# КОЛИЧЕСТВЕНА ОЦЕНКА НА КИБЕРРИСКА

**Боян Жеков, Васил Панайотов, Светлана Сярова**
*Университет по библиотекознание и информационни технологии*

**Резюме:** Оценката на риска е процесът на идентифициране, оценка и приоритизиране на рисковете за информационната сигурност. Тя изисква внимателен анализ на заплахите и уязвимостта на информацията. Предложен е метод, базиран на сравнение и оценка на сценарии на метода на двойните сравнения, чрез който се обобщават, систематизират и развиват практическите резултати от обработката на нечислова информация във връзка с оценката на риска на корпоративна система.

**Ключови думи:** киберриск, количествена оценка, нечислова информация.

## Въведение

Много от значимите рискове на днешните организации възникват във киберпространството и техните последици могат да имат пряко въздействие върху финансовите и оперативните дейности. В същото време глобалните щети от киберинциденти нарастват от година на година.

Защитата на информацията е първостепенна задача в новите условия на интернет. Загуба или кражба на тази информация би предизвикала спиране на услугите или компрометиране на цялата институция, предлагаща тази услуга. Това води след себе си големи загуби, включително финанси, репутация и др. Следва да се отбележи също, че човешкият фактор и съпътстващият контрол са от изключително значение при внедряването и използването на нови технологии за защита в различните сектори. Дори при най-модерните закупени технологии е необходим персонал, подготвен да борави с тях [1].

През последните години се наблюдава нарастваща зависимост на бизнеса от информационните технологии, което налага сериозно пренасочване на инвестиционните потоци към развитие на тези технологии. Инвестициите за развитие на дадено информационно решение следва да са насочени както към неговото технологично развитие, така и към подобряване на неговата сигурност. Първото и основно изискване на бизнеса е винаги едно решение да е максимално използваемо. На второ място, се очаква то да предоставя богата функционалност, а сигурността е приоритет преди всичко при възникване на проблем.

Оценката на риска е процесът на идентифициране, оценка и приоритизиране на рисковете за информационната сигурност. Тя изисква внимателен анализ на заплахите и уязвимостта на информацията чрез определяне на степента, до която обстоятелства или събития биха могли да окажат отрицателно въздействие върху организацията, и вероятността, с която ще възникнат такива обстоятелства или събития.

**Понятие за киберриск**

Сигурността винаги е относителна. Тя зависи правопропорционално от усилията, влагани за поддържане на определено ниво на сигурност, адекватността му по отношение на потенциални интрузионни възможности, влиянието на случайните фактори или наличието на грешки в етапа на синтезиране на определена система [2].

Щом не може да е абсолютна, то каква информационна сигурност може да се постигне и как да се поддържа?

Отговорът се крие в адекватното съответствие между сигурност и вероятни заплахи. В този аспект е необходимо да се оцени вероятността на възможните атаки срещу слабите места на системата и да се балансира стойността на защитата (включително изискванията на бизнеса) спрямо ценността на обектите, които защитава. Подробен метод за това е даден в [3]. Оценяването на мрежовата сигурност може да се свърже с оценката (финансовата стойност) на евентуалните загуби. С изключение на специални организации (военни, секретни, антитерористични, специални частни изследователски лаборатории), при които загубата на информация не може да се измери количествено, принципът на икономическия баланс е водещ.

От съществено значение при определяне на нивото на сигурността е необходимостта от оценка на възможните атаки по отношение на вероятните атаки. Оценката на вероятността за провеждане на успешна атака се нарича оценка на риска. Оценката на риска е от решаващо значение за успешното изграждане и провеждане на стратегията за постигане на определено ниво на информационна сигурност.

**Методология на изследването**

Рискът се оценява въз основа на следните два фактора:

1. Вероятността да се случи нежеланото събитие. Този фактор се нарича също „честота“;

2. Видът и размерът на щетата, за които се използва понятието „потенциал за възникване на щети“.

