Научная статья
УДК 004.056; DOI: 10.61260/2218-13X-2025-3-91-103

МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ ОРГАНИЗАЦИИ МЕЖМОДУЛЬНОГО ВЗАИМОДЕЙСТВИЯ В ИНТЕГРИРОВАННОЙ СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ

✉**Покусов Виктор Владимирович.**
Институт проблем информационной безопасности, г. Алматы, Республика Казахстан
✉***v@victor.kz***

Аннотация. Рассматривается задача построения интегрированных систем защиты информации в части организации информационного взаимодействия их модулей. Для обоснованного выбора наиболее эффективной организации такого взаимодействия предложена соответствующая пошаговая методика оценки, представленная в схематичном (с позиции эксперта и вычислительного средства) и аналитическом виде. В основе методики лежит графическое моделирование интегрированной системы защиты в аспекте взаимодействия ее модулей, что позволяет вычислить абсолютные показатели эффективности; используя такие же показатели для «идеальной» системы, определяются удельные показатели, подходящие для непосредственного сравнения и вычисления значения интегральной эффективности. Основываясь на предыдущих авторских исследованиях, предложены способы реализации шагов. Указывается новизна методики, ее теоретическая и практическая значимость, а также пути продолжения исследования.

Ключевые слова: интегрированная система защиты информации, архитектура, межмодульное взаимодействие, оценка эффективности, методика

Для цитирования: Покусов В.В. Методика оценки эффективности организации межмодульного взаимодействия в интегрированной системе защиты информации // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2025. № 3. С. 91–103. DOI: 10.61260/2218-13X-2025-3-91-103.

Scientific article

METHODOLOGY FOR ASSESSING THE EFFECTIVENESS OF ORGANIZING INTERMODULAR INTERACTION IN AN INTEGRATED INFORMATION SECURITY SYSTEM

✉**Pokusov Viktor V.**
Institute of Information Security Problems, Almaty, Republic of Kazakhstan
✉***v@victor.kz***

Abstract. This paper examines the problem of constructing integrated information security systems, specifically organizing the information interactions between their modules. To support a well-founded selection of the most effective organization for such interactions, a corresponding evaluation methodology is proposed, presented both schematically (from the perspective of an expert and a computing tool) and analytically. The methodology is based on graphical modeling of the integrated security system in terms of the interactions between its modules, enabling the calculation of absolute performance indicators. Using the same indicators for an «ideal» system, specific indicators are determined, suitable for direct comparison and the calculation of the integrated performance value. Based on the authors' previous research, methods for implementing these steps are proposed. The novelty of the methodology, its theoretical and practical significance, and potential future research are highlighted.

Keywords: integrated information security system, architecture, intermodule interaction, efficiency mark, methodology

For citation: Pokusov V.V. Methodology for assessing the effectiveness of organizing intermodular interaction in an integrated information security system // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2025. № 3. P. 91–103. DOI: 10.61260/2218-13X-2025-3-91-103.

Введение

Обеспечение информационной безопасности собственных ресурсов является одним из важнейших направлений деятельности любой современной организации [1]. Для этого, в частности, применяются соответствующие системы защиты, противодействующие информационным угрозам. Открытость ресурсов организаций приводит к необходимости применения ими сложных комплексов подсистем, предназначенных для отражения достаточно разнородных атак. Целенаправленность и многошаговость же проводимых атак требует от таких подсистем согласованного взаимодействия (что, впрочем, ведет с новому классу угроз информационно-технического взаимодействия [2]); например, в случае попытки проведения злоумышленником DDoS-атаки для выведения из строя электронного турникета с последующим физическим проникновением на территорию организации, системе защиты потребуется анализ как событий от сетевой подсистемы, так и от подсистемы контроля доступа. Одним из наиболее перспективных подходов к построению такого рода систем защиты является объединение их подсистем [3]. Так, в частности, автором ранее было предложено построение интегрированных систем защиты информации (ИСЗИ) на базе единого протокола [4]. Тем не менее, на сегодняшний день существуют и другие варианты построения ИСЗИ, обоснованный выбор наилучшей среди которых по критерию эффективности является достаточно сложной задачей [5]. Одним же из основных факторов, влияющих на успешность отражения атак (в особенности, многошаговых, действующих по различным каналам деструктивного воздействия), является организация «успешного» межмодульного взаимодействия в интегрированных системах защиты, предлагаемая методика оценки эффективности которой приводится далее.

