КОМПЛЕКСНАЯ ОЦЕНКА ИНФОРМАЦИОННЫХ РИСКОВ. II: АЛГОРИТМ ИДЕНТИФИКАЦИИ СТРУКТУРЫ ДЕРЕВА КОМПЛЕКСНОЙ ОЦЕНКИ ИНТЕГРАЛЬНОГО ИНФОРМАЦИОННОГО РИСКА

Рей А. С.[1], Широкий А. А.[2]
(*ФГБУН Институт проблем управления им. В.А. Трапезникова РАН, Москва*)

При оценке рисков информационной безопасности весьма важным представляется учет характерных для информационных систем видов неопределенности. Существующие методы и алгоритмы оценки информационных рисков могут не учитывать некоторые из них, вследствие чего полученные оценки рисков могут быть искажены. В связи с этим естественным образом возникает задача разработки нового или адаптации уже существующего метода для оценки рисков сложных систем с учётом всех характерных для рассматриваемого класса систем видов неопределенности. В настоящей работе развивается ранее предложенная идея применения для оценки информационных рисков метода комплексного оценивания, предполагающего агрегацию оценок информационной системы по стандартным критериям информационной безопасности – конфиденциальности, целостности и доступности. В первой части работы было показано, что этот метод при соответствующих модификациях позволяет учесть все нужные виды неопределенности. В этой части работы предлагается алгоритм идентификации структуры дерева комплексной оценки на основе принципа сворачивания связанных критериев. Работоспособность алгоритма продемонстрирована на примере построения деревьев оценки рисков конфиденциальности, целостности и доступности для SMART-систем на основе «Интернета вещей».

Ключевые слова: сложные информационные системы, интегральный риск, комплексная оценка, системы Интернета вещей.

1. Введение

В первой части работы (см. [16]) авторами были проанализированы укрупненные группы подходов и методов за период 2019–23 гг., направленные на оценку информационных рисков. Группы и их элементы были классифицированы по основанию учета характерных для сложных информационных систем видов неопределенности, а именно:

[1] *Анастасия Сергеевна Рей, м.н.с.* (*a.rey@ipu.ru*).
[2] *Александр Александрович Широкий, к.ф.-м.н., с.н.с.* (*shiroky@ipu.ru*).

A. неопределённость значений отдельных факторов оценки состояния системы в целом;

B. неопределённость взаимного влияния элементов системы друг на друга;

C. неопределённость зависимости риска системы в целом от значений локальных (точечных) рисков.

В обзоре был проведен анализ качественных и количественных методов, таких как безмодельный подход [27, 31, 38], статистический подход [18, 28], подход нечеткой математики [13, 14], энтропийный подход [20], использование открытых стандартов [8], теоретико-графовый подход [1, 20, 22, 24, 32, 33, 36], «когнитивная игра» [11, 15], социотехнический подход [7, 26], попарное сравнение [35], анализ иерархий [5, 30], сценарный подход [19, 21], ранжирование [34, 37], анализ уровня защиты и блокады [23], методы агрегирования [2, 3, 4, 6].

Анализ показал, что в настоящее время большинство исследований сфокусировано на оценке локальных рисков, небольшое число работ рассматривает неопределенность значений отдельных факторов оценки, а взаимное влияние элементов системы друг на друга и, как следствие, на ее интегральный риск не рассматривается практически совсем. Методов, позволяющих учесть одновременно неопределенности всех трех видов, в литературе обнаружено не было.

Тем не менее среди рассмотренных подходов и методов можно выделить ряд наиболее перспективных (в обсуждаемом смысле). К таковым авторы относят количественный метод «когнитивной игры» [11, 15] и качественный метод комплексного оценивания (МКО) [3, 6]. Последний представляет больший интерес, поскольку область применения качественных методов обычно шире, чем количественных. Поэтому главной задачей второй части настоящей работы является его адаптация для оценки информационных рисков сложных систем. В случае успеха в дальнейшем можно будет перейти к модификациям метода для учета неопределенности вышеперечисленных видов.

Для решения поставленной задачи был разработан алгоритм идентификации структуры дерева комплексной оценки на основе принципа сворачивания связанных критериев, в контексте оценки информационных рисков впервые предложенного в [12].

Работоспособность алгоритма продемонстрирована на примере построения деревьев оценки рисков конфиденциальности, целостности и доступности для SMART-систем на основе «Интернета вещей».

2. Материалы и методы

2.1. ОБЩАЯ ПОСТАНОВКА ЗАДАЧИ

Рассмотрим некоторую информационную систему *S*. Её безопасность оценивается в следующих аспектах: конфиденциальность (*C*), целостность (*I*), доступность (*A*) [25]. Будем считать, что значения соответствующих критериев лежат в следующих множествах:

(1) $CE = \{1, \dots, n_C\};\ IE = \{1, \dots, n_I\};\ AE = \{1, \dots, n_A\},$
$n_C, n_I, n_A \in \mathbb{N}.$

Пусть комплексная оценка информационной безопасности представляется одним из значений множества $SE = \{1, \dots, n_S\}$, $n_S \in \mathbb{N}$. Тогда процедура её получения сводится к определению некоторого отображения

(2) $E: CE \times IE \times AE \to SE,$

где $SE \subset \mathbb{N}$ – множество возможных значений (уровней) интегрального риска.