Рискът се изчислява по формулата:

| Риск = Честота х Потенциал за възникване на щети |
|---|

В горното равенство двата фактора: честота и потенциал за възникване на щети, се оценяват като еднакво значими, т.е. може да се приеме, че един често повтарящ се малък инцидент крие същите рискове, както една рядко случваща се голяма авария.

Съставя се списък от фактори, които влияят на показателя „Вероятност“ и на показателя „Щети“. На фиг. 1 са дадени елементите, които се включват в двата фактора.


*Фиг. 1. Система риск – фактор*

**Управление и минимизиране на риска**

Кибератаките са вече ежедневие в глобален мащаб. Свидетели сме, че ако не всеки ден, то поне всяка седмица или няколко пъти в месеца поредна голяма уебуслуга губи контрол над своята база данни. В същото време компаниите и потребителите се опитват да бъдат поне на крачка пред злонамерените актьори на дигиталната сцена. Колкото и да мразим постоянните хакерски набези и изтичането на данни, те са тук с единствената идея да останат задълго и да нанесат възможно най-големи щети. Един подобен пробив не трябва да предизвиква тотална паника, без значение колко значителни могат да бъдат откраднатите данни.

Хакерите постоянно успяват да откраднат данни от различни системи, но много често тези данни се оказват практически неизползваеми благодарение на практиките за сигурност, които включват термини като „хеширане“, „осоляване“ и „кодиране“. Ако обаче данните са под формата на чист и разбираем текст, това означава, че в случая не е използвана криптография и разчитането им е също толкова лесно, колкото на документ в Word или обикновен имейл. При хеширане данните се кодират по такъв начин, че не могат да бъдат декодирани обратно в обикновен текст. Затова тази техника е често използвана за защита на бази данни. Трябва да имате предвид обаче, че не всички методи за хеширане са еднакви и понякога това се оказва обратим процес. Затова като втора линия на защита една компания може да добави и друга функция за кодиране, наричана „осоляване“.

При методите за идентифициране на риска се изгражда информационен регистър на рисковете (понякога наричан „портфолио на риска“), които са известни и значими за системата.

Дефинирани са три основни метода за идентифициране на риска при анализ на конкретни процеси:

1. Метод на анализа на статистически данни от минали неблагоприятни събития;

2. Метод на теоретичния анализ на структурата на причинно-следствените връзки между отделни изследвани процеси;

3. Метод на експертния подход.

Изборът на метод за идентифициране на риска се основава на ресурсите, с които разполага фирмата и на наличието на достоверни данни от предишни или настоящи изследвания на риска в конкретна или подобна среда. Оптимално решение за оценката на риска е използването и миксирането на няколко метода за получаване на по-точни резултати.

**Резултати**

**Модел за оценка на риска**

От съществено значение за концептуалния модел на предлаганата система са видът и връзките между елементите в общата структура. Изборът на структура определя впоследствие логиката на обработката и анализа ѝ.

Важен акцент от предложеното определение е количествената оценка на риска. Тази оценка е възможност, от една страна, да се съпоставят различните източници на риск в процеса на управлението им и от друга страна, да се сравнят различни рискови среди. Без наличие на количествено оценяване на източниците на риск не може

да се реализира ефективна система за управление на риска. Дори в случаите, когато източниците на риска са оценени с грешка в сравнение с действителните стойности, това е по-добрият вариант.

Дадени са:

1. $R = (r_1, r_2, \dots, r_k)$ е наборът от разглеждани рискове за информационната сигурност на корпоративната система.

2. Всеки от разглежданите рискове за информационната сигурност на корпоративната система се характеризира с вектор от характеристики:

$$y(g) = \left(y_1(g), y_2(g), \dots, y_p(g), y_{p+1}(g), \dots, y_n(g)\right),$$

където $y_t(g), t = 1, \dots, p$ са нечислови характеристики на анализирания риск $r_g$,

$y_j(g), j = p + 1, \dots, n$ – числени характеристики.