Моделирование эффективности межмодульного взаимодействия в ИСЗИ

Ранее в работе [6] была описана общая идея авторского подхода к оценке эффективности межмодульного взаимодействия ИСЗИ, а также аналитический способ ее вычисления [7], суть чего заключается в следующих положениях.

Во-первых, любая ИСЗИ задается некоторой модульной архитектурой или архитектурой модулей, решающих определенные задачи и обменивающихся информацией (в том числе с внешней средой при реагировании на атаки) [8].

Во-вторых, взаимодействие модулей ИСЗИ описывается некоторой моделью [9].

В-третьих, каждый модуль имеет определенный тип, множество которых задается комбинацией элементов следующих категориальных пар: Человек VS Машина, Анализ VS Синтез, Данные VS Функция; таким образом, существует $2 \times 2 \times 2 = 8$ типов модулей.

В-четвертых, в интересах описания организации взаимодействия модулей достаточно воспользоваться только первыми двумя парами, поскольку третья не имеет существенного влияния на эффективность.

В-пятых, принцип работы ИСЗИ основан на том, что в ней присутствуют однотипные модули по детектированию каждого из классов атак [10] (например, программных [11, 12], сетевых [13], физических, социальных [14] и др.), а также модули, продуцирующие реакции противодействия соответствующим классам.

В-шестых, эффективность организации взаимодействия декомпозирована на три классических показателя: результативность – степень получения целевого эффекта, оперативность – быстрота его получения и ресурсоэкономность (или ресурсосбережение) – сохранение ресурсов для этого.

В-седьмых, поскольку точные значения показателей представляются сложновычислимыми, вместо них берется мера достижения таких же показателей, но для «идеальной» (скорее всего, теоретически реализуемой) ИСЗИ [15].

В-восьмых, каждый из показателей эффективности вычисляется, исходя из параметров, связанных с моделью взаимодействия в ИСЗИ.

В-девятых, данные параметры эффективности определяются по графическому представлению модели.

И, в-десятых, итоговая интегральная эффективность выводится на основании ее показателей и с учетом их весов, представляя собой в конечном итоге численное (скалярное) значение.

Схема методики, построенной на указанных выше положениях, приводится далее.

Схема методики

Схема методики (Методика) приведена на рис. 1; она состоит из трех слоев-столбцов: действия, выполняемые экспертом (левый столбец), непосредственные вычисления промежуточных и конечных значений (средний столбец), аналитическая схема вычисления (правый столбец). Также, числами в желтом круге отмечены шаги Методики, прямыми линиями – переходы между шагами, а пунктирными – связи по данным между шагами (кроме соседних, каждый из которых, как правило, использует результаты вычисления предыдущего); серый прямоугольник со скругленными краями соответствует группе шагов, выполняемых для каждой сравниваемой ИСЗИ; для компактности отображения схемы (но без потери сущности процесса) под эффективностью понимается относящаяся не к самой ИСЗИ в целом, а только к организации ее межмодульного информационного взаимодействия.

Автором описаны шаги Методики в порядке их выполнения (рис. 1):

Шаг 1. «Выбор способа моделирования» – выбор способа, с помощью которого архитектура каждой ИСЗИ будет переводиться в модель, построенную на едином базисе; формальная запись:

$$Modeling = Choice^{Modeling}(Modelings, Expert),$$

где $Modeling$ – способ моделирования ИСЗИ, $Choice^{Modeling}(\dots)$ – операция выбора способа моделирования, $Modelings$ – множество всех доступных способов моделирования, $Expert$ – производящий выбор эксперт.