Решение задачи (1) обсуждалось в работе [11]. При этом предполагалось, что значения $K_C \in CE$, $K_I \in IE$, $K_A \in AE$ уже тем или иным способом получены, т.е. известны. Древовидная структура для интегральной оценки строится из соображения частичной зависимости рисков доступности и целостности, так как утрата целостности необходимо ведет к утрате доступности. Следовательно, локальные критерии K_I и K_A следует свернуть в первую очередь. Утрата же конфиденциальности не влияет ни на целостность, ни на доступность, поэтому соответствующий критерий K_C следует сворачивать с результатом свёртки K_I и K_A (см. рис. 1).

Развивая этот подход, опишем способ идентификации поддеревьев комплексного оценивания, корнями которых являются критерии K_C, K_I и K_A. Вначале определим субкритерии, исходя из следующих соображений.

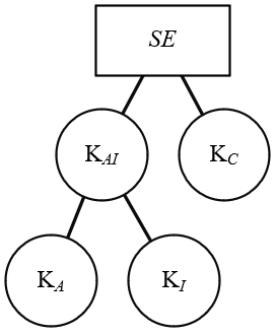


Рис. 1. Структура бинарного дерева комплексного оценивания интегрального информационного риска [11]

Каждая информационная система имеет особенности, которые потенциально снижают её конфиденциальность, целостность или доступность. Объединим особенности, известные лицу, принимающему решения, во множество уязвимостей *U*. Внешние или внутренние воздействия (целенаправленные или нет) на одну или несколько уязвимостей из множества *U* будем называть *атаками*.

Пусть A – множество атак. Будем называть *выполнимостью атаки* функцию

(3) $\mathfrak{f}: A \times 2^U \to \{0,1\}$.

Отметим, что

(4) $\forall a \in A\ \exists!\, u_a \subset 2^U : \mathfrak{f}(a,u) = \begin{cases} 1, & u \in u_a, \\ 0, & u \notin u_a. \end{cases}$

Множество u_a будем называть *множеством выполнимости атаки* a. Зададим функцию

(5) $\mathfrak{s}: 2^U \to \mathbb{R}$,

характеризующую тяжесть атаки. Если в рассматриваемой системе уязвимости не ранжированы тем или иным способом, то её значение для произвольной атаки $a \in A$ равно мощности соответствующего ей множества u_a, т.е.

(6) $\mathfrak{s}(u_a) = |u_a| \in \mathbb{N}$.

Если атаки a_i, a_j такие, что $u_{a_i} \cap u_{a_j} = \emptyset$, то будем их называть *независимыми*, в противном случае – зависимыми. Зададим функцию

(7) $\mathfrak{d}: 2^U \times 2^U \to \mathbb{R}$,

характеризующую степень зависимости атак друг от друга. Если в рассматриваемой системе уязвимости не ранжированы тем или иным способом, то для некоторых двух атак $a_i, a_j \in A$

(8) $\mathfrak{d}\left(u_{a_i}, u_{a_j}\right) = \left|u_{a_i} \cap u_{a_j}\right| \in \mathbb{N} \cup \{0\}$.

Поскольку в конкретной информационной системе ряд уязвимостей может отсутствовать, а также учитывая возможность развития системы во времени и, соответственно, изменения состава уязвимостей, использовать их в качестве критериев-вершин дерева комплексного оценивания неразумно: построенное таким образом дерево будет требовать перестройки при изменении системы, в том числе при выполнении действий, направленных на снижение её риска (удаление уязвимостей). Следовательно, роль вершин должны выполнять критерии, рассчитываемые как значения функции, характеризующей тяжесть атаки для рассматриваемой системы. Структура же дерева определяется взаимной зависимостью типовых атак, по аналогии с [8].

В следующем параграфе представлен алгоритм построения дерева комплексного оценивания, не зависящий от наличия или отсутствия конкретных уязвимостей в защищаемой системе.

2.2. АЛГОРИТМ ИДЕНТИФИКАЦИИ СТРУКТУРЫ ДЕРЕВА КОМПЛЕКСНОЙ ОЦЕНКИ ИНТЕГРАЛЬНОГО ИНФОРМАЦИОННОГО РИСКА

Предлагаемый алгоритм состоит из шести шагов и позволяет построить дерево комплексного оценивания интегрального риска для заданного класса информационных систем. При описании для простоты будем считать, что все типичные уязвимости для рассматриваемого класса систем эквивалентны в смысле их вклада в интегральный риск. Отметим, что алгоритм легко обобщается на случай ранжированных уязвимостей.

1. Определить множество уязвимостей U как перечень типичных уязвимостей для рассматриваемого класса информационных систем, а также множество типичных атак $A = A_C \cup A_I \cup A_A$, где A_C, A_I и A_A порождаются списками типов атак, влияющих на конфиденциальность, целостность и доступность защищаемой системы соответственно.

