УДК 004.7

В. О. Шапорин,
П. М. Тишин, **Р. О. Шапорин**, кандидаты техн. наук

ЛИНГВИСТИЧЕСКАЯ ОЦЕНКА АКТИВОВ СЛОЖНОЙ КОМПЬЮТЕРНОЙ СИСТЕМЫ ДЛЯ АНАЛИЗА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. *Предлагается подход к построению диаграмм активов информационной безопасности с использованием аппарата нечеткой логики. Рассмотрен процесс выявления активов, формирования отношений вреда между ними, а также построение термов оценок выявленных активов. Предлагается модель описания и оценивания активов организации, которая может входить в состав единого комплекса по оценке рисков информационной безопасности.*

Ключевые слова: *информационная безопасность, информационная система, компьютерная сеть, методология Coras, нечетка логика, лингвистические термы*

V. O. Shaporin,
P. M. Tishin, PhD., **R. O. Shaporin,** PhD.

LINGUISTIC VALUATION OF ASSETS OF INFORMATION SYSTEM FOR ANALYSIS INFORMATION SECURITY RISKS

Abstract*. An approach to diagramming information security assets using fuzzy logic. The process of identifying assets, formation damage relations between them, as well as the construction of the term assessments of identified assets. A model of the description and evaluation of the organization's assets, which may be part of a common set of risk assessment of information security.*

Keywords*: information security, information system, computer network, Coras method, fuzzy logic, linguistic terms*

В. О. Шапорін,
П. М. Тишин, Р. О. Шапорін, кандидати техн. наук

ЛІНГВІСТИЧНА ОЦІНКА АКТИВІВ ІНФОРМАЙНОЇ СИСТЕМИ ДЛЯ АНАЛІЗА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація*. Пропонується підхід до побудови діаграм активів інформаційної безпеки з використанням апарату нечіткої логіки. Розглянуто процес виявлення активів, формування відносин шкоди між ними, а також побудова термів оцінок виявлених активів. Пропонується модель опису та оцінювання активів організації, яка може входити до складу єдиного комплексу з оцінки ризиків інформаційної безпеки.*

Ключові слова*: інформаційна безпека, інформаційна система, комп'ютерна мережа, методологія Coras, нечітка логіка, лінгвістичні терми*

Введение. Проектирование информационной безопасности [1] состоит из множества этапов, самыми скрупулезными и длительными из которых являются анализ рисков безопасности и построение политик безопасности.

Когда решается задача анализа рисков [1], в первую очередь следует определить активы системы, которые подлежат защите. Затем производится оценка выявленных активов по определенным критериям. Однако, оценка активов, зачастую, субъективна и не отражает реальное состояние системы. Связано это с тем, что оценку, кроме специалистов информационной безопасности, проводит группа сотрудников предприятия имеющих различные представления о безопасности информации, последствиях нарушения этой безопасности и о ценности актива как такового. В связи с этими же сложностями тяжело определить влияние вреда одного актива на вред другого актива.

В области анализа рисков достаточно давно успешно применяется методология Coras [2], которая позволяет языком диаграмм описывать процессы, происходящие в информационной системе, проводить описание активов, угроз и рисков.

Постановка задачи. Разработка методов и инструментальных средств, которые позволяют автоматизировать мероприятия по оценке активов и их взаимного влияния.

Для решения поставленных задач предлагается использовать аппарат нечеткой ло-

гики [3 – 5]. Это с одной стороны внесет больший уровень достоверности и объективности в данные оценки, поскольку многие величины нельзя задать количественно. С другой стороны позволят провести качественную оценку моделируемых ситуаций.

Определение активов. Для определения рисков и угроз ИС необходимо построить диаграмму активов, которая позволит выявить сами активы и их оценку. При построении диаграммы активов необходимо определить участника, его активы и отношение вреда между активами.

Рассматривается некоторая организация, требующая разработки политики безопасности. Как правило, среди основных непрямых активов организации можно определить финансы организации (Company Finance, CF) и ее репутацию (Company Reputation, CR). Основные области для защиты любой ИС являются доступность, целостность и конфиденциальность.