Шаг 2. «Создание модели идеальной ИСЗИ» – проектирование гипотетической ИСЗИ, обладающей наивысшей эффективностью по всем показателям и построение модели, соответствующей архитектуре такой ИСЗИ [16]; формальная запись (здесь и далее, нижний индекс «0» соответствует идеальной ИСЗИ):

$$Model_0 = Modeling(Architecture_0, Expert),$$

где $Model_0$ – модель идеальной ИСЗИ; $Architecture_0$ – ее архитектура; $Expert$ – производящий моделирование эксперт.

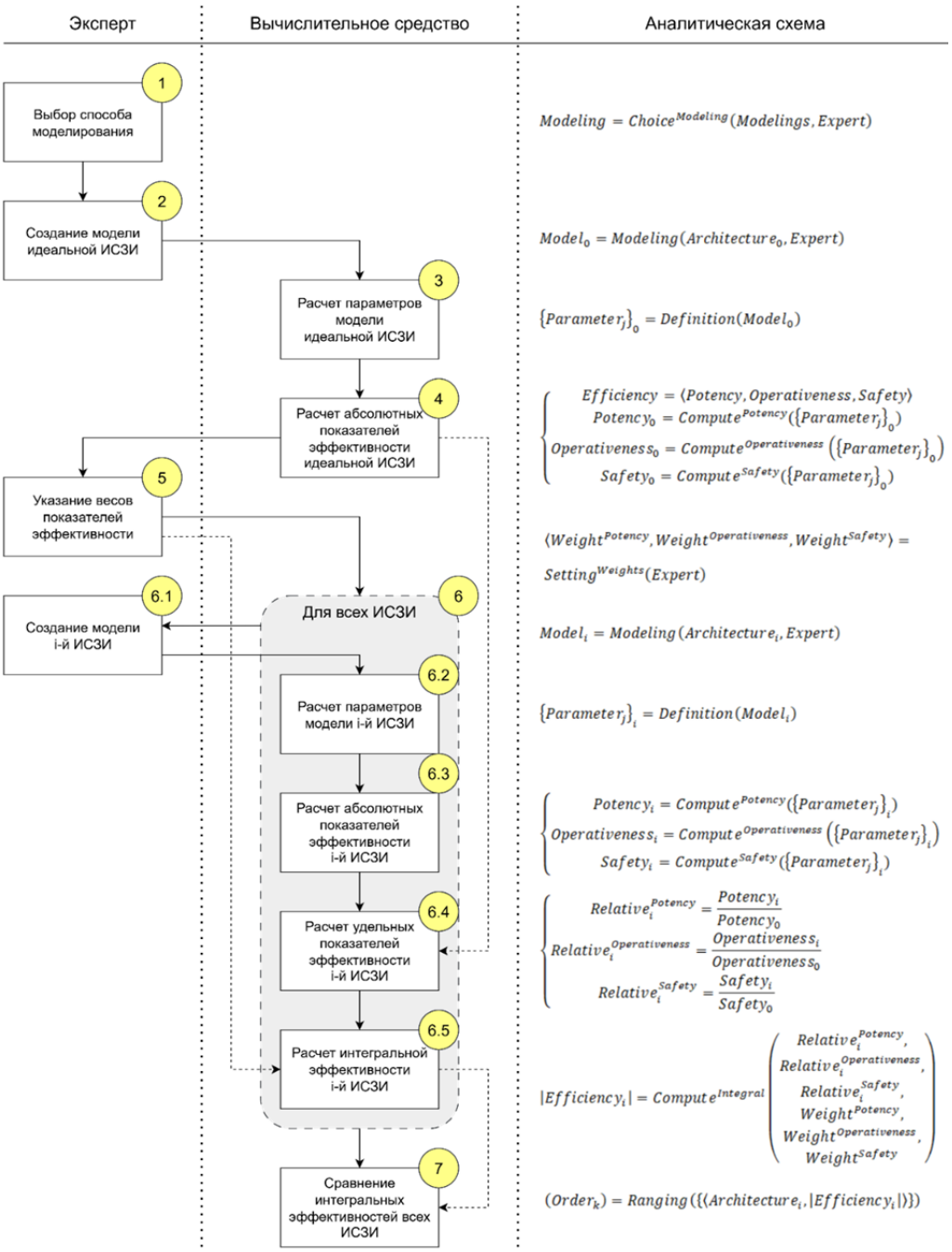

Рис. 1. **Схема методики оценки эффективности организации межмодульного информационного взаимодействия в ИСЗИ**

