АНАЛИЗ МЕТОДОВ И СРЕДСТВ, ИСПОЛЬЗУЕМЫХ НА РАЗЛИЧНЫХ ЭТАПАХ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Миков Дмитрий Александрович

В работе анализируются возможности методов и средств оценки рисков информационной безопасности применительно к различным этапам процесса оценки. Построена схема процесса в виде вложенных алгоритмов с указанием взаимосвязей между всеми этапами. Рассмотрены наиболее эффективные способы реализации этих этапов.

***Ключевые слова**: информационная безопасность, оценка информационных рисков, факторы риска, метод Дельфи, коэффициент конкордации, симплекс–метод, искусственный интеллект, ожидаемые годовые потери, окупаемость инвестиций, внутренняя норма доходности.*

ANALISYS OF METHODS AND TOOLS WHICH ARE USED IN THE VARIOUS STAGES OF INFORMATION SECURITY RISK ASSESSMENT

Dmitry Mikov

This paper analyzes the possibilities of methods and tools to assess information security risks in relation to the various phases of evaluation process. A scheme of the process has been designed in the form of embedded algorithms showing the relationship between all stages. The most effective ways for implementation of these steps have been considered.

***Keywords**: information security, threat, damage, vulnerability, countermeasure, information security risk assessment, IDEFO, DFD, expert assessments, Delphi method, coefficient of concordance, fuzzy sets, neural networks, learning vector, soft–computing, hybrid models, annual loss expected, benefits, return on investment, internal rate of return.*

Введение

Управление информационной безопасностью имеет большое значение для любой организации, которая в своей деятельности использует современные технологии сбора, хранения и обработки информации. Неотъемлемой частью этого процесса является оценка рисков информационной безопасности, которую необходимо периодически проводить в целях эффективного внедрения мероприятий по управлению информационной безопасностью, учёта новых угроз и уязвимостей, а также изменений в требованиях и приоритетах деятельности организации.

В настоящее время для оценки рисков информационной безопасности используется множество различных методов и средств. В них предлагаются разные способы сопоставления возможного ущерба в результате инцидентов информационной безопасности с вероятностью реализации угроз и получения соответствующих выводов, предлагаются разные шкалы измерения уровня риска. При этом в исследованиях, изучающих и сравнивающих эффективность этих методов в различных условиях, не принимается во внимание немаловажный факт.

Оценка информационных рисков, несмотря на имеющиеся специфические для неё нюансы в различных сферах деятельности, представляет собой упорядоченный процесс, состоящий из одних и тех же этапов, на каждом из которых могут быть применены свои методы и средства. Поэтому первоочередное внимание в исследованиях такого рода следует уделять не результативности методов вообще, а их эффективности на том или ином этапе, возможностям их сочетаний и комбинаций, способам перехода от одного метода к другому,

обеспечивающим корректную интерпретацию результатов.

Задача настоящей работы – выделить и разграничить этапы процесса оценки информационных рисков, установить взаимосвязи между ними, определить набор возможных методов и средств оценки, наиболее подходящих и применимых к каждому из этапов.

1. Процесс оценки рисков информационной безопасности, его основные этапы и особенности

Теоретики и практики не дают единого универсального определения понятию риска информационной безопасности, поэтому в литературе существует несколько таких определений. В соответствии с ISACA (Ассоциация по аудиту и контролю информационных систем), это вероятность наступления события, которое будет оказывать нежелательный эффект на данную организацию и её информационные системы [1]. В соответствии с ГОСТ Р ИСО/МЭК 27005-2010, риск информационной безопасности – это возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесёт ущерб организации. Он измеряется исходя из комбинации вероятности события и его последствия [2]. Так или иначе, из всех определений следует, что риск информационной безопасности ($\boldsymbol{R}$) – это комплексная величина, определяемая как функция (или функционал) ряда факторов, а именно:

1) угрозы информационной безопасности ($\boldsymbol{X_1}$);
2) потенциально возможного ущерба ($\boldsymbol{X_2}$);
3) уязвимости информационной системы ($\boldsymbol{X_3}$).