2. Построить бинарные матрицы E_C, E_I, E_A размерностей $|2^{A_C}| \times |2^U|, |2^{A_I}| \times |2^U|, |2^{A_A}| \times |2^U|$ соответственно, описывающие, с одной стороны, возможность осуществления атаки конкретного типа при наличии той или иной комбинации уязвимостей, а с другой – зависимость типов атак друг от друга через общие комбинации зависимостей. Если атака $a \in A_C$ (или некоторая их комбинация $P \in 2^{A_C}$) может быть проведена с использованием уязвимости $u \in U$ (или комбинации уязвимостей $Q \in 2^U$), то в соответствующей клетке матрицы E_C должна стоять 1, в противном случае – 0. Матрицы E_I и E_A заполняются аналогично.

3. Для матриц E_C, E_I, E_A рассчитать векторы S_C, S_I, S_A размерностей $|2^{A_C}|, |2^{A_I}|, |2^{A_A}|$ соответственно, элементы которых являются суммами строк матриц E_C, E_I, E_A. Элементами этих векторов будут числа, отражающие число комбинаций уязвимостей, с использованием которых может быть реализована конкретная атака (или их комбинация). Отметим, что в случае ранжированных уязвимостей в клетках матриц E_C, E_I, E_A вместо нулей и единиц будут содержаться некоторые числа, характеризующие опасность уязвимости. В этом случае суммы, являющиеся элементами векторов S_C, S_I, S_A, затруднительно содержательно интерпретировать. Однако учитывая, что получаемые с их помощью значения мы в дальнейшем будем использовать лишь для ранжирования, это не является проблемой.

4. Аналогично п. 2 построить матрицы D_C, D_I, D_A с тем отличием, что единица в клетке матрицы D_C (D_I, D_A) ставится в случае, если соответствующая комбинация уязвимостей была отмечена в матрице E_C (E_I, E_A) единицей хотя бы для одной атаки из соответствующей текущей строке комбинации.

5. Аналогично п. 3 рассчитать векторы B_C, B_I, B_A как суммы строк матриц D_C, D_I, D_A соответственно.

6. Рассчитать векторы $Y_C = \frac{S_C}{B_C}, Y_I = \frac{S_I}{B_I}, Y_A = \frac{S_A}{B_A}$. Элементы этих векторов будут рассматриваться как показатели зависимости соответствующих атак.

7. Построить поддеревья комплексного оценивания, корнями которых являются критерии K_C, K_I и K_A, пошагово по следующему принципу: на текущем шаге агрегируются те пары под-

структур, соответствующее значение показателя зависимости которых является максимальным среди всех пар допустимых к агрегации на текущем шаге подструктур. Агрегация подразумевает добавление в дерево новой вершины-критерия с двумя рёбрами, соединяющими её с агрегируемым подструктурами. Например, на первом шаге мы можем агрегировать только листья будущего дерева (вершины, соответствующие типовым атакам, определённым на шаге 1). На втором шаге агрегации могут подвергаться как не агрегированные ранее вершины, соответствующие атакам, так и новые вершины, добавленные на предшествующих шагах и являющиеся корнями некоторых поддеревьев.

8. Установить значения для каждого из листьев, построенных на предыдущем шаге поддеревьев комплексного оценивания. В качестве базового значения можно использовать первые $|A_C|, |A_I|, |A_A|$ элементов векторов S_C, S_I, S_A соответственно, характеризующие опасность атаки для рассматриваемого класса информационных систем. Эти значения необходимо привести к порядковой шкале с n градациями. Стандартный вариант шкалы обычно включает три уровня: высокий, средний или низкий уровень риска [9].

9. Задать монотонные матрицы сверток размерностью $n \times n$ для определения значений агрегированных критериев, соответствующих вершинам дерева КО, не являющимся листьями. Допустимо использовать правила построения матриц с помощью метода порогового агрегирования [4] (см. рис. 2).

$\boldsymbol{K_1}$	**1**	3	2	1
	2	3	2	2
	3	3	3	3
		3	**2**	**1**
	$\boldsymbol{K_2}$			

Рис. 2. Пример монотонной матрицы свёртки

Следует упомянуть о возможных предельных случаях, с которыми можно столкнуться при осуществлении такой оценки:

1. Если атаки в пределах поддерева независимы ($u_{a_i} \cap u_{a_j} = \emptyset \; \forall i \neq j : a_i, a_j \in A_C$ для поддерева конфиденциаль-

ности, для других поддеревьев запись будет аналогичной), то построить дерево комплексной оценки на основе взаимной зависимости критериев не получится и следует использовать другие методы, например, рассчитать значение соответствующего локального критерия как взвешенную сумму значений (для поддерева конфиденциальности $K_C = \sum_{a_C \in A_C} k_{a_C} \cdot \mathfrak{s}(u_{a_C})$, где k_{a_C} – некоторые коэффициенты).

2. Если в пределах поддерева соответствующие атакам множества подмножеств уязвимостей, на которых атака выполнима, непусты и совпадают ($u_{a_i} = u_{a_j} \neq \emptyset \; \forall i \neq j: a_i, a_j \in A_C$ для поддерева конфиденциальности, для других поддеревьев запись будет аналогичной), то для получения значения соответствующего критерия следует воспользоваться методом порогового агрегирования [4].

3. Наконец, возможна ситуация, когда в пределах поддерева окажутся три или более атак с равномощными попарными пересечениями их множеств выполнимости. В этом случае решение задачи порождения поддерева КО не будет единственным и выбор конкретного поддерева следует сделать на следующем этапе, когда при рассмотрении конкретной информационной системы будет возможно провести ранжирование уязвимостей.

