ОБЕСПЕЧЕНИЕ СОГЛАСОВАННОСТИ И АДЕКВАТНОСТИ ОЦЕНКИ ФАКТОРОВ РИСКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ[1]

Булдакова Т. И.[2], Миков Д.А.[3]

Рассмотрен важный этап анализа рисков информационной безопасности – оценка факторов риска. Выделены показатели, влияющие на эффективность реализации этого этапа – согласованность и адекватность оценок, чувствительность риска. На основе выявленных показателей сформулирована задача повышения эффективности оценки факторов риска. Построена структурная модель факторов риска (угрозы информационной безопасности, потенциально возможный ущерб, уязвимости автоматизированной системы, контрмеры), отображающая их составляющие и взаимосвязи между ними. Предложена вербально–числовая шкала для оценки показателей, составляющих факторы риска. Приведён способ расчёта значений факторов риска по оценённым показателям, связывающий структурную модель факторов с предложенной шкалой оценки. Разработан оригинальный метод проведения экспертного опроса, обеспечивающий соответствие требованиям к этапу оценки факторов риска – максимизация согласованности и адекватности оценок. Показан принцип использования коэффициента конкордации для повышения согласованности экспертных мнений, представлен гибридный метод отсеивания оценок на основе шкал Марголина и Харрингтона. Проиллюстрировано сведение оценок факторов риска к задаче линейного программирования, решаемой с помощью симплекс–метода, что позволяет учитывать влияние на итоговые оценки как наиболее критичных, так и менее значимых факторов, тем самым повышая показатель адекватности оценки.

***Ключевые слова**: оценка факторов риска, угроза информационной безопасности, потенциально возможный ущерб, уязвимость автоматизированной системы, контрмера, согласованность и адекватность экспертных мнений, коэффициент конкордации, шкала Марголина, шкала Харрингтона*

DOI: 10.21681/2311-3456-2017-3-8-15

Введение

Анализ рисков информационной безопасности – это упорядоченный процесс, состоящий из оценки факторов риска и уровня самого риска, оценки соотношения стоимости контрмер и возможного ущерба, реализации управления риском.

На этапе оценки факторов риска составляется перечень всех факторов и производится их оценка. На следующем этапе определяется уровень риска для конкретной организации. Особенностью этапа оценки соотношения контрмер и возможного ущерба является то, что он присутствует в процессе анализа только в том случае, если уровень риска информационной безопасности выше приемлемого, то есть необходимо применить дополнительные контрмеры. Реализация управления рисками – это заключительный этап процесса анализа, в результате которого на основании оценки уровня риска, а также соотношения контрмер и возможного ущерба производится выбор необходимого метода управления риском и его реализация.

На каждом из этапов должны применяться наиболее эффективные методы и средства [1, 2]. Рекомендации по их выбору представлены в работе [3], в работах [4, 5] приведены примеры методики анализа рисков информационной безопасности.

Данная статья посвящена решению задачи обеспечения максимальной согласованности и адекватности оценок факторов риска, полученных по результатам экспертных опросов.

1. Постановка задачи

Введем следующие обозначения. Пусть $x = \{X_1, X_2, X_3, X_4\}$ – множество факторов риска.

Среди факторов риска здесь выделены:

$X_1 = \{X_{11}, X_{12}, X_{13}\}$ – множество угроз (X_{11} – естественные угрозы, X_{12} – антропогенные угрозы, X_{13} – техногенные угрозы);

$X_2 = \{X_{21}, X_{22}, X_{23}\}$ – множество видов ущерба (X_{21} – ущерб данным (нарушение конфиденциальности, целостности и/или доступности), X_{22} – ущерб финансам, X_{23} – ущерб репутации);

1 Выполнено при финансовой поддержке РФФИ, проект №16-07-00878.

2 Булдакова Татьяна Ивановна, д.т.н., профессор, МГТУ им. Н.Э. Баумана, Москва, Россия. E-mail: buldakova@bmstu.ru

3 Миков Дмитрий Александрович, ассистент кафедры ИУ8 МГТУ им. Н.Э. Баумана, Москва, Россия. E-mail: MikovDA@yandex.ru

$X_3 = \{X_{31}, X_{32}, X_{33}\}$ – множество уязвимостей (X_{31} – инженерно-технические уязвимости, X_{32} – организационно-правовые уязвимости, X_{33} – программно-аппаратные уязвимости);

$X_4 = \{X_{41}, X_{42}, X_{43}\}$ – множество контрмер (X_{41} – существующие контрмеры, X_{42} – необходимые контрмеры (максимизация результатов при минимизации прибыли в соответствии с критерием Вальда), X_{43} – достаточные контрмеры (минимизация результатов при максимизации прибыли в соответствии с критерием Сэвиджа)).