Однако при практическом применении анализа активов предприятия следует более глубоко рассматривать данные области рисков:

– с точки зрения доступности рассматриваются доступность легальных пользователей системы (User availability, Ua), доступность сегментов сети (LAN availability, La) и доступность сервера (Server availability, Sa);

– с точки зрения целостности рассматриваются целостность сервера (Server integrity, Si) и целостность информации (Information integrity);

– с точки зрения конфиденциальности рассматривается конфиденциальность информации (Information confidentiality, Ic).

Выявление данных активов предусматривает тесное взаимодействие проектировщика системы анализа рисков и ключевых фигурантов ИС организации.

Определение отношений. При построении диаграмм активов возможно только одно качественное отношение – отношение вреда (harm). Следовательно, задача сводится только к количественному определению отношений типа «кто с кем». Для решения данной задачи проводится построение диаграммы активов с использованием методологии Coras (рис. 1). Построенные отношения носят причинно-следственный характер, что проявляется при оценивании активов. Процесс построения отношений основывается на логике работы ИС организации, архитектурных особенностей телекоммуникационной системы организации и мнении уполномоченных лиц, принимающих участие в проектировании политик безопасности.

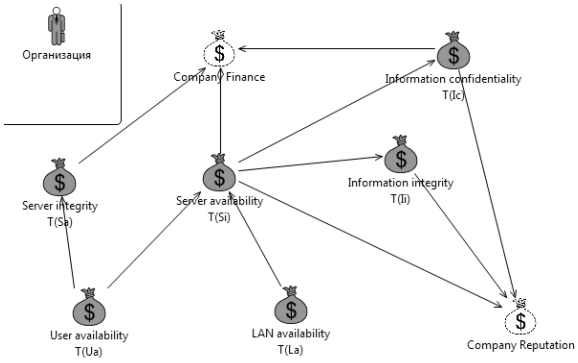


Рис. 1. Диаграмма активов Coras

Построение термов оценок. После определения активов и отношений между ними, оценивание данных активов и определение силы связей отношений производится с помощью лингвистических переменных [6 – 7].

При оценивании активов CF, CR, Si, Sa, Ii, Ic, La, Ua достаточно сложно дать количественную оценку ущерба активу или его собственную ценность. По этому предлагается ввести качественные оценки в лингвистических терм-множествах. Для адекватного восприятия оценки активов принята градация из пяти оценок:

$$T(x) = \{t_н, t_м, t_{ср}, t_в, t_{кр}\},$$

где $t_н$ – незначительна важность; $t_м$ – низкая важность; $t_{ср}$ – средняя важность; $t_в$ – высокая важность; $t_{кр}$ – критическая важность.

Данное терм-множество оценок позволяет назначить каждому активу адекватную степень важности, $x \in \{CF, GR, Si, Sa, Ii, Ic, La, Ua\}$.

Качественное описание отношений между активами предлагается выражать также в виде терм-множеств. Однако, в отличие от активов, данные множества должны характеризовать степень влияния вреда одного актива на другой актив.

Поэтому сконструирован следующий набор термов:

$$C(y) = \{c_л, c_c, c_m\},$$

где $c_л$ – легкие последствия; c_c – средние последствия; c_m – тяжелые последствия, y = {*Ua→Sa, La→Sa Ua→Si Sa→Ii Sa→Ic Sa→CF, Si→CF, Ic→CF Sa→CR, Ii→CR, Ic→CR* }.

Представленные множества $T(x)$ и $C(x)$ позволяют дать описание диаграммы активов в виде лингвистических переменных $\tilde{p}_i, i = 1..\tilde{N}_P$, где $\tilde{N}_P$ – количество лингвистических переменных. Для каждой лингвистической переменной определено полное ортогональное семантическое пространство (ПОСП) [8].

Для этого на множествах значений лингвистических переменных D_i, системы, определим множества нечетких термов $\widetilde{D}_i = \{\tilde{p}_i^k\}_{k=1..K_i}$, где K_i – количество термов для i-ой лингвистической переменной.