3. Приема се, че одиторът разполага с коефициенти за тегло на риска $k_m$, които отчитат числовите параметри

$$y_j(g), j = p + 1, \dots, n, l = p + 1 \dots, n, m = p = 1, \dots, n.$$

За числовите параметри това не е трудна задача. Коефициентът на тегло $k_m$ е цяло положително число и носи информация за сравнителния риск $r_l$ спрямо риска $r_m$ за разглежданата характеристика. Използва се само за нареждане на рисковете $R = (r_1, r_2, r_3, \dots, r_k)$ и определяне на приоритетните действия за предотвратяване на инциденти.

**Изводи/Дискусия**

Поставената формализирана задача се среща в практиката на съвременния контрол на информационната сигурност на корпоративните системи. Един от вариантите на нейното решение се основава на резултатите от математическите методи на теорията на квалиметричните скали, модела на линейното подреждане на алтернативи и сравнения по двойки [4], [5]. Всички различни от горните методи не позволяват решаването на проблема с приемлива за практически нужди и разходи за изчислителни ресурси точност.

Посочената в таблица 1 скала в линеен ред извършва количественото определяне на качествените субективни преценки на експерта за нивото на риска $r_g$ чрез фиксирана характеристика $y_i(g), i = 1, \dots, p$, описана с нечислова стойност.

*Таблица 1. Количествени оценки на експерта за нивото на риска*

| **Квалиметрични точки от скалата $h_i$** | **Определяне на значението** | **Коментар относно определяне на значението** |
|---|---|---|
| $h_0$ | Значимостта на анализирания риск е практически ниска. | Експертът смята, че има малък или никакъв риск. |
| $h_2$ | Значимостта на анализирания риск е умерена. | Експертът смята, че има риск. |
| $h_4$ | Значимостта на анализирания риск е съществена. | Експертът смята, че рискът е съществен. |
| $h_1, h_3, h_5$ | Междинни оценки между две съседни оценки. | Използва се в компромисни случаи. |
| $h_6$ | Значимостта на анализирания риск е много силна. | Експертът смята, че има голям риск. |

Нека рискове $r_t$ и $r_s$ според фиксирана нечислова характеристика да бъдат приписани от одитора на риск $r_t$ до точка $h_p$ от линейната квалиметрична скала от порядък:

$S =< H, R >>$, където $H = (h_1, h_2, h_3, h_4, h_5, h_6)$, двойка $(h_i, h_{i+1}) \in R\ i = 0,1, \dots,5, h_i, i = 1,..,6$ – точки в таблица 1 на скалата $S, R >$ – отношение на строго линеен ред, определен на носителя $H$ и риск $r_s$ до точка $r_q$, p≠q.

Общото наличие на риск изчисляваме по формулата:

$$R_{all} = \sum R_I,$$

където $R_{all}$ е резултатът от сумирането на всички точки.

**Заключение**

Навременността и коректността на оценката на информационните рискове на компанията до голяма степен определят ефективността на системата за информационна сигурност [6]. В предложения метод, базиран на сравнение и оценка на сценарии на метода на двойните сравнения, се обобщават, систематизират и развиват практическите резултати от обработката на нечислова информация във връзка с

оценката на риска на корпоративна система. Резултатите от работата могат да бъдат използвани за създаване на нов, по-ефективен и практически обоснован подход за оценка на информационните рискове на една компания и създаване на подходящ софтуерен продукт.

**References/Литература**

1. **Ader**, H. J. Modelirovaniye. – V: **Adèr**, H. J., Dzh. Dzh. **Mellenberg** (Red.). Konsul'tatsii po metodam issledovaniya: naparnik konsul'tanta. Huizen, Niderlandy: Johannes van Kessel Publishing, 2008, s. 271 – 304.