Факторы $\boldsymbol{X_1}$ и $\boldsymbol{X_3}$ в совокупности и определяют вероятность наступления неблагоприятного события. Также влияние на уровень информационных рисков оказывают контрмеры – мероприятия по защите информации ($\boldsymbol{X_4}$). Таким образом, риск информационной безопасности можно представить в виде следующей функции:

$$R = f(X_1, X_2, X_3, X_4)$$

В свою очередь, каждый из факторов информационного риска включает в себя несколько составляющих (табл. 1).

***Таблица 1**. Факторы риска информационной безопасности и их составляющие*

Факторы риска	Составляющие факторов
Угрозы ($\boldsymbol{X_1}$)	Естественные (природные) угрозы ($\boldsymbol{X_{11}}$)
	Антропогенные (человеческие) угрозы ($\boldsymbol{X_{12}}$)
Ущерб ($\boldsymbol{X_2}$)	Ущерб конфиденциальности ($\boldsymbol{X_{21}}$)
	Ущерб целостности ($\boldsymbol{X_{22}}$)
	Ущерб доступности ($\boldsymbol{X_{23}}$)
Уязвимости ($\boldsymbol{X_3}$)	Технические уязвимости ($\boldsymbol{X_{31}}$)
	Уязвимости в управлении ($\boldsymbol{X_{32}}$)
Контрмеры ($\boldsymbol{X_4}$)	Существующие контрмеры ($\boldsymbol{X_{41}}$)
	Необходимые контрмеры ($\boldsymbol{X_{42}}$)

Основные этапы процесса оценки информационных рисков могут быть представлены в виде вложенных алгоритмов (процедур), представленных на рис. 1.

Данный процесс и его этапы аналогичны для любых организаций, независимо от сферы их деятельности, масштабов, уровня организационной зрелости [3]. Однако все перечисленные этапы решают конкретные задачи и имеют специфические особенности, поэтому для оценки информационных рисков необходимо на разных этапах применять различные механизмы их реализации. Далее будут рассмотрены цели и задачи каждого из этапов и методы, которые следует использовать при их осуществлении.

2. Этапы оценки информационных рисков, методы и средства их реализации

На этапе анализа потоков данных в информационной системе строится модель информационной системы, определяется назначение её элементов и подсистем и взаимосвязи между ними, а также маршруты циркулирующих потоков информации. Цель данного этапа – выявить недостатки, «узкие места» в информационной системе, имеющие значение для информационной безопасности. Следовательно, модель системы должна быть наглядной и удобной для анализа. Такими свойствами обладают функциональные модели, строящиеся с помощью методов структурного анализа в графической форме с содержательным описанием, позво-