3. Результаты и обсуждение

3.1. ИЛЛЮСТРАЦИЯ РЕЗУЛЬТАТОВ

Для иллюстрации описанного выше алгоритма составим синтетический пример. Рассмотрим некоторую сложную систему, характеризующуюся четырьмя видами уязвимостей $u_1, \dots, u_4$ и тремя видами атак $a_1, \dots, a_3$. Пусть

$U = \{u_1, u_2, u_3, u_4\}, A = \{a_1, a_2, a_3\},$

$u_{a_1} = \{u_2, u_3, u_4\}, u_{a_2} = \{u_1, u_4\}, u_{a_3} = \{u_2, u_3\}.$

Тогда матрица соответствия уязвимостей атакам будет иметь следующий вид (таблица 1).

Составим матрицу E для данной системы и рассчитаем значения вектора S. Результат в транспонированном виде (для удобства чтения) представлен в таблице 2.

Таблица 1. Матрица соответствия уязвимостей атакам

	u_1	u_2	u_3	u_4
a_1		1	1	1
a_2	1			1
a_3		1	1	

Таблица 2. Транспонированная матрица E и значения вектора S

	a_1	a_2	a_3	a_1, a_2	a_1, a_3	a_2, a_3	a_1, a_2, a_3
u_1		1		0	0	0	0
u_2	1		1	0	1	0	0
u_3	1		1	0	1	0	0
u_4	1	1		1	0	0	0
u_1, u_2	0	0	0	0	0	0	0
u_1, u_3	0	0	0	0	0	0	0
u_1, u_4	0	1	0	0	0	0	0
u_2, u_3	1	0	1	0	1	0	0
u_2, u_4	1	0	0	0	0	0	0
u_3, u_4	1	0	0	0	0	0	0
u_1, u_2, u_3	0	0	0	0	0	0	0
u_1, u_2, u_4	0	0	0	0	0	0	0
u_1, u_3, u_4	0	0	0	0	0	0	0
u_2, u_3, u_4	1	0	0	0	0	0	0
u_1, u_2, u_3, u_4	0	0	0	0	0	0	0
S	7	3	3	1	3	0	0

Теперь составим матрицу D и рассчитаем векторы B и Y для рассматриваемой системы. Результаты в транспонированном виде приведены в таблице 3.

Исходя из получившихся значений в соответствии с п. 7 алгоритма в первую очередь мы должны свернуть критерии-атаки a_1 и a_3, а затем – результат их свёртки с a_2. Получившееся дерево комплексной оценки приведено на рис. 3.

Далее можно переходить к получению оценки интегрального риска. Предположим, что в ходе аудита безопасности риск реализации атаки a_1 был оценён как высокий (3 балла), а риски реализации атак a_2 и a_3 – как низкие (1 балл).

Таблица 3. Матрица D и значения векторов B и Y

	a_1	a_2	a_3	a_1, a_2	a_1, a_3	a_2, a_3	a_1, a_2, a_3
u_1		1		1	0	1	1
u_2	1		1	1	1	1	1
u_3	1		1	1	1	1	1
u_4	1	1		1	1	1	1
u_1, u_2	0	0	0	0	0	0	0
u_1, u_3	0	0	0	0	0	0	0
u_1, u_4	0	1	0	1	0	1	1
u_2, u_3	1	0	1	1	1	1	1
u_2, u_4	1	0	0	1	1	0	1
u_3, u_4	1	0	0	1	1	0	1
u_1, u_2, u_3	0	0	0	0	0	0	0
u_1, u_2, u_4	0	0	0	0	0	0	0
u_1, u_3, u_4	0	0	0	0	0	0	0
u_2, u_3, u_4	1	0	0	1	1	0	1
u_1, u_2, u_3, u_4	0	0	0	0	0	0	0
B	7	3	3	9	7	6	9
Y	1	1	1	1 / 9	3 / 7	0	0

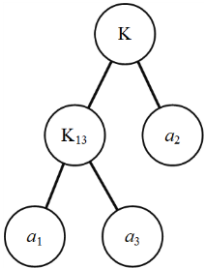


Рис. 3. Дерево комплексной оценки

Тогда при использовании стандартной матрицы свертки (см. рис. 2) получим $K_{13} = 3$ и $K = 3$, следовательно интегральный риск системы оценивается как высокий. Теперь предположим, что ущерб в результате реализации атаки a_1 не очень велик и матрица свёртки критерия K_{13} имеет следующий вид (см. рис. 4):

$\boldsymbol{K_1}$	**1**	3	2	1
	2	3	2	1
	3	3	3	2
		3	**2**	**1**
	$\boldsymbol{K_3}$			

Рис. 4. Пример матрицы свёртки критерия K_{13}

Матрицу свёртки критерия K оставим прежней. Тогда $K_{13} = 2$ и $K = 2$, и интегральный риск системы оценивается как средний.