Обозначим согласованность оценок факторов риска как $A = [0;1]$ и адекватность оценок факторов риска как $B = [0;1]$.

Далее введем понятие «чувствительность риска», связанное с неравномерным влиянием различных составляющих факторов риска на уровень риска в тех или иных условиях.

Обозначим чувствительность риска как

$$F = \begin{bmatrix} f_{11} & f_{12} & f_{13} \\ f_{21} & f_{22} & f_{23} \\ f_{31} & f_{32} & f_{33} \\ f_{41} & f_{42} & f_{43} \end{bmatrix},$$

где $f_{ij} = [0;1]$, $i = \{1;\ 2;\ 3;4\}$, $j = \{1;\ 2;\ 3\}$ – показатели чувствительности риска к различным факторам.

Учёт чувствительности необходим для выявления составляющих, подлежащих как можно более точной оценке, и составляющих, при оценке которых точность менее важна, вследствие меньшей зависимости уровня риска от них.

Тогда постановка задачи исследования может быть представлена следующим образом:

$$\sum_{i=1}^{4}\sum_{j=1}^{3} f_{ij} \times A \times B \rightarrow max.$$

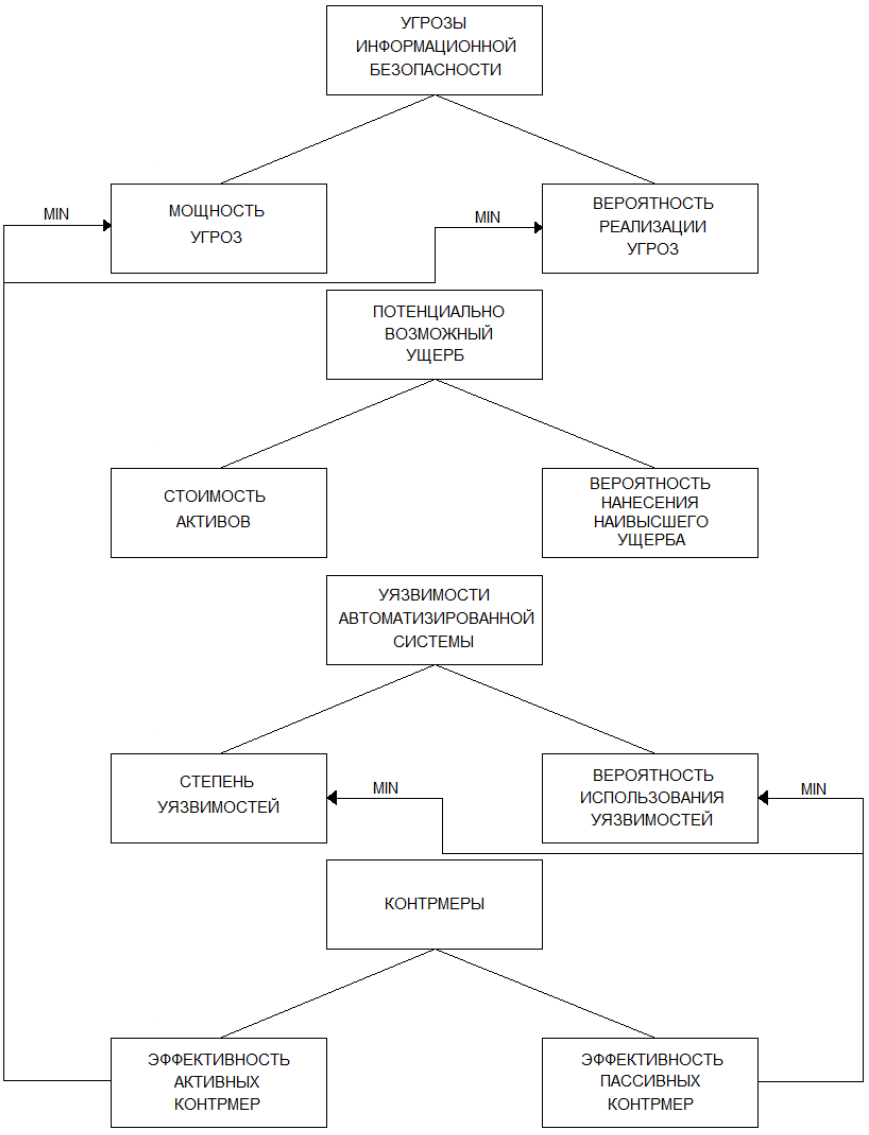

***Рис. 1**. Структура факторов риска*

Таким образом, целью данной работы является разработка метода, обеспечивающего согласованность и адекватность оценок факторов риска и учитывающего чувствительность риска к различным факторам.

2. Обеспечение согласованности оценок факторов риска

После составления перечня факторов риска следует процесс оценки факторов риска. При этом оценка каждого фактора из перечня неразрывно связана с оценкой 2 показателей (рис. 1):

1) угроза информационной безопасности зависит от показателей мощности угрозы (силы воздействия на автоматизированную систему и её активы в случае реализации) и вероятности её реализации;

2) потенциально возможный ущерб состоит из показателей стоимости актива, которому он может быть нанесён, и вероятности нанесения наивысшего ущерба из всего диапазона;

3) уязвимость автоматизированной системы включает в себя показатели степени уязвимости (опасности для автоматизированной системы и её активов в случае использования) и вероятности её использования;

4) контрмеры являются особым фактором, так как уровень риска информационной безопасности обратно пропорционально зависит от показателя их эффективности, в отличие от остальных факторов, где наблюдается прямая пропорциональная зависимость. Контрмеры направлены на снижение мощности и вероятности реализации угроз (активные контрмеры) и степени уязвимостей и вероятности их использования (пассивные контрмеры).