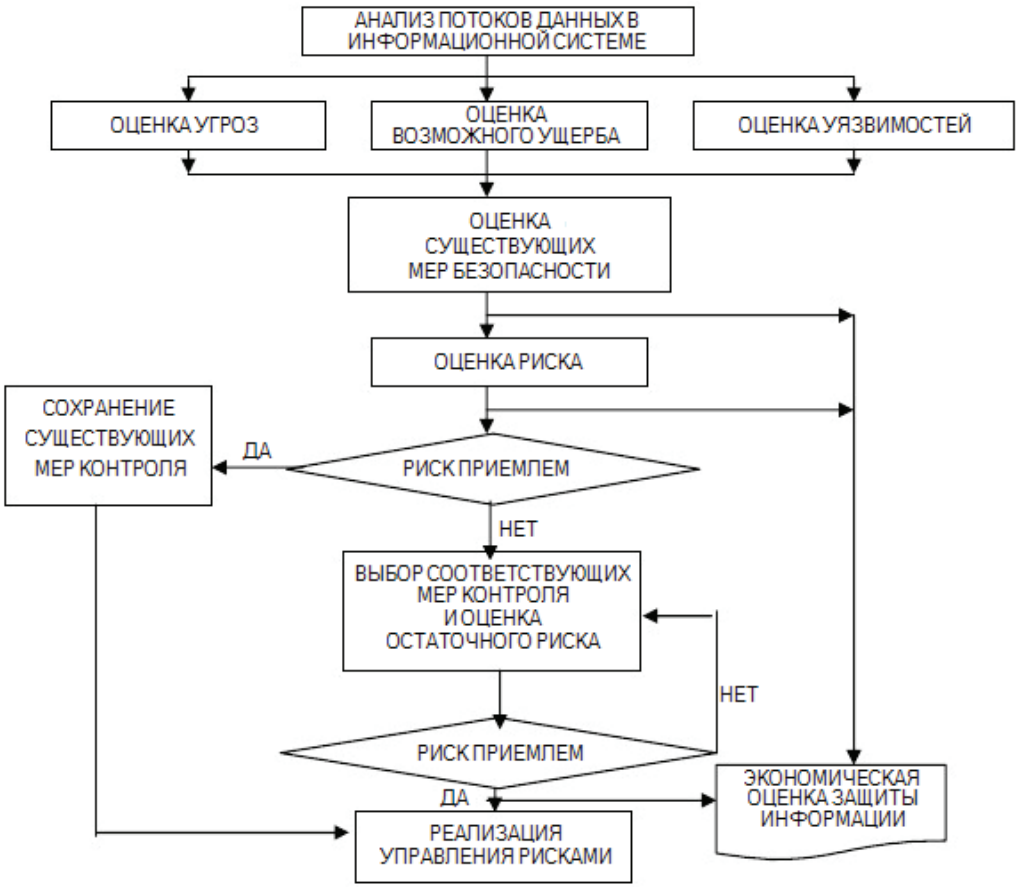

Рис. 1. *Процесс оценки рисков информационной безопасности*

ляющим анализировать диаграммы. Например, в работе [4] рассматривается реализация данного этапа с помощью методологии DFD. В работах [5, 6] приведён пример анализа информационных потоков в виртуальных инфраструктурах здравоохранения на основе методологии IDEF0.

На следующем этапе решается задача оценки 3 факторов риска – X_1, X_2 и X_3. Методы, решающие задачу оценки, можно разделить на количественные и качественные, которые отличаются в выборе шкалы измерения – числовой и лингвистической соответственно. У каждой из этих групп методов существуют свои преимущества и недостатки (табл. 2).

Таблица 2. *Преимущества и недостатки количественных и качественных методов*

Методы оценки	Количественные методы	Качественные методы
Преимущества	1. Позволяют численно оценить требуемые параметры. 2. Реализуют анализ затрат и прибыли при выборе защиты. 3. Предоставляют более точное отображение искомых значений.	1. Позволяют определить области критичных уровней в короткое время и без значительных затрат. 2. Позволяют оценивать относительно легко и дёшево.
Недостатки	1. Количественные меры зависят от объёма и точности используемой шкалы измерения. 2. Результаты оценки могут быть неточными и вводить в заблуждение. 3. Должны быть дополнены качественным описанием. 4. Оценка, проводящаяся с применением этих методов, как правило, дороже, требует большего опыта и современного инструментария.	1. Не позволяют определить вероятности и результаты с использованием числовых коэффициентов. 2. Анализ затрат и выгод при выборе защиты более сложен. 3. Полученные результаты носят общий, приближённый характер.

Свести перечисленные недостатки к минимуму позволяет комбинация количественных и качественных методов – использование шкалы числовых коэффициентов совместно с лингвистическим описанием её отдельных интервалов (уровней). Поэтому именно такие смешанные методы и следует использовать как на данном, так и на следующем этапе – при оценке существующих мер безопасности.