3.2. ПОСТРОЕНИЕ ДЕРЕВА КОМПЛЕКСНОЙ ОЦЕНКИ ДЛЯ SMART-СИСТЕМ НА БАЗЕ «ИНТЕРНЕТА ВЕЩЕЙ»

Теперь применим предлагаемый алгоритм для построения дерева комплексной оценки интегрального риска SMART-системы на базе «Интернета вещей». Сформируем перечень типичных уязвимостей U и атак A на основе работ [17, 29]. Результаты представлены в таблицах 4 и 5.

Таблица 4. Перечень распространённых уязвимостей «Интернета вещей»

U	Уязвимость	Ссылка
u_1	Гетерогенная архитектура	[17]
u_2	Недостаточная физическая безопасность	[29]
u_3	Недостаточный сбор энергии	[29]
u_4	Ненужные открытые порты	[29]
u_5	Устаревшие протоколы	[17]
u_6	Слабое шифрование	[17, 29]
u_7	Ограниченный объем памяти и процессора	[17]
u_8	Небезопасные приложения	[17]
u_9	Недостаточный контроль доступа	[29]
u_{10}	Плохая аутентификация	[17, 29]
u_{11}	Слабые методы программирования	[29]
u_{12}	Неправильная возможность обновления ПО	[17, 29]
u_{13}	Недостаточные механизмы аудита	[29]

Таблица 5. Перечень атак в направлении «Интернета вещей»

A	Вид атаки	Затрагиваемые критерии ИБ (**К**онфиденциальность, **Ц**елостность, **Д**оступность)	Комментарии
a_1	Заражение	К, Ц, Д	Вредоносное ПО, программы вымогатели, вредоносные устройства, вредоносный код, заражение трояном
a_2	Подслушивание	К	Прослушивание, сканирование, сбор голосовых данных
a_3	Перегрузка возможностей системы	Д	Отказ в обслуживании, переполнение буфера, атака срыва стека, DoS, DDoS
a_4	Кража данных	К	Фишинг
a_5	Перенаправление	К, Д	Спуфинг (IP - , MAC - ,DNA -), имперсонация, атака посредника
a_6	Модификация	Ц, Д	Атаки на модификацию фирменного системного или программного обеспечения
a_7	Ввод	Ц	Атака с вводом ложных данных
a_8	Изменение	Д	Изменение топологии сети и снижение производительности сети, напр. атака «воронки»
a_9	Подбор	К, Ц	Подбор ключа путем перебора всех возможных вариантов (Brute-force), перебор по словарю
a_{10}	Атака по сторонним каналам	К	Анализ мощности, атака по времени, атака по ошибкам вычисления
a_{11}	Истощение	Д	Атаки - вампиры, атаки, истощающие батарею, напр. карусельные атаки, растягивающие атаки
a_{12}	Зашумление	Д	Сигналы с помехами: однотональными, узкополосными, частичными, широкополосными

Таблица 5 также содержит сведения о критериях информационной безопасности, которые будут нарушены при успешном выполнении соответствующего типа атаки. Построим матрицы соответствия уязвимостей атакам для критериев конфиденциальности, целостности и доступности (рис. 5). Нули в столбцах, соответствующих уязвимости u_1 «гетерогенная архитектура» отражают тот факт, что эта уязвимость не может быть использована для реализации какой-либо атаки сама по себе, а только в комбинации с другими уязвимостями.

	u_1	u_2	u_4	u_5	u_6	u_8	u_9	u_{10}	u_{11}	u_{12}	u_{13}
a_1	0		1	1	1	1		1	1	1	1
a_2	0	1	1	1	1		1		1		1
a_4				1	1		1	1	1		1
a_5	0			1	1	1					1
a_9					1			1			
a_{10}		1			1						

а) *Соответствие уязвимостей атакам на конфиденциальность*

	u_1	u_2	u_4	u_5	u_6	u_8	u_{10}	u_{11}	u_{12}	u_{13}
a_1	0		1	1	1	1	1	1	1	1
a_6		1						1	1	1
a_7							1	1		1
a_9					1		1			

б) *Соответствие уязвимостей атакам на целостность*

	u_1	u_2	u_3	u_4	u_5	u_6	u_7	u_8	u_{10}	u_{11}	u_{12}	u_{13}
a_1	0			1	1	1		1	1	1	1	1
a_3	0			1	1		1			1	1	1
a_5	0				1	1		1				1
a_6		1								1	1	1
a_8	0		1						1			
a_{11}	0		1									
a_{12}	0		1									

в) *Соответствие уязвимостей атакам на доступность*

Рис. 5. Соответствие типичных уязвимостей SMART-системы на основе Интернета вещей типовым атакам на этот класс систем

Отметим, что для технических систем, к которым относятся SMART-системы на основе «Интернета вещей», установление таких соответствий не представляет трудности. Для других классов сложных систем идентификация соответствий может быть отдельной задачей, требующей привлечения экспертов и использования специальных методов согласования экспертных оценок.