Следовательно, угрозы и уязвимости вместе с их показателями сначала должны быть оценены «в чистом виде», а затем полученные оценки следует скорректировать путём вычитания показателей эффективности активных и пассивных контрмер из соответствующих первоначальных оценок.

Таким образом, группа экспертов, осуществляющих оценку факторов риска, должна оценить все вышеперечисленные показатели, а также чувствительность риска к точности оценки каждого фактора.

Вероятности можно оценить по статистическим данным, а для оценки мощности угроз, величины ущерба (стоимости активов), степени уязвимостей и эффективности контрмер необходимо использовать шкалу (табл. 1).

Таблица 1.
Шкала оценки показателей, составляющих факторы риска

Уровни шкалы	Мощность угрозы	Величина ущерба (стоимость актива)	Степень уязвимости	Эффективность контрмеры
Очень низкий [0; 2]	Угроза, которой можно пренебречь	Незначительные потери материальных средств и ресурсов, которые быстро восполняются, или незначительное влияние на репутацию	Уязвимость, которой можно пренебречь	Контрмера способна устранить очень низкую угрозу/уязвимость или очень незначительно снизить угрозу/уязвимость более высокого уровня
Низкий (2; 4]	Незначительная угроза, которую легко устранить	Более заметные потери материальных активов, более существенное влияние на репутацию или ущемление интересов	Незначительная уязвимость, которую легко устранить	Контрмера способна устранить низкую угрозу/уязвимость или незначительно снизить угрозу/уязвимость более высокого уровня
Средний (4; 6]	Умеренная угроза	Достаточные потери материальных активов или ресурсов, или достаточный урон репутации и интересам	Умеренная уязвимость	Контрмера способна устранить среднюю угрозу/уязвимость или умеренно снизить угрозу/уязвимость более высокого уровня
Высокий (6; 8]	Серьёзная угроза, ликвидация которой возможна, но связана со значительными затратами	Значительный урон репутации и интересам, что может представлять угрозу для продолжения деятельности	Серьёзная уязвимость, ликвидация которой возможна, но связана со значительными затратами	Контрмера способна устранить высокую угрозу/уязвимость или значительно снизить очень высокую угрозу/уязвимость
Очень высокий (8; 10]	Критическая угроза, которая ставит под сомнение возможность её устранения	Разрушительные последствия и невозможность ведения деятельности	Критическая уязвимость, которая ставит под сомнение возможность её устранения	Контрмера способна устранить любую угрозу/уязвимость