Особенностью этих этапов является то, что оценить факторы риска (по сути, входные данные для оценки самого риска) можно только экспертно. Особенно это касается оценка возможного ущерба, включающего в себя такой сложный, неоднозначный и субъективный процесс, как определение стоимости информационных активов и ресурсов. При оценке остальных факторов в качестве вспомогательной информации эксперты могут использовать результаты анализа потоков данных в информационной системе, полученные на первом этапе, и накопленные статистические данные (если таковые имеются) об угрозах, уязвимостях и эффективности существующих мер безопасности.

Ещё одной важной проблемой является выбор механизмов проведения экспертного опроса. Шкала оценки выбирается экспертами произвольно, и в различных исследованиях существуют абсолютно разные выводы об эффективности использования тех или иных шкал. Также существует необходимость обеспечения адекватности и согласованности экспертных мнений. В работе [7] проведён сравнительный анализ экспертных методов, который показал, что наибольшую адекватность и согласованность обеспечивают метод Дельфи и использование коэффициента конкордации:

$$W = \frac{12S}{n^2(m^3 - m)},$$

где W – коэффициент конкордации, S – сумма квадратов отклонений сумм оценок (ответов, данных всеми экспертами на каждый вопрос) от среднего арифметического сумм оценок, n – число экспертов (число ответов на один вопрос), m – число вопросов.

При этом сделан вывод, что метод конкордации обладает меньшей громоздкостью при той же эффективности, что и метод Дельфи. Коэффициент конкордации W лежит в интервале [0, 1]. Чем ближе значение коэффициента к единице, тем больше уровень согласованности экспертных мнений. Обычно минимально допустимое значение коэффициента конкордации составляет 0,4. Поэтому при достаточно согласованном результате $W \geq 0{,}4$.

Также для обеспечения адекватности экспертных мнений можно использовать решение задачи линейного программирования симплекс-методом, где вероятности реализации угрозы информационной безопасности (x_1), нанесения наивысшего возможного ущерба (x_2) и использования уязвимости информационной системы (x_3) должны быть в интервале [0, 1]:

$$\begin{cases} 0 \leq x_1 \leq 1, \\ 0 \leq x_2 \leq 1, \\ 0 \leq x_3 \leq 1. \end{cases}$$

Итоговая система уравнений выглядит следующим образом:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 \leq b_1, \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 \leq b_2, \\ \qquad\qquad \dots \\ a_{n1}x_1 + a_{n2}x_2 + a_{n3}x_3 \leq b_n, \end{cases}$$

$$a_{ij} \in [0, 10];\ b_i \in [0, 30];\ i \in 1, 2, \dots, n; j \in 1, 2, 3,$$

где a_{i1} – экспертные оценки мощности угрозы; a_{i2} – экспертные оценки величины ущерба; a_{i3} – экспертные оценки степени уязвимости; b_i – оценки риска; n – число экспертов.

Следующий этап – оценка риска. Для него статистические данные и экспертные оценки недостаточны. Здесь необходимы сложные математические расчёты, которые смогли бы обрабатывать данные о факторах риска X_1, X_2, X_3 и X_4, получаемые от экспертов на предыдущих этапах. Такими возможностями обладают методы, использующие элементы искусственного интеллекта (табл. 3) [8].

При этом наибольшей эффективностью в оценке информационных рисков обладают гибридные модели, совмещающие несколько методов искусственного интеллекта, так как они учитывают как числовые значения факторов риска, так и качественные данные, получаемые от экспертов. Например, в работе [9] представлен модуль нечёткого вывода на основе нейронных сетей для динамического итеративного анализа информационных рисков, а в работе [10] – нейронечёткая сеть, оценивающая уровень информационных рисков по 3 переменным в среде программного комплекса MATLAB.

Этап оценки риска повторяется до тех пор, пока уровень остаточного риска, сниженного в результате внедрения контрмер, не будет приемлемым.