Шаг 3. «Расчет параметров модели идеальной ИСЗИ» – вычисление значений параметров модели согласно ее графическому представлению для идеальной ИСЗИ; формальная запись:

$$\{Parameter_j\}_0 = Definition(Model_0),$$

где $Parameter_j$ – j-й параметр модели ИСЗИ; $\{\dots\}_0$ – множество всех параметров модели идеальной ИСЗИ; $Definition(\dots)$ – операция определения параметров по графическому представлению модели.

Шаг 4. «Расчет абсолютных показателей эффективности идеальной ИСЗИ» – вычисление значений показателей эффективности организации взаимодействия в идеальной ИСЗИ; формальная запись:

$$\begin{cases} Efficiency = \langle Potency, Operativeness, Safety \rangle \\ Potency_0 = Compute^{Potency}(\{Parameter_j\}_0) \\ Operativeness_0 = Compute^{Operativeness}\left(\{Parameter_j\}_0\right) \\ Safety_0 = Compute^{Safety}\left(\{Parameter_j\}_0\right), \end{cases}$$

где E – эффективность для идеальной ИСЗИ в форме кортежа $\langle \dots \rangle$ из ее показателей; $Potency_0$, $Operativeness_0$, $Safety_0$ – показатели эффективности (результативность, оперативность и ресурсоэкономность [17]); $Compute^{\cdots}(\dots)$ – соответствующие операции вычисления каждого из них.

Шаг 5. «Указание весов показателей эффективности» – экспертное задание весовой важности каждого из показателей эффективности; формальная запись:

$$\langle Weight^{Potency}, Weight^{Operativeness}, Weight^{Safety} \rangle = Setting^{Weights}(Expert),$$

где $Weight^{Potency}$, $Weight^{Operativeness}$, $Weight^{Safety}$ – веса показателей; $Expert$ – производящий «взвешивание» эксперт.

Шаг 6. «Для всех ИСЗИ» – блок подшагов, выполняемых для каждой тестовой ИСЗИ, эффективность организации взаимодействия которой необходимо сравнить.

Шаг 6.1. «Создание модели *i*-й ИСЗИ» – шаг, аналогичный 2-му, но для *i*-й тестовой ИСЗИ; формальная запись:

$$Model_i = Modeling(Architecture_i, Expert),$$

где $Model_i$ – модель *i*-й тестовой ИСЗИ; $Architecture_i$ – ее архитектура.

Шаг 6.2. «Расчет параметров модели *i*-й ИСЗИ» – шаг, аналогичный 3-му, но для *i*-й тестовой ИСЗИ; формальная запись:

$$\{Parameter_j\}_i = Definition(Model_i),$$

где $\{\dots\}_i$ – параметры для модели *i*-й тестовой ИСЗИ.

Шаг 6.3. «Расчет абсолютных показателей эффективности *i*-й ИСЗИ» – шаг, аналогичный 4-му, но для *i*-й тестовой ИСЗИ; формальная запись:

$$\begin{cases} Potency_i = Compute^{Potency}(\{Parameter_j\}_i) \\ Operativeness_i = Compute^{Operativeness}\left(\{Parameter_j\}_i\right) \\ Safety_i = Compute^{Safety}\left(\{Parameter_j\}_i\right), \end{cases}$$

где $Potency_i$, $Operativeness_i$, $Safety_i$ – показатели эффективности организации взаимодействия для *i*-й тестовой ИСЗИ.