Оценка факторов риска выполняется следующим образом:

$$x_{ij1} = x^*_{ij1} \times p_{ij1} \times f_{ij1} - x_{ij4a}, \quad (1)$$

$$x_{ij2} = x^*_{ij2} \times p_{ij2} \times f_{ij2}, \quad (2)$$

$$x_{ij3} = x^*_{ij3} \times p_{ij3} \times f_{ij3} - x_{ij4p}, \quad (3)$$

$$x_{ij4a} = x^*_{ij4a} \times f_{ij4a}, \quad (4)$$

$$x_{ij4p} = x^*_{ij4p} \times f_{ij4p}, \quad (5)$$

где x_{ij1} – оценка угрозы; $x^*_{ij1} \in [0;10]$ – мощность угрозы; $p_{ij1} \in [0;1]$ – вероятность реализации угрозы; $f_{ij1} \in [0;1]$ – чувствительность риска к оценке угрозы; x_{ij2} – оценка потенциально возможного ущерба; $x^*_{ij2} \in [0;10]$ – стоимость актива; $p_{ij2} \in [0;1]$ – вероятность нанесения активу наивысшего ущерба; $f_{ij2} \in [0;1]$ – чувствительность риска к оценке возможного ущерба; x_{ij3} – оценка уязвимости; $x^*_{ij3} \in [0;10]$ – степень уязвимости; $p_{ij3} \in [0;1]$ – вероятность использования уязвимости; $f_{ij3} \in [0;1]$ – чувствительность риска к оценке уязвимости; x_{ij4a} – оценка активной контрмеры; $x^*_{ij4a} \in [0;10]$ – эффективность активной контрмеры; $f_{ij4a} \in [0;1]$ – чувствительность риска к эффективности активной контрмеры; x_{ij4p} – оценка пассивной контрмеры; $x^*_{ij4p} \in [0;10]$ – эффективность пассивной контрмеры; $f_{ij4p} \in [0;1]$ – чувствительность риска к эффективности пассивной контрмеры; $i = \{1;2;\ldots;m\}$ – эксперты, выполняющие оценку; $j = \{1;2;\ldots;n\}$ – факторы из перечня.

В итоге перечень факторов риска принимает вид таблицы, содержащей список факторов и оценки их составляющих (табл. 2). При этом необходимые и достаточные контрмеры на данном этапе не подлежат оценке.

Таблица 2.
Таблица оценки факторов риска

ФАКТОРЫ	**ОЦЕНКИ ЭКСПЕРТОВ**			
Угрозы информационной безопасности	**Мощность угрозы (x^*_{ij1})**	**Вероятность реализации (p_{ij1})**	**Чувствительность риска (f_{ij1})**	***Оценка угрозы (x_{ij1})***
Естественные (природные) угрозы				
Антропогенные (человеческие) угрозы				
Техногенные угрозы				
Потенциально возможный ущерб	**Стоимость актива (x^*_{ij2})**	**Вероятность нанесения (p_{ij2})**	**Чувствительность риска (f_{ij2})**	***Оценка ущерба (x_{ij2})***
Информационные активы				
Материальные и финансовые активы				
Факторы, влияющие на репутацию				
Уязвимости автоматизированной системы	**Степень уязвимости (x^*_{ij3})**	**Вероятность использования (p_{ij3})**	**Чувствительность риска (f_{ij3})**	***Оценка уязвимости (x_{ij3})***
Инженерно-технические уязвимости				
Организационно-правовые уязвимости				
Программно-аппаратные уязвимости				
Контрмеры	**Эффект контрмеры (x^*_{ij4a}, x^*_{ij4p})**	**Активная или пассивная**	**Чувствительность риска (f_{ij4a}, f_{ij4p})**	***Оценка контрмеры (x_{ij4a}, x_{ij4p})***
Существующие контрмеры				