Отдельным этапом идёт экономическая оценка защиты информации, целью которой является расчёт соотношений риска информационной безопасности, затрат на контрмеры и выгод, получаемых от их внедрения. Особенностью этой оценки является то, что она должна быть выражена строго

Таблица 3. *Интеллектуальные подходы к оценке рисков информационной безопасности*

Категория	Некоторые подходы
Нейронные сети	1. Многослойный перцептрон 2. Метод обратного распространения ошибки 3. Нейронная сеть радиально-базисных функций 4. Вероятностная нейронная сеть 5. Самоорганизованная конкуренция
Обучающий вектор	1. Метод опорных векторов
Мягкие вычисления	1. Приближённые множества 2. «Серые отношения» 3. Генетический алгоритм 4. Нечёткие множества
Гибридные модели	1. Байесовская нечёткая сеть 2. Нейронечёткая сеть 3. Нечётко-приближённые множества 4. Нечёткий метод анализа иерархий 5. Нечёткий метод анализа сетей 6. «Серая иерархическая модель» 7. Нейронная сеть с генетическим алгоритмом

в количественной форме, причём в финансовом эквиваленте. Для этого также существует несколько методов (табл. 4) [11].

В зависимости от уровня риска и оценки экономических затрат на его снижение реализуется завершающий этап – управление рисками. Существует 4 типовых метода его реализации:

1) минимизация риска (выполнение действий для уменьшения вероятности и/или негативных последствий, связанных с риском);

2) принятие риска (готовность организации понести ущерб от конкретного риска в случае, если его уровень считается приемлемым);

3) уклонение от риска (отказ от вовлечения в рискованную ситуацию или действие, предупреждающее её возникновение);

4) передача риска (перенесение ответственности за риск на третьи лица).

Таблица 4. *Методы экономической оценки защиты информации*

Метод	Обозначение	Способ вычисления значения
Ожидаемые годовые потери	ALE	$$ALE = \sum_{i=1}^{n} I(O_i)F_i,$$ где $\{O_1, O_2, \ldots O_n\}$ – множество негативных последствий события, $I(O_i)$ – значение, выражающее потери в результате события, F_i – частота события i.
Сокращение расходов в ALE	S	*S=ALE* (базовые) – *ALE* (с новой защитой)
Прибыль	B	*B=S* + Прибыль от нововведений
Окупаемость инвестиций	ROI	$$ROI = \frac{B}{C},$$ где C – стоимость защиты.
Окупаемость инвестиций безопасности	ROSI	$$\overline{ROSI = \frac{\Delta R - C}{C}},$$ где ΔR – величина снижения риска, C – стоимость защиты.
Внутренняя норма доходности	IRR	$$C_0 = \sum_{t=1}^{n} \frac{CF_t}{(1 + IRR)^t},$$ где C_0 – первоначальная стоимость инвестиций, C_t – стоимость инвестиций за t-й год.

Выводы

Показано, что при оценке рисков информационной безопасности следует использовать не один универсальный метод, а комбинировать методы и средства на разных этапах этого процесса: DFD или IDEF0 – на этапе анализа потоков данных в информационной системе, экспертный опрос с методами Дельфи, конкордации или симплекс-методом – на этапе оценки факторов риска, методы искусственного интеллекта, особенно гибридные модели – на этапе оценки риска, соответствующие математические методы – на этапе экономической оценки защиты информации и минимизация, принятие, передача или уклонение от риска – на этапе реализации управления рисками.