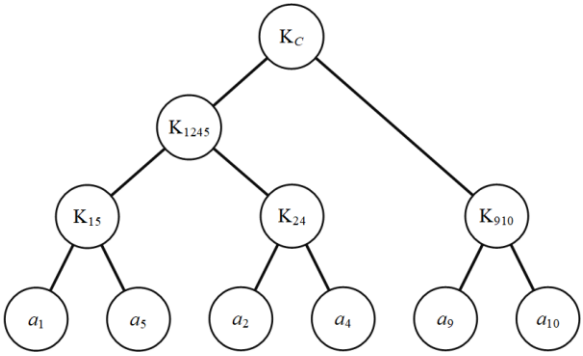
Построим матрицы E_C, E_I, E_A для поддеревьев конфиденциальности, целостности и доступности. Их размерность составит 63 × 2047, …, … соответственно. Такую же размерность будут иметь и матрицы D_C, D_I, D_A. Рассчитаем векторы S_C, S_I, S_A, B_C, B_I, B_A и, наконец, Y_C, Y_I, Y_A. В таблице 6 приведён фрагмент вектора Y_C, включающий показатели зависимостей всех пар атак на конфиденциальность.

Таблица 6. Рассчитанные показатели попарной зависимости атак на конфиденциальность; округление до 4 знака после запятой

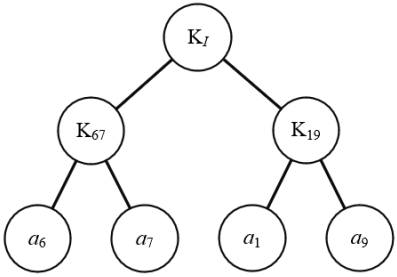
	Показатель зависимости Y_C	Порядок свёртки
a_1, a_2	0,0882	
a_1, a_4	0,0571	
a_1, a_5	0,0587	3
a_1, a_9	0,0059	
a_1, a_{10}	0,0019	
a_2, a_4	0,1080	2
a_2, a_5	0,0517	
a_2, a_9	0,0039	
a_2, a_{10}	0,0118	
a_4, a_5	0,0805	
a_4, a_9	0,0476	
a_4, a_{10}	0,0154	
a_5, a_9	0,0303	
a_5, a_{10}	0,0303	
a_9, a_{10}	0,2000	1

На основе значений элементов векторов Y_C, Y_I, Y_A построим поддеревья комплексной оценки рисков конфиденциальности, целостности и доступности. Как видно из таблицы 6, в поддереве конфиденциальности пары (a_9, a_{10}), (a_2, a_4) и (a_1, a_5) будут свёрнуты в первую очередь. Затем будут свёрнуты промежуточные критерии K_{15} и K_{24} с показателем зависимости, приблизительно равным 0,005 (для комбинации атак a_1, a_2, a_4, a_5), являющиеся результатом свёртки пар (a_1, a_5) и (a_2, a_4) соответственно. Наконец, комплексная оценка риска конфиденциальности получается как свёртка промежуточных критериев K_{910} и K_{1245}, являющихся в свою очередь свёртками соответственно (a_9, a_{10}) и (K_{15}, K_{24}).

Аналогичным образом строятся поддеревья комплексной оценки риска целостности и доступности. Результаты построения приведены на рис. 6, 7.



а) *Поддерево комплексной оценки риска конфиденциальности*



б) *Поддерево комплексной оценки риска целостности*

Рис. 6. Поддеревья комплексной оценки риска конфиденциальности и целостности

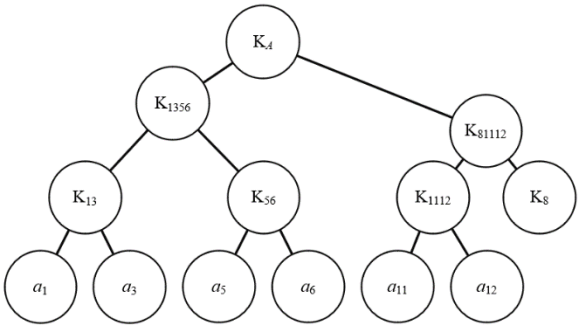


Рис. 7. Поддерево комплексной оценки риска доступности

4. Заключение

В настоящей работе описан алгоритм формирования структуры дерева комплексной оценки интегрального риска сложной информационной системы. В его основе лежит принцип агрегирования критериев по их взаимной зависимости. Предложенный в более ранней работе для свёртки стандартных критериев информационной безопасности – конфиденциальности, целостности и доступности, – он был распространён на задачу построения соответствующих им поддеревьев комплексной оценки. Базовыми критериями при этом выступают типичные для рассматриваемого класса систем атаки, а связь определяется на основе общих для них типовых уязвимостей. В данной работе алгоритм был применён для построения дерева комплексной оценки интегрального риска SMART-системы на основе «Интернета вещей», но предложенный подход может быть распространён на любые сложные системы с идентифицируемыми перечнями уязвимостей и атак.

Дальнейшим развитием данной работы видится модификация метода комплексного оценивания для учёта различных видов неопределенности.