Экземпляр данной таблицы следует выдать для заполнения каждому эксперту. Для обеспечения согласованности мнений экспертов рабочей группы (показатель A) необходимо использовать коэффициент конкордации W [6-8], который обычно рассчитывают по формуле, предложенной Кендаллом. При этом W определяют как отношение фактически полученной величины S к её максимальному значению S_{max} для одной и той же группы экспертов и числа сравниваемых вариантов по формулам ($k = \{1; 2; 3\}$):

$$x_{jk} = \sum_{i=1}^{m} x_{ijk}, \quad (6)$$

$$x_k = \frac{1}{n}\sum_{i=1}^{m}\sum_{j=1}^{n} x_{ijk}, \quad (7)$$

$$S = \sum_{j=1}^{n}\sum_{k=1}^{3}\left(x_{jk} - x_k\right)^2, \quad (8)$$

$$W = \frac{12S}{m^2\left(n^3 - n\right)}. \quad (9)$$

Для оценки согласованности мнений экспертов следует использовать гибридный метод, основанный на вербально-числовых шкалах Марголина (табл. 3) [9] и Харрингтона (табл. 4) [8].

Если $W \leq 0{,}5$, то необходимо циклически отсеивать у каждого фактора крайнюю оценку, наиболее отличающуюся от среднего арифметического всех оценок данного фактора, чтобы $W > 0{,}5$. При этом число отсеянных оценок не должно превосходить половину от их общего числа m (количество циклов должно быть не больше $m/2$). Если после $m/2$ циклов $W > 0{,}37$, то процесс отсеивания завершается. Если же после $m/2$ циклов $W \leq 0{,}37$, то необходимо переформировать экспертную группу и заново провести оценку факторов риска. В результате обеспечивается необходимый уровень согласованности экспертных оценок.

Таблица 3.
Оценка согласованности мнений экспертов по Марголину

Значение коэффициента конкордации	Согласованность мнений экспертов
$W \in [0;\ 0{,}1]$	Согласованность отсутствует
$W \in (0{,}1;\ 0{,}3]$	Согласованность очень слабая
$W \in (0{,}3;\ 0{,}5]$	Согласованность слабая
$W \in (0{,}5;\ 0{,}7]$	Согласованность умеренная
$W \in (0{,}7;\ 0{,}9]$	Согласованность высокая
$W \in (0{,}9;\ 1]$	Согласованность очень высокая

Таблица 4.
Оценка согласованности мнений экспертов по Харрингтону

Значение коэффициента конкордации	Согласованность мнений экспертов
$W \in [0;\ 0{,}2]$	Согласованность очень низкая
$W \in (0{,}2;\ 0{,}37]$	Согласованность низкая
$W \in (0{,}37;\ 0{,}64]$	Согласованность средняя
$W \in (0{,}64;\ 0{,}8]$	Согласованность высокая
$W \in (0{,}8;\ 1]$	Согласованность очень высокая

3. Обеспечение адекватности оценок факторов риска

Вычисление итоговых значений уровней угрозы (x_1), потенциально возможного ущерба (x_2) и уязвимости в автоматизированной системе (x_3) на основе обработки оставшихся после отсеивания экспертных оценок и обеспечение их адекватности (показатель *B*) связано с 2 проблемами:

1) неэффективность вычисления итоговых оценок факторов риска через среднее арифметическое оставшихся после отсеивания экспертных оценок, так как критичные факторы оказывают значительно большее влияние на уровень риска, чем маловажные;

2) неэффективность вычисления итоговых оценок факторов риска через присвоение им значений максимальных экспертных оценок среди оставшихся, так как в таком случае эффект маловажных факторов не учитывается вообще, несмотря на то, что они снижают уровень риска.

Таким образом, необходимо максимизировать функцию $F(x) = x_1 + x_2 + x_3 \rightarrow max$, при этом учитывая ограничения в виде влияния всех факторов на уровень риска. Эти требования могут быть успешно выполнены путём построения системы уравнений, содержащей количество оставшихся после отсеивания оценок угроз, потенциально возможного ущерба и уязвимостей у каждого эксперта, а также сумму оценок каждого эксперта. Система уравнений сводится к оптимизационной задаче линейного программирования и решается с использованием симплекс-метода.

Для построения данной системы необходимо составить сводную таблицу оставшихся после отсеивания экспертных оценок и подсчитать общую сумму оценок у каждого эксперта (табл. 5).