Шаг 6.4. «Расчет удельных показателей эффективности *i*-й ИСЗИ» – вычисление показателей эффективности организации взаимодействия как степени достижения *i*-й тестовой ИСЗИ значений таких же показателей для идеальной ИСЗИ:

$$\begin{cases} Relative_i^{Potency} = \dfrac{Potency_i}{Potency_0} \\ Relative_i^{Operativeness} = \dfrac{Operativeness_i}{Operativeness_0} \\ Relative_i^{Safety} = \dfrac{Safety_i}{Safety_0}, \end{cases}$$

где $Relative_i^{Potency}$, $Relative_i^{Operativeness}$ и $Relative_i^{Safety}$ – удельные показатели эффективности для *i*-й тестовой ИСЗИ.

Шаг 6.5. «Расчет интегральной эффективности *i*-й ИСЗИ» – вычисление итогового значения интегральной эффективности [18] организации взаимодействия для *i*-й тестовой ИСЗИ на основании ее показателей и с учетом весов каждого:

$$|Efficiency_i| = Compute^{Integral}\begin{pmatrix} Relative_i^{Potency}, \\ Relative_i^{Operativeness}, \\ Relative_i^{Safety}, \\ Weight^{Potency}, \\ Weight^{Operativeness}, \\ Weight^{Safety} \end{pmatrix},$$

где $|Efficiency_i|$ – интегральное значение эффективности; $Compute^{Integral}(\dots)$ – операция ее вычисления по удельным показателям и их весам.

Шаг 7. «Сравнение интегральных эффективностей всех ИСЗИ» – ранжирование архитектур всех тестовых ИСЗИ на основании значений их интегральных эффективностей:

$$(Order_k) = Ranging(\{\langle Architecture_i, |Efficiency_i|\rangle\}),$$

где $(\dots)$ – последовательность индексов тестовых ИСЗИ в порядке уменьшения; $Order_k$ – индекс тестовой ИСЗИ, находящийся в k-й позиции ранжирования согласно интегральной эффективности (то есть $Order_1$ – индекс ИСЗИ с наивысшим рангом и эффективностью организации взаимодействия); $Ranging(\dots)$ – операция ранжирования ИСЗИ согласно их эффективностям, принимающая в качестве параметра множество кортежей из архитектуры *i*-й тестовой ИСЗИ ($Architecture_i$) и вычисленной для нее интегральной эффективностью организации взаимодействия модулей.

Реализация методики

Кратко описана авторскую реализация каждого шага Методики.

На Шаге 1 в качестве способа моделирования можно воспользоваться предложенным ранее категориальным делением модулей на типы, соответствующие некоторой уникальной (в рамках ИСЗИ) задаче; организация же взаимодействия в ИСЗИ будет определяться информационными потоками между выделенными таким образом модулями.

Шаг 2 предназначен для создания модели идеальной ИСЗИ, предложенный вид которой приведен на рис. 2.

Согласно идеальной ИСЗИ (рис. 2), как группа человекоориентированных, так и группа машиноориентированных модулей, осуществляющие анализ и синтез, обладают крайне высокой интеграцией (в рамках группы), поскольку не имеют внешних (относительно себя) каналов обмена информацией.

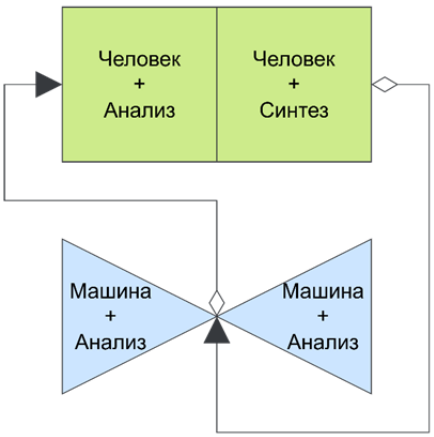

Рис. 2. **Модель идеальной ИСЗИ**

Шаги 3 и 6.2 предназначены для вычисления параметров модели по ее графическому представлению, что может быть сделано следующим образом. Модель имеет три параметра, каждый из которых влияет на собственный показатель эффективности организации межмодульного взаимодействия и вычисляется следующим образом.

