни мерки при проектиране на системи за информационна сигурност се осъществява в рамките на концепцията за приемлив риск. Особеност при този подход е използването на качествени критерии и характеристики на риска.В тази ситуация от изключителна актуалност са въпросите за разработване и систематизация на теоретично обосновани методи, способни да служат като методологична основа за решаване на приложни задачи. В този смисъл целта на предложената работа е да предложи подход при прогнозиране на качествени характеристики на риска при приемане на решения, свързани със защитата на конфиденциална информация в информационните системи с различно предназначение.

2. Постановка на проблема

Както е известно, за всяка информационна система или мрежа, в която се обработва, съхранява или пренася конфиденциална информация се изготвят специални изисквания за сигурност. Те се формират по време на най-ранния стадий от проектирането й и се детайлизират и развиват в процеса на изграждането й.

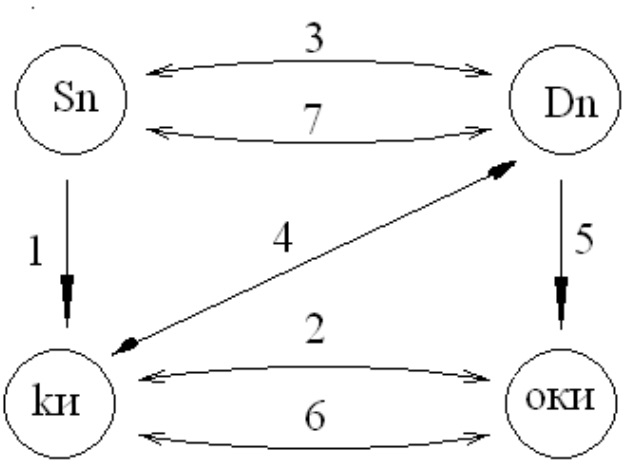
Изискванията за сигурност определят управлението и контрола на сигурността на информационната система или мрежа, като съдържат описание на формата на представяне и ниво на класификация на обработваната информация; групите потребители според нивото на достъп и начина на взаимодействие със системата; физическа среда и функционални елементи, архитектура, връзки, заплахи и уязвимост, глобалната, локална и електронна среда и режима на сигурност на информационната система и мрежа като цяло. Целта на предложената работа е да предложи обобщен подход за анализ и прогнозиране на количествени характеристики на риска при вземане на решение за защита на конфиденциална информация в информационни системи и мрежи. Този подход е свързан преди всичко с количественото определяне на рисковата стойност на конфиденциалната информация. Ако се приеме, че конфиденциалната информация е анонс на скъпоструващ продукт с ниска трайност (информацията бързо старее) то рисковата й стойност може да се определи с израза [4]:

$$C_k = A_c(1 - e^{-\frac{V_k}{V_0}})e^{-\frac{\tau_{\text{тк}}}{\text{T}_0}} \quad (1)$$

където A_c е мащабен множител, съответстващ на категорията на конфиденциалната информация; V_c е обемът от конфиденциалната информация, достъпен на субектите и осъществяващ въздействие върху нея, с цел нейното обезценяване, V_o – обемът необходим за реализацията на това въздействие; $\tau_к$ и T_o са съответно времената на въздействие и необходимото време на въздействие за извършване на процеса на

обезценяване на информацията. Увеличаването на несигурността е резултат от различни фактори. В съвременния свят неопределеността ражда риск, рискът увеличава неопределеността.

Най-обща схема на бизнес процеса, по осигуряване на информационна сигурност на даден обект може да се представи на фиг. 1.



фиг.1

Субектът Sn осъществява въздействие върху конфиденциалната информация (ки – събитие 1) с цел превеждането ѝ в обезценено състояние (оки – събитие 2), чрез нейното разкриване като прихващане и разшифроване или чрез нейното компрометиране като изкривяване или разрушаване

Обикновено не е възможно веднага да се определи количествената оценка на конфиденциалната информация чрез A_c във формула (1). В този случай е удобно да се премине от абсолютни към относителни стойности на $C_к$:

$$(2) \qquad C_k / A_k = (1 - e^{-\frac{V_k}{V_0}}) e^{-\frac{\tau_{zk}}{T_0}}$$

Като се осигуряват изчисления чрез серии итерации с последователно уточняване стийностите на мащабния множител $A_к$, като се използват методите основани на експертни оценки и статистически данни [1,3]