Литература

1. АБДУЛОВА Е.А., КАЛАШНИКОВ А.О. *К вопросу управления рисками критической информационной инфраструктуры* // Управление развитием крупномасштабных систем (MLSD'2021): Труды 14-й Международной конференции. – 2021. – С. 1275–1282.
2. АЛЕКСЕЕВ А.О. *Исследование устойчивости механизмов комплексного оценивания к стратегическому поведению агентов (на примере согласования политики организации в области риск-менеджмента)* // Прикладная математика и вопросы управления. – 2019. – №4. – С. 136–154.
3. АЛЕКСЕЕВ А.О., КАТАЕВА Т.А. *Применение механизмов комплексного оценивания и матричных неанонимных обобщенных медианных механизмов согласования интересов агентов* // Вестник Южно-Уральского государственного университета. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2021. – №3. – С. 75–89.
4. АЛЕСКЕРОВ Ф.Т., ЯКУБА В.И. *Метод порогового агрегирования трехградационных ранжировок* // Доклады академии наук. – 2007. – Т. 413, №2. – С. 181–183.
5. БАКЕЕВ Д.Ш., ТИШИНА Н.А. *Программная реализация оценки рисков безопасности информации на основе гибридного метода* // Приоритетные направления инновационной деятельности в промышленности. Сборник научных статей по итогам пятой международной научной конференции. – 2020. – Т. 2. – С. 6–12.
6. БАРКАЛОВ С.А., НОВИКОВ Д.А., НОВОСЕЛЬЦЕВ В.И. и др. *Модели управления конфликтами и рисками* / Под ред. Д.А. Новикова]. – Воронеж: Научная книга, 2008. – 495 с.
7. БЕЗЗАТЕЕВ С.В., ЕЛИНА Т.Н., МЫЛЬНИКОВ В.А. и др. *Методика оценки рисков информационных систем на основе анализа поведения пользователей и инцидентов информационной безопасности* // Научно-технический вестник информационных технологий, механики и оптики. – 2021. – Т. 21, №4. – С. 553–561.

8. ВЛАСОВА Е.А., КАРПОВ Ю.А., ТАРАСОВ Б.В. *Построение дерева сверток для комплексной оценки на основе матрицы парных сравнений критериев* // Вестник Воронежского государственного технического университета. – 2009. – Т. 5, №10. – С. 187–191.
9. *ГОСТ Р 51901.1-2002 Менеджмент риска. Анализ риска технологических систем. – Официальное издание*. – М.: ИПК Изд-во стандартов, 2002 год.
10. ЗИМА В.М., КРЮКОВ Р.О., КРАВЧУК А.В. *Методика оценивания информационных рисков на основе анализа уязвимостей* // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. – 2019. – №11-12. – С. 36–46.
11. КАЛАШНИКОВ А.О., АНИКИНА Е.В. *Модели управления информационными рисками сложных систем* // Информационная безопасность. – 2020. – Т. 23, №2. – С. 191–202.
12. КАЛАШНИКОВ А.О. *Управление информационными рисками организационных систем: механизмы комплексного оценивания* // Информационная безопасность. – 2016. – Т. 3, №1. – С. 315–322.
13. КИСЕЛЕВА Т.В., МАСЛОВА Е.В. *Классификация рисков ИТ-сервисов и способы оценивания вероятностей их возникновения* // ИТНОУ: информационные технологии в науке, образовании и управлении. – 2020. – №1(15). – С. 67–71.
14. КОЛОСОК И.Н., ГУРИНА Л.А. *Оценка рисков управления киберфизической ЭЭС на основе теории нечетких множеств* // Методические вопросы исследования надежности больших систем энергетики. – 2019. – Т. 1, №70. – С. 238–247.
15. НОВИКОВ Д.А. *«Когнитивные игры»: линейная импульсная модель* // Проблемы управления. – 2008. – №3. – С. 14–22.
16. РЕЙ А.С., КАЛАШНИКОВ А.О. *Комплексная оценка информационных рисков. I: Краткий обзор подходов и методов* // Управление большими системами: сборник трудов. – 2024. – №110. – С. 68–86.
17. ABDULLAH A.A., WALEED A., MALEBARY S. et al. *A review of cyber security challenges attacks and solutions for Internet of Things based smart home* // Int. J. Comput. Sci. Netw. Secur. – 2019. – Vol. 9, No. 9. – P. 139–146.

18. AKINROLABU O., NURSE J.R.C., MARTIN A. et al. *Cyber risk assessment in cloud provider environments: Current models and future needs* // Computers & Security. – 2019. – Vol. 87. – P. 101600.
19. BOLBOT V., THEOTOKATOS G., BOULOUGOURIS E. et al. *A novel cyber-risk assessment method for ship systems* // Safety science. – 2020. – P. 104908.
20. ERSHADI M.J., FOROUZANDEH M. *Information Security Risk Management of Research Information Systems: A hybrid approach of Fuzzy FMEA, AHP, TOPSIS and Shannon Entropy* // J. Digit. Inf. Manag. – 2019. – Vol. 17, No. 6. – P. 321.
21. GUNES B., KAYISOGLU G., BOLAT P. *Cyber security risk assessment for seaports: A case study of a container port* // Computers & Security. – 2021. – Vol. 103. – P. 102196.
22. HÄCKEL B. *Assessing IT availability risks in smart factory networks* // Business Research. – 2019. – Vol. 12, No. 2. – P. 523–558.
23. HAN C.H., HAN C.H. *Semi-quantitative cybersecurity risk assessment by blockade and defense level analysis* // Process Safety and Environmental Protection. – 2021. – Vol. 155. – P. 306–316.
24. HE W., LI H., LI J. *Unknown vulnerability risk assessment based on directed graph models: a survey* // IEEE Access. – 2019. – Vol. 7. – P. 168201–168225.
25. *ISO/IEC 27005:2022(EN) Information security, cybersecurity and privacy protection — Guidance on managing information security risks* [Электронный ресурс]. – Режим доступа: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27005:ed-4:v1:en.
26. KIOSKLI K., POLEMI N. *A Socio-Technical Approach to Cyber-Risk Assessment* // World Academy of Science, Engineering and Technology Int. Journal of Electrical and Computer Engineerin. – 2020. – Vol. 14, No. 10. – P. 305–309.
27. KORNEEV N.V., KORNEEVA J.V., YURKEVICHYUS S.P. et al. *An Approach to Risk Assessment and Threat Prediction for Complex Object Security Based on a Predicative Self-Configuring Neural System* // Symmetry. – 2022. – Vol. 14, No. 1. – P. 102.
28. KRISPER M., DOBAJ J., MACHER. G. et al. *RISKEE: A risk-tree based method for assessing risk in cyber security* // European Conf. on Software Process Improvement. – 2019. – P. 45–56.