Во-первых, результативность интерпретируется как отказоустойчивость ИСЗИ при отражении атак [19], вероятность чего имеет обратную зависимость от максимальной нагрузки на один из модулей, определяемой максимальным количеством его информационных потоков – связей между модулями в модели (то есть чем больше связей, тем более вероятна перегрузка данного модуля системы и, следовательно, невозможность реагирования на атаку); формальная запись параметра следующая:

$$Parameter^{Connections} = \max(\{|Module_x^{Connections}|\}),$$

где $Parameter^{Connections}$ – параметр модели, связанный с количеством соединений; $\max(\dots)$ – операция вычисления максимального значения из множества; $Module_x^{Connections}$ – множество соединений x-го модуля с остальными; $|\dots|$ – размер множества (в данном случае количество соединений модуля).

Во-вторых, оперативность интерпретируется как время реагирования на атаку [20], что имеет обратную зависимость от максимальной длины пути информации от момента детектирования атаки до момента продуцирования реакции на нее (то есть чем через большее количество модулей необходимо пройти сигналу об атаке, тем с большим опозданием будет создана противодействующая реакция); формальная запись параметра следующая:

$$Parameter^{Length} = \max(\{Path^{In,Out}(Model_i)\}),$$

где $Parameter^{Length}$ – параметр модели, связанный с длиной пути; $Path^{In,Out}(\dots)$ – операция вычисления пути между модулями In и Out (используя заданную модель организации межмодульного взаимодействия, передаваемую через параметр); In и Out – модули детектирования какого-либо класса атаки и реагирования на него.

И, в-третьих, ресурсоэкономность интерпретируется как минимизация ресурсов для построения ИСЗИ [21], что имеет обратную зависимость от количества всех используемых модулей (то есть чем больше количество, тем больше ресурсов требуется); формальная запись параметра следующая:

$$Parameter^{Modules} = |\{Module_l\}|,$$

где $Parameter^{Modules}$ – параметр модели, связанный с количеством модулей; $Module_l$ – l-ый модуль из множества архитектуры ИСЗИ (соответственно, $|...|$ – их количество).

На шагах 4 и 6.3 производится вычисление абсолютных значений показателей эффективности по параметрам, вычисленным на предыдущих шагах, указанным ранее способом:

$$\begin{cases} Parameter^{Connections} = \max\left(\left\{\left|Module_x^{Connections}\right|\right\}\right) \\ Operativeness \sim \dfrac{1}{Parameter^{Length}} \\ Safery \sim \dfrac{1}{Parameter^{Modules}}, \end{cases}$$

где в данном случае знак «~» соответствует зависимости между показателями эффективности и параметрами модели, что, хотя и не позволяет вычислить точные значения, однако может быть преобразовано в некоторый коэффициент (его значение не принципиально, так как оно будет «сокращено» при вычислениях на следующих шагах).

Шаг 5 выполняется экспертом и предназначен для выбора веса каждого показателя в интегральной эффективности организации межмодульного взаимодействия [22], которые в общем случае могут считаться равными:

$$Weight^{Potency} = Weight^{Operativeness} = Weight^{Safety}.$$

На шаге 6.1 эксперт по выбранной ИСЗИ создает ее модель, отражающую взаимодействие модулей архитектуры. Так, автором были выделены следующие ИСЗИ и их особенности: децентрализованная – для каждого класса атак предназначены собственные слабо зависимые службы (осуществляющие, впрочем, информационный обмен для согласованного противодействия комплексным атакам) [23]; централизованная, в которой, в отличие от децентрализованной, выделена центральная группа тесно связанных модулей для анализа атак и синтеза противодействий им; линейная, в которой службы по противодействию каждому классу атак полностью независимы (то есть не имеют каких-либо связей для передачи информации касательно других классов атак); каскадная – близкая к децентрализованной за отличием того, что атакующие воздействия обрабатывают в определенном порядке; и авторская – гипотетическая, построенная на едином протоколе взаимодействия модулей.