3. Подход за оценка и прогнозиране на риска при защита на конфиденциална информация

При така въведената в т. 2 постановка на проблема е възможен следният подход за решаване на общи типови задачи по защита на конфиденциалната информация. Приемливия риск [2,3] минимизира сумарните загуби за даден обект – физическо лице, организация, фирма, колектив или околна среда и т.н., свързани с достигането на конкретна поставена цел. От (1) се вижда, че при $V_k << V_o$ или $\tau_к >> T_o$ стойността $C_к \rightarrow 0$. За субекта S_k това означава невъзможност да приведе конфиденциалната информация в обезценено състояние, вследствие нейното остаряване във времето. Рисковата стойност се отличава от ценността на конфиденциалната информация за нейния собственик, която се определя чрез мащабния коефицент $A_к$ в парично изражение или по друга скала. Съвпадане е възможно само при $V_k \rightarrow \infty$ и $T_o \rightarrow 0$. От тук следва, че стойностите V_o и T_o изразяват кумулативността на конфиденциалната

информация, под която се разбира свойството минимален обем от данни да дават максимална информация за състоянието на обекта [1,5].

Добре известно е, че основният инструмент при разработване на различни варианти на бъдещи събития е сценарийното планиране. Този метод разделя предвидимите тенденции от непознатата несигурност, след което разиграва възможните им въздействия, ползвайки ограничен брой сценарии [3]. Нека тогава субектът S_k, принадлежащ към съвкупност n[1,N] разглежда k сценарии на развитие на събитията насочени към достигане на определена цел с позитивен ефект (печалба) F_k, която може да бъде постигната с вероятност P_p при загуби G_k, обезпечени с вероятност P_g. Тогава за обекта S_n печалбата $F_k = C_k$, т.е. се определя с рисковата стойност на конфиденциалната информация. При това, S_n предполага, че k-тия сценарий води до достигане на целта с вероятмост P_k, която характеризира определени обективни обстоятелства. Тогава за критерий за ефективността на k-тия сценарий може да бъде въведена величината

$$(3) \qquad Q_k = P_k(P_F F_k - P_G G_k)$$

която в дадения случай може да се определи като прогнозируема мярка за оправданост на риска. В (3) външната вероятност зависи от $P_G G_K$. Ако субектът S_n не предприема действия за обезценяване на конфиденциалната информация и вследствие на това не отиде към загуби G_k, получаването на печалбата $F_k=G_k$ е малко вероятно. С увеличаването на $P_G G_K$ тази вероятност трябва да нараства. Затова зависимостта $P_k(P_G G_K)$ е подходящо да се моделира чрез експоненциална функция:

$$(4) \qquad P_k(P_G G_k) = 1 - e^{-P_G G_K / Go}$$

Тук с G_o са означени загубите, свързани с реализацията на основния, базов сценарий, условно приет за единица на отчета. От (4) следва, че $P_k \rightarrow 0$ при $G_k << G_o$ или $P_G << 1$ и $P_k \leq 1$ при $G_k >> G_o$ и $PG \rightarrow 1$. От (4) и (3) може да се формулира прогнозна мярка за оправдаността на риска във вида:

$$(5) \qquad Q_k = (1 - e^{-P_G G_K / Go})(P_k G_k - P_g G_k)$$

Оптималният сценарий в най-важния за практиката случай за $P_F - P_G = 1$, съответства на решимостта и потенциалната възможност на субекта S_n да осигури със своите сили постигането на поставената цел. Тогава поставената задача може да бъде формулирана по следния начин: Съществува ли сценарий, при който (5) достига оптимум $Q_{опт.}$ и какви, в разглеждания случай, са загубите $G_{опт}$ в сравнение с $G_k=F_o$, където F_o е печалбата на базовия сценарий. Максимумът на (5) се определя от условието:

$$(6) \qquad \frac{dQ_k}{dG_k} = 0$$

което може да се преобразува в:

$$(7) \qquad G_k/G_o = ln[1 + (F_o - G_k)/G_o] = 0$$

Ако в разлагането на логаритъма, отчетем основния, първия член, то получаваме в приближен вид:

$$(8) \qquad G_{опт} = \frac{F_o}{2}$$

Следователно търсеният оптимум съществува. В частен случай той може да съответства и на базовия сценарий. Най-целесъобразните сценарии ще отговарят на загуби, съответстващи приблизително половината печалба. От (8) и (5) се получава, че:

(9) $$Q_{опт} = P_{опт} F_o/2$$

където $P_{опт} = 1 - e^{-Fo/2Go}$

Това равенство определя вероятността за постигане на печалба F_o при оптимален сценарий. Практически това означава, че ако субектът S_n планира мероприятия, свързани с разкриването или компрометиране на конфиденциалната информация, той трябва да бъде уверен, че очакваната печалба (най-често в паричен смисъл или друга изгода), два пъти не превишава разходите, свързани с реализацията на най-добрия сценарий.