Каждое нечеткое число $\tilde{p}_i^k \in \widetilde{D}_i$ определим через функцию принадлежности следующего вида:

$$\tilde{p}_k^i \Rightarrow \mu_k^i(p_i') = \begin{cases} 0, & p_i' \le p_{kb}^i, p_i' \ge p_{ke}^i \\ \dfrac{p_i' - p_{kb}^i}{p_{kb_1}^i - p_{kb}^i}, & p_{kb}^i < p_i' < p_{kb_1}^i \\ 1, & p_{kb_1}^i \le p_i' \le p_{ke_1}^i \\ \dfrac{p_i' - p_{ke}^i}{p_{ke_1}^i - p_{ke}^i}, & p_{ke_1}^i < p_i' < p_{ke}^i \end{cases}, \quad (1)$$

$$i = 1..\tilde{N}_P, k = 1..K_i$$

где p_i' – некоторое четкое значение i-ой лингвистической переменной; p_{kb}^i, p_{ke}^i – начальное и конечное значения соответственно интервала значений базового множества D_i; на котором функция принадлежности k-го нечеткого значения i-ой лингвистической переменной положительно определена; $p_{kb_1}^i, p_{ke_1}^i$ – начальное и конечное значения соответственно интервала значений базового множества D_i, на котором функция принадлежности k-го нечеткого значения i-ой лингвистической переменной равна единице.

Относительно функций (1) предполагается выполнение следующих условий:

$$\begin{cases} \mu_k^i(p_i') = 1 - \mu_{k-1}^i(p_i'), p_{kb}^i < p_i' < p_{kb_1}^i \\ \mu_k^i(p_i') = 1 - \mu_{k+1}^i(p_i'), p_{ke_1}^i < p_i' < p_{ke}^i \end{cases}, \quad (2)$$

$$k = 2..(K-1)$$

$$\begin{cases} p_{1b}^i = p_{1b_1}^i = \min\limits_{D_i}(p_i) \\ p_{Ke}^i = p_{Ke_1}^i = \max\limits_{D_i}(p_i) \end{cases}, \quad i = 1..\tilde{N}_P \quad (3)$$

В условиях (1 – 3) выполняются соотношения

$$\mu_1^i \prec_{\widetilde{D}_i} \mu_2^i \prec_{\widetilde{D}_i} ... \prec_{\widetilde{D}_i} \mu_{K_i}^i, \quad (4)$$

где $\prec_{\widetilde{D}_i}$ – отношение строго порядка на множестве нечетких значений i-ой лингвистической переменной.

Данное отношение (4), можно использовать для сравнения значений получаемых i-ой лингвистической переменной и проведения выбора наиболее удовлетворяющих оценок и значений в рамках рассматриваемой системы.

При построении диаграммы активов приняты следующие элементы и отношения:

Party = p (название) – участник;

заинтересованное лицо, требующее защиты активов;

Direct Asset = da (название, оценка) – прямой актив, подлежащий оценке;

Indirect Asset = ia (название, оценка) – непрямой актив, подверженный влиянию прямых активов;

Harm = da→da, da→ia – отношение вреда между активами рассматриваемой системы.

В итоге, сформированная диаграмма активов качественно описывается следующим образом:

The_main = p (организация);

Ua = da (User availability, (T_{Ua}));

La = da (LAN availability, (T_{La}));

Sa = da (Server availability, (T_{Sa}));

Si = da (Server integrity, (T_{Si}));

Ii = da (Information integrity, (T_{Ii}));

Ic = da (Information confidentiality, (T_{Ic}));

CR = ia (Company Reputation, (⊥));

CF = ia (Company Finance, (⊥)),

где $T_{Ua}, T_{La}, T_{Sa}, T_{Si}, T_{Ii}$ – выбранные термы соответствующих лингвистических переменных $x \in \{CF, GR, Si, Sa, Ii, Ic, La, Ua\}$.

Отношения вреда в разработанной модели несут следующий смысл:

Ua→Sa, La→Sa – влияние на оценку актива «доступность сервера» оценок «доступность пользователя» и «доступность сети» с учетом причиненного вреда.