29. NESHENKO N., BOU-HARB E., CRICHIGNO J. et al. *Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations* // IEEE Communications Surveys & Tutorials. – 2019. – Vol. 21, No. 3. – P. 2702–2733.
30. NTAFLOUKAS K., MCCRUM D.P., PASQUALE L. *A Socio-Technical Approach to Cyber-Risk Assessment* // A cyber-physical risk assessment approach for Internet of Things enabled transportation infrastructure. – 2022. – Vol. 12, No. 18. – P. 9241.
31. PALKO D., BABENKO T., BIGDAN A. et al. *Cyber Security Risk Modeling in Distributed Information Systems* // Appl. Sci. – 2023. – Vol. 13, No. 4. – P. 2393.
32. RIOS E., REGO A., ITURBE E. et al. *Continuous quantitative risk management in smart grids using attack defense trees* // Sensors. – 2020. – Vol. 20. – P. 4404.
33. SCHMITZ C., PAPE S. *LiSRA: Lightweight security risk assessment for decision support in information security* // Computers & Security. – 2020. – Vol. 90. – P. 101656.
34. SUBRIADI A.P., NAJWA N.F. *The consistency analysis of failure mode and effect analysis (FMEA) in information technology risk assessment* // Heliyon. – 2020. – Vol. 6, No. 1. – e03161.
35. TUSHER H.M., MUNIM Z.H., NOTTEBOOM T.E. et al. *Cyber security risk assessment in autonomous shipping* // Maritime Economics & Logistics. – 2022. – Vol. 24, No. 2. – P. 208–227.
36. TUSHER H.M., MUNIM Z.H., NOTTEBOOM T.E. et al. *Development of the mechanism of assessing cyber risks in the internet of things projects* // 12th Conf. on Internet of Things, Smart Spaces, and Next Generation Networks and Systems., ruSMART-2019. St. Petersburg: Springer Int. Publishing. – 2019. – P. 481–494.
37. WANG Y., WANG Y.-H., QIN H. et al. *A systematic risk assessment framework of automotive cybersecurity* // Automotive Innovation. – 2021. – Vol. 4. – P. 253–261.
38. WANG Y., XUE W., ZHANG A. *Application of Big Data Technology in Enterprise Information Security Management and Risk Assessment* // Journal of Global Information Management (JGIM). – 2023. – Vol. 31, No. 3. – P. 1–16.

COMPLEX INFORMATION RISKS ASSESSMENT. II: ALGORITHM FOR IDENTIFYING THE STRUCTURE OF THE TREE OF INTEGRATED INFORMATION RISK ASSESSMENT

Anastasiya Rey, V.A. Trapeznikov Institute of Control Sciences of RAS, Moscow, Junior Researcher (a.rey@ipu.ru).
Alexander Shiroky, V.A. Trapeznikov Institute of Control Sciences of RAS, Moscow, Ph.D. in Physics and Mathematics Science, Senior Researcher (shiroky@ipu.ru).

Abstract: When assessing information security risks, it is essential to take into account the various types of uncertainties that are inherent in information systems. Current methods and algorithms for risk assessment may not account for all of these uncertainties, which can lead to inaccurate risk estimates. Therefore, it becomes necessary to develop a new or adapt an existing method for risk assessment that considers all types of uncertainty specific to the class of system under consideration. In this paper, we build on our previous idea of using an integrated assessment method to evaluate information risks. This method aggregates assessments of information systems based on standard information security criteria such as confidentiality, integrity, and availability. By incorporating these criteria, we aim to obtain more accurate and reliable risk estimates that take into account all relevant uncertainties. In the first part of the work, we demonstrated that this method, with appropriate modifications, allows for taking into account all necessary types of uncertainty. We propose an algorithm for identifying the structure of an integrated assessment tree based on the principle of combining related criteria. We demonstrate the efficiency of the algorithm by building risk assessment trees for confidentiality, integrity, and accessibility in SMART systems based on the Internet of Things using this approach.

Keywords: complex information systems, integral risk, complex assessment, accounting for uncertainty.

УДК 004.056.5
ББК 16.8
DOI: 10.25728/ubs.2024.111.04

Статья представлена к публикации членом редакционной коллегии И.В. Бычковым.

Поступила в редакцию 18.04.2024.
Опубликована 30.09.2024.