XXVIII Международной конференции. 16 декабря 2020 г., Москва. – Москва: ИПУ РАН, 2020. – С. 102-108.

4. *Исмаилов Ж.И., Кононов Д.А.* Новый Шелковый путь: эффективное управление контейнерными перевозками в условиях неопределенности / Труды 12-й Международной конференции «Управление развитием крупномасштабных систем» (MLSD'2019, Москва). – М.: ИПУ РАН, 2019. – С. 613-620.

5. *Исмаилов Ж.И., Кононов Д.А.* Оптимальное планирование грузооборота в условиях неопределенности / Управление развитием крупномасштабных систем (MLSD'2018). Материалы 11 международной конференции. В 2-х томах. – М.: ИПУ РАН, 2018. – Том. II. Секции 8-16. – С. 67-68.

6. *Исмаилов Ж.И., Кононов Д.А.* Система управления на железнодорожном транспорте: оптимальное планирование грузооборота в условиях неопределенности / Труды 11-й международной конференции «Управление развитием крупномасштабных систем» (MLSD'2018, Москва). В 3 томах. – М.: ИПУ РАН, 2018. – Т. 2. Секции 7-11. – С. 175-181.

DOI: 10.25728/iccss.2023.32.41.049

Рей А.С.

Способ построения оценки интегрального риска информационных систем на основе механизма комплексного оценивания

Аннотация: Идентификация и оценка рисков являются ключевыми задачами в управлении рисками. На основе полученных оценок осуществляется отбор мер по снижению уязвимостей и реагированию на инциденты безопасности. Существующие стандарты информационной безопасности описывают порядок действий лица, принимающего решения в этой области, но выбор конкретных моделей, методов и инструментов преимущественно оставляют на усмотрение последнего. Предлагаемые к применению стандартами в отдельных случаях количественные показатели требуют для расчета долговременных статистических данных, накопление

которых для информационных систем затруднительно в силу их высокой гибкости и изменчивости, делающей статистику прошлых периодов нерелевантной. Таким образом, создание новых и адаптация существующих в смежных областях методов оценки рисков информационных систем в условиях неопределенности остается актуальной задачей. В настоящей работе предлагается вариант адаптации механизма комплексного оценивания из теории управления организационными системами для оценки информационных рисков в условиях неопределенности.

Ключевые слова: оценка рисков, информационные системы, комплексное оценивание, информационная безопасность, атаки, уязвимости

В настоящее время активное развитие информационных систем вызывает необходимость совершенствовать методы по управлению информационными рисками, в том числе, по их оценке. Методы оценки риска в стандартах семейств ISO 27005 и 31000 подразделяются на качественные, количественные и комбинированные [1, 2]. При этом стандартами (за единичными исключениями) не зафиксированы рекомендации к применению конкретных способов и алгоритмов получения того или иного показателя. Также они не предлагают способов оценки риска системы в целом (интегрального риска), а описывают процедуры оценивания отдельно взятых активов, с дальнейшим их ранжированием для приоритезации осуществления защитных мер.

Отметим, что предложенные в [1] методы оценки локальных рисков сводятся к определению ценности активов, уровней угроз и уязвимостей с последующим учетом параметров степени вероятности возникновения угрозы и простоты использования уязвимости. В связи с этим, возникает необходимость в применении некой процедуры агрегирования, позволяющей получить оценку значения интегрального риска, характеризующего уровень защищенности системы в целом. Такая процедура должна быть применимой к качественным оценкам локальных рисков, а также обладать устойчивостью к изменениям оценок отдельных локальных рисков.

Информационные системы в целом позволяют накапливать большие объемы статистических данных о своем функционировании, причем обычно с относительно малыми затратами ресурсов. С учетом этого соображения представляется естественным применять при оценке их локальных рисков количественные подходы. Однако, на практике большинство информационных систем непрерывно эволюционируют и в значительной степени меняют порядок своего функционирования, что делает накопленный ранее массив исторических данных бесполезным. По этой причине в данной работе предлагается способ общей оценке интегрального риска информационных систем в условиях ограниченных данных.

Предлагаемая автором процедура базируется на механизме комплексного оценивания (МКО) [3]. Его преимуществом является устойчивость к изменениям оценок отдельных локальных рисков (в терминах теории управления организационными системами – неманипулируемость, [4]).

Ранее в [5] упомянутый механизм уже использовался для агрегирования оценок основных аспектов информационной безопасности – конфиденциальности, целостности и доступности. Однако автор не рассматривал способы построения самих оценок.

Построим способ комплексного оценивания интегрального риска информационных систем на основе оценок локальных рисков: конфиденциальности (C), целостности (I), доступности (A). Будем считать, что каждый из них оценивается в порядковой шкале и принимает одно из возможных значений $k_C \in K_C, k_I \in K_I, k_A \in K_A$ соответственно, причем $K_C, K_I, K_A \subset \mathbb{N}$. Тогда вектор $k = (k_C, k_I, k_A)^T$ описывает возможное состояние системы, и задача построения МКО сводится к нахождению отображения:

$$w(\cdot): K_C \times K_I \times K_A \to K_S, \qquad (1)$$

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

Решение задачи (1) обсуждалось в работе [5] исходя из посылки, что значения k_C, k_I, k_A уже получены тем или иным способом. В частности, структура дерева комплексного оценивания

была определена тем, что ввиду частичной зависимости целостности и доступности (утрата целостности ведет к утрате доступности), свертку этих локальных рисков следует рассматривать в первую очередь (рисунок 1).