При этом лингвистическая переменная $C(Ua \to Sa)$, описывает влияние для отношения *Ua→Sa,* а лингвистическая переменная $C(La \to Sa)$, описывает влияние для отношения *La→Sa:*

Ua→Si – влияние на оценку актива «целостность сервера» оценки «доступность пользователя». При этом лингвистическая переменная $C(Ua \to Si)$, описывает влияние для отношения *Ua→Si*;

Sa→Ii – влияние на оценку актива «целостность информации» оценки «доступность сервера».

При этом лингвистическая переменная $C(Sa \to Ii)$, описывает влияние для отношения *Sa→Ii*:

Sa→Ic – влияние на оценку актива «конфиденциальность информации» оценки «доступность сервера». При этом лингвистическая переменная $C(Sa \to Ic)$, описывает влияние для отношения *Sa→Ic*.

Влияние на непрямые активы:

Sa→CF, Si→CF, Ic→CF – каково влияние на финансовое состояние организации вреда активам «доступность сервера», «целостность сервера» и «конфиденциальность информации».

При этом лингвистические переменные $C(Sa \to CF)$, $C(Si \to CF)$, $C(Ic \to CF)$, описывают влияние для отношений *Sa→CF, Si→CF, Ic→CF:*

Sa→CR, Ii→CR, Ic→CR – каково влияние на репутацию организации вреда активам «доступность сервера», «целостность информации» и «конфиденциальность информации».

При этом лингвистические переменные $C(Sa \to CR)$, $C(Ii \to CR)$, $C(Ic \to CR)$, описывают влияние для отношений *Sa→CR, Ii→CR, Ic→CR*.

Заключение. Полученная модель активов и их взаимоотношений с использованием указанных нечетких лингвистических термножеств позволяет достигнуть большей степени автоматизации процесса анализа и расчета рисков ИС благодаря возможности качественного описания ситуации. Это позволяет снизить влияние человеческого фактора в оценку рисков и ценности активов ИС.

Список использованной литературы

1. Радько Н. М. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа // Н. М. Радько, И. О. Скобелев. – М. : РадиоСофт, 2010. – 232 с.

2. Mass Soldal Lund, Bjornar Solhaug, Ketil Stolen, (2011), Model-Driven Risk Analysis. Berlin. Springer-Verlag, pp. 55 – 62.

3. . Шапорин В. О. Нечеткие лингвистические модели обеспечения безопасности компьютерных сетей / В. О. Шапорин, П. М. Тишин, Н. Б. Копытчук, Р. О. Шапорин // Современные информационные и электронные технологии: 14-я международная научно-практическая конференция. – Одесса : – С. 155 – 156.

4. Шапорин В. О. Оценка вероятности проведения атаки на сетевые ресурсы с использованием аппарата нечеткой логики / В. О. Шапорин, П. М. Тишин, Н. Б. Копытчук, Р. О. Шапорин // Электротехнические и компьютерные системы. – К. : Техника. – 2013.– № 12 (88). – С. 95 – 101.

5. Шапорин В. О. Разработка нечетких лингвистических моделей атак для анализа рисков в распределенных информационных системах / В. О. Шапорин, П. М. Тишин, Н. Б. Копытчук, Р. О. Шапорин //Современные информационные и электронные технологии: 15-я международная научно-практическая конференция. – Одесса : – С. 131 – 132.

6. Нестеренко С. А. Модель онтологии априорного подхода прогнозирования проблемных ситуаций в сложных вычислительных системах / С. А. Нестеренко, П. М. Тишин, А. С. Маковецкий // Электротехнические и компьютерные системы. – 2013. – К. : Техника. – № 10 (86). – С. 111 – 119.

7. Копытчук Н. Б. Процедура создания нечетких моделей анализа рисков в сложных вычислительных системах / Н. Б. Копытчук, П. М. Тишин, М. В. Цюрупа // Электротех-

нические и компьютерные системы. – К. : Техника. – 2014. – № 13 (89). – С. 215 – 222.

8. Рыжов А. П. Элементы теории нечетких множеств и ее приложений. – М. : – 2003. Диалог-МГУ. – С. 53 – 65.