[**Адер**, Х. Дж, „Моделирование", в **Адер**, Х. Дж; **Мелленберг**, Дж. Дж. (Ред.), Консультации по методам исследования: напарник консультанта, Huizen, Нидерланды: Johannes van Kessel Publishing, 2008, с. 271 – 304].

2. **Koks**, D. R. Printsipy statisticheskogo vyvoda. Cambridge University Press, 2006.

[**Кокс**, Д. Р., Принципы статистического вывода, Cambridge University Press, 2006].

3. **Radulov**, N. SIGURNOST 4.0. Nauchnotehnicheski sayuz po mashinostroene „Industriya 4.0". ISBN 978-619-7383-15-7.

[**Радулов**, Н., СИГУРНОСТ 4.0, Научнотехнически съюз по машиностроене „Индустрия 4.0. ISBN 978-619-7383-15-7]

4. **Konishi**, S., G. **Kitagava**. Informatsionnyye kriterii i statisticheskoye modelirovaniye. Springer, 2008.

[**Кониши**, С., Г. **Китагава**, Информационные критерии и статистическое моделирование, Springer, 2008].

5. **ABernem**, K. P., D. R. **Anderson**. Vybor modeli i mnogomodel'nyy vyvod (2-ye izd.). Springer-Verlag, 2002.

[**Бернем**, К. П; **Андерсон**, Д. Р., Выбор модели и многомодельный вывод (2-е изд.), Springer-Verlag, 2002].

6. **Kalchev**, K. Izmervane na parametri v sistemite za kibersigurnost. VA „Georgi Stoykov Rakovski", 2018. ISBN 978-619-7478-04-4.

[**Калчев**, К., Измерване на параметри в системите за киберсигурност, ВА „Георги Стойков Раковски", издател, 2018. ISBN 978-619-7478-04-4]

**За авторите**

**Боян Жеков** е заместник-декан на ФИН на УниБИТ. Професионалните му интереси са в областа на киберсигурността и метавселената. Координатор е на редица проекти в тези области.

За контакт с автора: b.jekov@unibit.bg

**Васил Панайотов** е завършил магистратура и защитил дисертация по киберсигурност в катедра „Национална сигурност“ към ФИН на УниБИТ. Понастоящем работи в бизнеса.

За контакт с автора: panayotov@gmail.com

**Светлана Сярова** е главен асистент в катедра „Компютърни науки“ към ФИН на УниБИТ. Професионалните ѝ интереси са в областта на киберсигурността.

За контакт с автора: s.syarova@unibit.bg

# QUANTITATIVE ASSESSMENT OF CYBER RISK

**Boyan Jekov, Vasil Panayotov, Svetlana Syarova**
*University of Library Studies and Information Technologies*

**Abstract:** Risk assessment is the process of identifying, assessing and prioritizing information security risks. It requires careful analysis of the threats and vulnerabilities of information. A method based on comparison and evaluation of scenarios of the double comparison method is proposed, through which the practical results of the processing of non-numerical information in connection with the risk assessment of a corporate system are summarized, systematized and developed.

**Keywords:** cyber risk, quantitative assessment, non-numerical information.

**About the authors**

**Boyan Jekov** is Deputy Dean of the Faculty of Information Sciences at ULSIT. His professional interests are in the field of cybersecurity and the meta universe. He is the coordinator of a number of projects in these areas.

To contact the author: b.jekov@unibit,bg

**Vasil Panayotov** has a Master's degree and defended his dissertation on cybersecurity in the Department of National Security at the Faculty of Information Sciences at ULSIT. He is currently working in business.

To contact the author: panayotov@gmail.com

**Svetlana Syarova** is a senior assistant at the Department of Computer Sciences at the Faculty of Information Sciences at ULSIT. Her professional interests are in the field of cybersecurity.

To contact the author: s.syarova@unibit.bg