Таблица 5.
Сводная таблица экспертных оценок

ФАКТОРЫ	**ОЦЕНКИ ЭКСПЕРТОВ**			
Угрозы информационной безопасности	**1**	**2**	**…**	**m**
Естественные (природные) угрозы				
Антропогенные (человеческие) угрозы				
Техногенные угрозы				
Потенциально возможный ущерб	**1**	**2**	**…**	**m**
Информационные активы				
Материальные и финансовые активы				
Факторы, влияющие на репутацию				
Уязвимости автоматизированной системы	**1**	**2**	**…**	**m**
Инженерно-технические уязвимости				
Организационно-правовые уязвимости				
Программно-аппаратные уязвимости				
Сумма всех экспертных оценок	b_1	b_2	…	b_m

На основе сводной таблицы необходимо построить систему уравнений:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 \le b_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 \le b_2 \\ a_{m1}x_1 + a_{m2}x_2 + a_{m3}x_3 \le b_m, \end{cases} \quad (10)$$

где $x_1 \in [0;10]$ – итоговая оценка уровня угрозы; $x_2 \in [0;10]$ – итоговая оценка уровня ущерба; $x_3 \in [0;10]$ – итоговая оценка уровня уязвимости; $a_{i1} \in \{0;1;\dots;m\}$ – число оставшихся оценок угроз у ***i***-го эксперта; $a_{i2} \in \{0;1;\dots;m\}$ – число оставшихся оценок ущерба у *i*-го эксперта; $a_{i3} \in \{0;1;\dots;m\}$ – число оставшихся оценок уязвимостей у *i*-го эксперта; b_i – сумма всех оценок *i*-го эксперта.

Решение оптимизационной задачи линейного программирования симплекс-методом повышает эффективность обработки экспертных оценок [10].

Влияние наиболее критичных факторов риска на итоговые оценки учитывается путём максимизации целевой функции, а усреднённое влияние остальных факторов – с помощью установления соответствующих ограничений b_i.

В результате обеспечивается адекватность итоговых оценок, значения которых также могут быть дополнены качественными оценками по вербально-числовой шкале из табл. 1 для облегчения восприятия при последующей оценке уровня риска.

Выводы

Разработанный метод проведения экспертного опроса на основе вербально-числовой шкалы и обработки полученных оценок факторов риска с помощью коэффициента конкордации и симплекс-метода обеспечивает требуемые показатели эффективности (согласованность и адекватность оценок), а также позволяет учитывать чувствительность риска к различным факторам. Достигнутое повышение эффективности оценки факторов риска позволяет увеличить точность последующей оценки уровня риска информационной безопасности.

***Рецензент**: Федичев Андрей Валерьевич, кандидат технических наук, доцент, действительный государственный советник 3 класса, директор ФБУ «Научный центр правовой информации при Министерстве юстиции Российской Федерации». E-mail: andrey.fedichev@scli.ru*

Литература

1. Миков Д.А. Анализ методов и средств, используемых на различных этапах оценки рисков информационной безопасности // Вопросы кибербезопасности. 2014. №4 (7). С. 49-54.
2. Baskerville R. An analysis survey of information system security design methods: Implications for Information Systems Development. ACM Computing Survey. 1993. Pp. 375-414.
3. Миков Д.А. Анализ методов изучения потоков данных для оценки рисков информационной безопасности // Ежемесячный научный журнал «Prospero». 2014. №7. С. 28-33.
4. Булдакова Т.И., Миков Д.А. Методика анализа информационных рисков с применением нейро-нечёткой сети // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2015. №4. С. 13-17.
5. Булдакова Т.И., Миков Д.А. Реализация методики оценки рисков информационной безопасности в среде MATLAB // Вопросы кибербезопасности. 2015. №4 (12). С. 53-61.
6. Булдакова Т.И., Миков Д.А. Метод повышения адекватности оценок информационных рисков // Инженерный журнал: наука и инновации. 2012. №3 (3). С. 36.
7. Миков Д.А. Управление информационными рисками с использованием экспертного опроса. Германия, Саарбрюккен: LAP LAMBERT Academic Publishing, 2013. 83 с.
8. Постников В.М., Спиридонов С.Б. Подход к расчёту весовых коэффициентов ранговых оценок экспертов при выборе варианта развития информационной системы // Наука и образование: электронное научно-техническое издание. 2013. №8. С. 395-412.
9. Марголин Е. Методика обработки данных экспертного опроса // Полиграфия. 2006. №5. С. 14-16.
10. Чернобай М.Л. Методы и модели комбинирования экспертных оценок характеристик надёжности. [Автореферат]. СПб. СПбГЛТУ, 2004.