Получено 24.03.2015

References

1. Radko N.M., and Skobelev I.O. Risk-models Informatsionno-telekommunikatsionnyih Sistem pri Realizatsii Ugroz Udalennogo i Neposredstvennogo Dustup, [Risk Model for Information and Telecommunication Systems in the Realization of threats Remote and Immediate Access], (2010), Moscow, Russian Federation, *RadioSoft,* 232 p. [In Russian].

2. Mass Soldal Lund, Bjornar Solhaug, and Ketil Stolen, (2011). Model-Driven Risk Analysis. Berlin, Springer-Verlag, pp. 55 – 62.

3. Shaporin V.O., Tishin P.M., Kopytchuk N.B., and Shaporin R.O., Nechetkie lingvisticheskie modeli obespecheniya bezopasnosti kompyuternyih setey, [Fuzzy Linguistic Models of Computer Network Security], (2013), *Modern Information and Electronic Technologies, 14th International Scientific and Practical Conference*. Odessa, Ukraine, pp. 155 – 156 (In Russian).

4. Shaporin V.O., Tishin P.M., Kopytchuk N.B., and Shaporin R.O. Osaka Veroyatnosti provedeniya ataki na setevyie resursyi s ispolzovaniem apparata nechetkoy logiki, [Assessment of the Possibility of Attacks on Network Resources Using Fuzzy Logic], (2013), *Electrotechnic and Computer Systems,* Kiev, Ukraine, *Technical*, No. 12 (88), pp. 95 – 101 (In Russian)

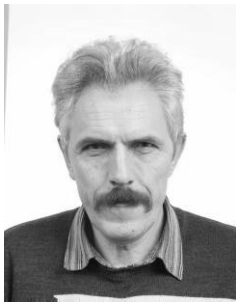
5. Shaporin V.O., Tishin P.M, Kopytchuk N.B., and Shaporin R.O., Razrabotka nechetkih lingvisticheskih modeley setevyih atak dlya analiza riskov v raspredelennyih informatsionnyih sistemah, [Development of Fuzzy Linguistic Models of Network Attacks for Risk Analysis in Distributed Information Systems], (2013), *Modern Information and Electronic Technologies: 15th International Scientific and Practical Conference*. Odessa, Ukraine, pp 131 – 132 (In Russian).

6. Nesterenko S.A., Tishin P.M., and Makovetskiy A.S. Model ontologii apriornogo podhoda prognozirovaniya problemnyih situatsiy v slozhnyih vyichislitelnyih sistemah [The Ontology Model of the Apriority Approach Predicting Problematic Situations in Complex Computer Systems], (2013), *Electrotechnic and Computer Systems,* Kiev, Ukraine, No. 10 (86), pp. 111 – 119 (In Russian).

7. Kopytchuk N.B., Tishin P.M., and Tsyurupa M.V. Protsedura sozdaniya nechetkih modeley analiza riskov v slozhnyih vichislitelnyih systemic, [Creation Procedure of the Fuzzy Risk Assessment Model for Complex Computer Systems], (2014), *Electrotechnic and Computer Systems,* Kiev, Ukraine, No. 13 (89), pp. 215 – 222 (In Russian).

8. Ryjov A.P., Elementyi teorii nechetkih mnozhestv i ee prilozheniy, [Elements of the theory of Fuzzy Sets and its Applications], (2003), Moscow, Russian Federation, *Dialog-MGU,* pp. 53 – 65 (In Russian).

Шапорин
Владимир Олегович,
ст. преподаватель
каф. компьютерных
интеллектуальных
систем и сетей
Одесского нац. политехн.
ун-та, м/т 093-5643450.
E-mail:
shaporin_v@ukr.net



Тишин
Петр Металинович,
канд. физ.-мат. наук,
доц. каф. компьютерных
интеллектуальных систем
и сетей Одесского нац.
политехн. ун-та,
м/т 098-8050448.
E-mail: tik88@mail.ru

Шапорин
Руслан Олегович,
канд. техн. наук, доц.
каф. компьютерных ин-
теллектуальных систем и
сетей Одесского нац. по-
литехн. ун-та,
м/т 067-4877362.
E-mail: shaporin@ukr.net