В съответствие с фиг. 1 на субекта S_n, решаващо при k-тия сценарий, на задачата за достигане на печалба F_k, противостои неговия противник D_n, решаващ противоположна задача. Субектът S_n рискува, D_n се защитава, осигурявайки своята безопасност. Успехът на S_n и обратния резултат, успехът на противника му D_n трябва да образуват пълна група събития. Тогава в качеството на критерий на ефективността на противодействие на k-тия сценарий D_n, може да се определи величината:

(10) $$W_k = (1-P_k)(P_F F_k - P_H H_k)$$

Тук P_H е вероятността за реализиране на загуба H_k, насочени към противника с цел предотвратяване на печалбата му F_k, която той с вероятност P_F може да достигне в рамките на k-тия сценарий. По аналогия с равенство (3), стойността на W_k може да се определи като прогнозируема мярка за ефективността на защита.

Изводи

Защитата на конфиденциалната информация изисква комплексни, включително финансови разходи, които е необходимо да се измерват с цената на риска в условията на използване на динамично развиващите се съвременни информационни технологии. Синтезираните в предложената работа сравнително прости от гледна точка на математиката и логиката модели (3) и (10) са полезни в такъв смисъл, че позволяват обективно да се проследят стратегическите закономерности на субекта S_n и неговия противник Dn, преследващи противоположни цели. За решаването на тактически въпроси, свързани с динамиката на развитие на събитията на фиг.1 е необходимо да се проведе допълнителен анализ на особеностите за оперативна оценка на прогнозирана мярка за оправданост на риска, респективно на ефективността на защитата. В този случай наред с предложените упростени модели, в зависимост от спецификата на решаваната задача може да се окаже целесъобразно тяхното усложняване и универсализация чрез използване на вероятностни функции, принадлежащи на семейство устойчиви закони и опиращи се на фундаментални гранични теореми на съвременната теория на вероятностите [5] .

ЛИТЕРАТУРА

[1] Schemaker P. Strategies for Succeeding No Matter Wat the Future Brings. Profiting from Uncertainty, 2005
[2] Bozek F., R. Urban, Manegemet rizika, Brno, 2008
[3] Dohery N. Integrited Risk Management, NJ:M/c Graw – H-ll, 2000
[4] Jednot A., Analiza a rizeni rizik v doprave. Praha, BEN, 2008

ANALYSIS AND RISK ASSESSMENT IN THE PROTECTION OF INFORMATION MANAGEMENT SYSTEMS ANALYSIS

Hristina Spiridonova, Antonio Andonov, Mariana Mihova
hristinaspiridonova@abv.bg, andonov@vtu.bg

Todor Kableshkov University of Transport,
158 Geo Milev Street, Sofia 1574,
BULGARIA

Key words: *information Security, risk, confidential information*

Abstract*:In modern business processes protecting confidential information is important the component of the activity related to develop, support and managing the information technology. In this paper the measures proposed for forecasting quantity characteristics of the risk associated with the protection of confidential information in analytical systems of different designation Central to the these issues occupy tasks to select options for scenario planned alternatives, strategies, plans, etc., optimal with respect to one or another criterion. In the scientific literature on these problems exist noticeable differences between working with theory considered logical foundations of the choice axiomatics, general principles of coherence and rationality, and most applicable works are dedicated to construction of of specific models and procedures in significant part heuristicstical and applied nature*

In this situation of extreme topicality are questions about develop and systematization of theoretically justified methods capable of serving as a methodological basis for solving practical problems. Is thus intended of the proposed work is to propose an approach for prediction of quality characteristics of the risk in taking decisions relating to the protection of confidential information in analytical systems. Received assessments of projected levels of risk at impact on Confidenciality information to its devaluation as well as of the effectiveness of its protection, allowing to track down regularities of strategic behavior of the entities involved pursuing conflicting objectives.