ENSURING THE CONCORDANCE AND THE ADEQUACY OF INFORMATION SECURITY RISK FACTORS ASSESSMENT

T. Buldakova[4], D. Mikov[5]

Risk factors assessment as important stage of information security risk analysis has been presented. Such indicators as assessment consistency and adequacy, risk sensitivity, which influence the risk factors assessment efficiency, have been identified. A problem of increase in risk factors assessment efficiency based on identified indicators has been formulated. A structural model of risk factors (information security threats, potentially possible damage, automated system vulnerabilities, countermeasures), which displays their components and relationships between them, has been designed. A verbal–numeric scale for assessment of indicators, which risk factors consist of, has been proposed. A method for calculating the risk factors values using assessed indicators, which connects the structure model with proposed assessment scale, has been suggested. An original expert survey method, which provides compliance with the requirements of concordance and adequacy maximization for risk factors assessment stage, has been developed. Concordance coefficient using to improve expert opinions consistency has been showed, a hybrid values screening method based on Margolin and Harrington scales has been presented. Risk factors assessment reduction to a linear programming problem solved by simplex method, which takes into account both the most critical and less important factors, and increased the assessment adequacy has been illustrated.

Keywords: *risk factors assessment, information security threat, potentially possible damage, automated system vulnerability, countermeasure, expert opinions concordance and adequacy, concordance coefficient, Margolin scale, Harrington scale*

References

1. Mikov D.A. Analiz metodov i sredstv, ispol'zuemykh na razlitchnykh etapakh otsenki riskov informatsionnoy bezopasnosti // Voprosy kiberbezopasnosti. 2014. №4 (7). S. 49-54.
2. Baskerville R. An analysis survey of information system security design methods: Implications for Information Systems Development. ACM Computing Survey. 1993. Pp. 375-414.
3. Mikov D.A. Analiz metodov izutcheniya potokov dannykh dlya otsenki riskov informatsionnoy bezopasnosti // Ezhemesyatchnyy nautchnyy zhurnal «Prospero». 2014. №7. S. 28-33.
4. Buldakova T.I., Mikov D.A. Metodika analiza informatsionnykh riskov s primeneniem neyro-netchyotkoy seti // Nautchno-tekhnitcheskaya informatsiya. Seriya 2: Informatsionnye protsessy i sistemy. 2015. №4. S. 13-17.
5. Buldakova T.I., Mikov D.A. Realizatsiya metodiki otsenki riskov informatsionnoy bezopasnosti v srede MATLAB // Voprosy kiberbezopasnosti. 2015. №4 (12). S. 53-61.
6. Buldakova T.I., Mikov D.A. Metod povysheniya adekvatnosti otsenok informatsionnykh riskov // Inzhenernyy zhurnal: nauka i innovatsii. 2012. №3 (3). S. 36.
7. Mikov D.A. Upravlenie Informatsionnymi riskami s ispol'zovaniem ekspertnogo oprosa. Germaniya, Saarbryukken: LAP LAMBERT Academic Publishing, 2013. 83 s.
8. Postnikov V.M., Spiridonov S.B. Podkhod k rastchyotu vesovykh koeffitsientov rangovykh otsenok ekspertov pri vybore varianta razvitiya informatsionnoy sistemy //Nauka i obrazovanie: elektronnoe nautchno-tekhnitcheskoe izdanie. 2013. №8. S. 395-412.
9. Margolin E. Metodika obrabotki dannykh ekspertnogo oprosa // Poligrafiya. 2006. №5. S. 14-16.
10. Tchernobay M.L. Metody i modeli kombinirovaniya ekspertnykh otsenok kharakteristik nadyozhnosti. [Avtoreferat]. SPb.SPbGLTU, 2004.

4 Tatiana Buldskova, Doctor of Technical Sciences, Professor, BMSTU, Moscow, Russia. E-mail: buldakova@bmstu.ru
5 Dmitry Mikov, assistant Professor, BMSTU, Moscow, Russia. E-mail: MikovDA@yandex.ru