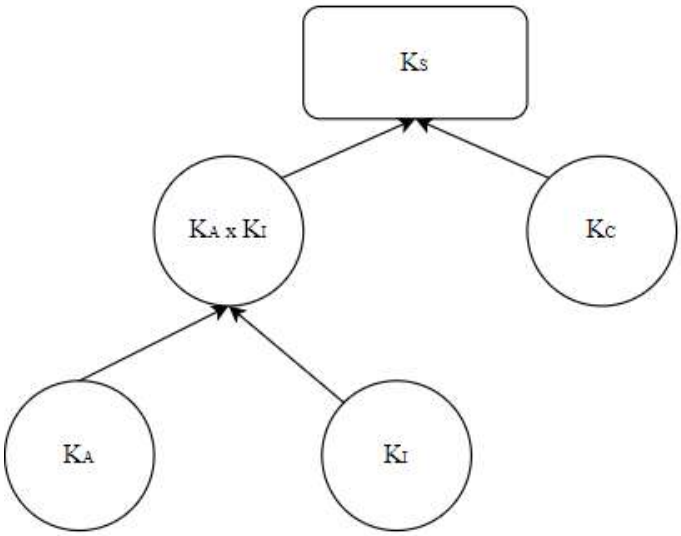

Рисунок 1 – Последовательная бинарная структура интегральной оценки информационного риска

Оценим значения локальных рисков по следующему алгоритму из шести шагов.

1. Составить список типичных для класса систем, соответствующего защищаемой информационной системы, уязвимостей U, а также списки известных разновидностей атак A_C, A_I и A_A, влияющих на конфиденциальность, целостность и доступность защищаемой системы соответственно.

2. Построить бинарные матрицы E_C, E_I, E_A размерностей $A_C \times U, A_I \times U, A_A \times U$ соответственно, описывающие соответствие уязвимостей атакам. Например, если атака $a \in A_C$ может быть проведена с эксплуатацией уязвимости $u \in U$, то в соответствующей клетке матрицы должна стоять 1, в противном случае – 0.

3. Присвоить классам атак в каждом из множеств A_C, A_I, A_A ранги в соответствии с числом возможных эксплуатируемых уязвимостей. Первый ранг присваивается той атаке или атакам, которые задействуют наибольшее число уязвимостей, ранг 2

присваивается атаке или атакам, которые задействуют следующее число уязвимостей после атак под рангом 1 и так далее.

4. Построить деревья комплексного оценивания для локальных рисков конфиденциальности, целостности и доступности в соответствии со следующими принципами:

4.1. Располагать ближе к корням критерии с наибольшей удельной степенью влияния на значения локальных рисков. Иными словами, чем больше уязвимостей можно задействовать для реализации атаки, тем больше значение соответствующего критерия влияет на локальный риск.

4.2. Сворачивать пары критериев с похожей удельной степенью влияния (в нашем случае – рангом, определенном на шаге 3).

Более подробно правила построения деревьев комплексного оценивания обсуждаются в работе [6].

5. Определить множества возможных значений для каждого из узлов дерева комплексного оценивания. При отсутствии особых соображений можно воспользоваться шкалой из трех значений, соответствующих низкому, среднему и высокому уровню риска [1].

6. Построить монотонные матрицы свертки критериев для каждого из узлов деревьев комплексного оценивания, полученных на шаге 4. При отсутствии особых соображений можно использовать матрицу, получающуюся применением метода порогового агрегирования [7] (рисунок 2).

K_2	**3**	1	2	3
	2	1	2	2
	1	1	1	1
		1	**2**	**3**
	K_1			

Рисунок 2 – Пример монотонной матрицы свертки

В заключение автор хотел бы отметить, что предложенный способ учитывает специфику информационных систем, а именно частую необходимость прибегать к экспертным оценкам при определении значений показателей уязвимостей. Кроме того, получаемые с его помощью оценки локальных рисков являются устойчивыми к изменениям отдельных сворачиваемых критериев.

В дальнейшем планируется перейти к рассмотрению задачи управления риском путем выделения ресурсов из ограниченного пула в модели «Защитник-Атакующий». При этом ее постановка будет отличаться от классической, поскольку Защитник будет оперировать уязвимостями, а атакующий – работать с атаками. В связи с тем, что данный вопрос не был рассмотрен в настоящей работе, потребуется определить, подходят ли для этой задачи известные методы или необходимо искать новые.

Литература:

1. ISO/IEC 27005:2022(en) Information security, cybersecurity and privacy protection – Guidance on managing information security risks. – URL: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27005:ed-4:v1:en (дата обращения 9.10.2023).

2. ISO 31000:2018 Risk management. – Guidelines. – URL: https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en (дата обращения 9.10.2023).

3. *Баркалов С.А., Новиков Д.А., Новосельцев В.И., Половинкина А.И., Шипилов В.Н.* Модели управления конфликтами и рисками: монография / Под ред. Д.А. Новикова. – Воронеж: Научная книга, 2008. – 497 с.

4. *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.

5. *Калашников А.О.* Управление информационными рисками организационных систем: механизмы комплексного оценивания // Информационная безопасность. – 2016. – Т. 3. № 1. – С. 315-322.

6. *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.

7. *Алескеров Ф.Т., Якуба В.И.* Метод порогового агрегирования трехградационных ранжировок // Доклады академии наук. – 2007. – Т. 413. №2. – С. 181-183.