Литература:

1. M. Ryba. Multidimensional methodology of analysis and management of IT systems risk – MIR-2M (In Polish), Doctoral thesis AGH, Cracow, 2006.
2. ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»
3. Fu S, Xiao Y. (2012), «Strengthening the research for Information security risk assessment». International Conference on Biological and Biomedical Science Advanced in Biomedical Engineering, Vol. 9; pp. 386-392.
4. Информационные риски: количественная оценка / В. Зинкевич, Д. Штатов // Бухгалтерия и банки. 2007. №2. С. 50-53.
5. Булдакова Т. И., Миков Д. А. Анализ информационных процессов виртуального центра охраны здоровья / Научно-техническая информация. Серия 2: Информационные процессы и системы. 2014. № 2. С. 10-20.
6. Анализ информационных рисков виртуальных инфраструктур здравоохранения / Т. И. Булдакова, С. И. Суятинов, Д. А. Миков // Информационное общество. 2013. №4. С. 6.
7. Миков Д. А. Управление информационными рисками с использованием экспертного опроса. Германия, Саарбрюккен: LAP LAMBERT Academic Publishing, 2013. 83 с.
8. Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method / Ming-Chang Lee // International Journal of Computer Science & Information Technology (IJCSIT). 2014. Vol 6. No1. Pp. 29-45.
9. Атаманов А. Н. Модуль нечеткого вывода на основе нейронных сетей для динамического итеративного анализа рисков информационной безопасности // Безопасность информационных технологий. 2011. № 1. С. 7.
10. Булдакова Т. И., Миков Д. А. Оценка информационных рисков в автоматизированных системах с помощью нейро-нечеткой модели // Наука и образование: электронное научно-техническое издание. 2013. № 11. С. 295-310.
11. Rot A. IT Risk Assessment: Quantitative and Qualitative Approach // Proceedings of the World Congress on Engineering and Computer Science. 2008. Pp. 1073-1078.

References:

1. M. Ryba. Multidimensional methodology of analysis and management of IT systems risk – MIR-2M (In Polish), Doctoral thesis AGH, Cracow, 2006.
2. GOST R ISO/MEC 27005-2010 «Informatsionnaya tekhnologiya. Metody i sredstva obespetcheniya bezopasnosti. Menedzhment riska informatsionnoy bezopasnosti»
3. Fu S, Xiao Y., «Strengthening the research for Information security risk assessment». International Conference on Biological and Biomedical Science Advanced in Biomedical Engineering, 2012. Vol. 9; pp. 386-392.
4. Informatsionnye riski: kolitchestvennaya otsenka / B. Zinkevitch, Д. Shtatov // Bukhgalteriya i banki. 2007. №2. S. 50-53.
5. Buldakova T. I., Mikov D. A. Analiz informatsionnykh protsessov virtual'nogo tsentra okhrany zdorov'ya / Nautchno-tekhnitcheskaya informatsiya. Seriya 2: Informatsionnye protsessy i sistemy. 2014. № 2. S. 10-20.
6. Analiz informatsionnykh riskov virtual'nykh infrastruktur zdravookhraneniya / T. I. Buldakova, S. I. Suyatinov, D. A. Mikov // Informatsionnoe obshchestvo. 2013. №4. S. 6.
7. Mikov D. A. Upravlenie Informatsionnymi riskami s ispol'zovaniem ekspertnogo oprosa. Germaniya, Saarbryukken: LAP LAMBERT Academic Publishing, 2013. 83 s.
8. Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method / Ming-Chang Lee // International Journal of Computer Science & Information Technology (IJCSIT). 2014. Vol 6. No1. Pp. 29-45.
9. Atamanov A. N. Modul' netchyotkogo vyvoda na osnove neyronnykh setey dlya dinamitcheskogo iterativnogo analiza riskov informatsionnoy bezopasnosti // Bezopasnost' informatsionnykh tekhnologiy. 2011. № 1. S. 7.
10. Buldakova T. I., Mikov D. A. Otsenka informatsionnykh riskov v avtomatizirovannykh sistemakh s pomoshch'yu neyro-netchyotkoy modeli // Nauka i obrazovanie: elektronnoe nautchno-tekhnitcheskoe izdanie. 2013. № 11. S. 295-310.
11. Rot A. IT Risk Assessment: Quantitative and Qualitative Approach // Proceedings of the World Congress on Engineering and Computer Science. 2008. Pp. 1073-1078.