Шаг 6.4 производит вычисление удельных показателей эффективности, равных доле абсолютных показателей каждой тестовой ИСЗИ к идеальной. Именно на этом шаге происходит сокращение коэффициентов, заменяеющих операцию «~» на шагах 4 и 6.3.

На шаге 6.5 производится итоговое вычисление эффективности организации взаимодействия на основании ее удельных показателей и с учетом их весов, что может быть представлено как среднеквадратичное суммирование с весами:

$$|Efficiency_i| = \sqrt{\begin{matrix} \left(Weight^{Potency} \times Relative_i^{Potency}\right)^2 + \\ \left(Weight^{Operativeness} \times Relative_i^{Operativeness}\right)^2 + \\ \left(Weight^{Safety} \times Relative_i^{Safety}\right)^2. \end{matrix}}$$

Весовые коэффициенты должны быть нормированы соответствующим образом.

Шаг 7 является более формальным, поскольку предназначен для итогового ранжирования всех ИСЗИ по значению эффективностей организации их межмодульного взаимодействия. Соответственно, индекс ИСЗИ с наивысшей эффективностью будет находиться первым в ранжированном списке, за которым будет следовать второй и т.д. В случае наличия идеальной ИСЗИ среди тестируемых, она всегда будет на первом месте.

Необходимо отметить, при существенном усложнении параметров модели и показателей эффективности, механизм ранжирования также будет усложнен, в частности, применением искусственного интеллекта [24].

Таким образом, все шаги Методики не только имеют аналитическую запись (корректность которой обосновывает общую ее работоспособность), но и могут быть реализованы практически (инстурементально).

Заключение

На данном этапе авторского исследования феномена ИСЗИ предложена многошаговая методика оценки эффективности организации в ней межмодульного информационного взаимодействия, представленная в схематичном или аналитическом виде. В процессе ее применения вычисляются интегральные эффективности для тестовых ИСЗИ, за чем следует их сравнение. Новизна предложенной методики заключается в переходе от абстрактных архитектур модулей ИСЗИ (в графической форме) к конкретным числовым значениям показателей эффективности, способы вычисления которых на данный момент отсутствуют в принципе. Теоретическая значимость методики заключается в получении строгой аналитической схемы ее проведения, а практическая значимость – в возможности обоснованного выбора схемы взаимодействия модулей ИСЗИ при проектировании ее архитектуры. Продолжением работы должна стать проверка методики на практике и оценка влияния результатов ее применения на целевое противодействие информационным атакам [25].

Список источников

1. Цифровые технологии и проблемы информационной безопасности / Т.И. Абдуллин [и др.]. СПб.: Санкт-Петербургский государственный экономический университет, 2021. 163 с.

2. Буйневич М.В., Покусов В.В., Израилов К.Е. Модель угроз информационно-технического взаимодействия в интегрированной системе защиты информации // Информатизация и связь. 2021. № 4. С. 66–73. DOI: 10.34219/2078-8320-2021-12-4-66-73.

3. Assessment of Information Security in Integrated Systems / T.Yu. Khashirova [et al.] // Quality management, transport and information security, information technologies: the proceedings of international conference. Yaroslavl, 2021. P. 201–205. DOI: 10.1109/ITQMIS53292.2021.9642824.

4. Покусов В.В. Формализация и определение корректности протокола информационно-технического взаимодействия (на примере интегрированной системы защиты информации) // Информатизация и связь. 2021. № 2. С. 55–68. DOI: 10.34219/2078-8320-2021-12-2-55-68.

5. Буйневич М.В., Ложкина О.В., Ярошенко А.Ю. Архитектурные модели комплексной и интегрированной безопасности информационных систем: сравнительный анализ подходов // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2021. № 1. С. 100–108.

6. Покусов В.В. Оценка эффективности системы обеспечения ИБ. Часть 1. Показатели и модели представления // Защита информации. Инсайд. 2019. № 2 (86). С. 54–60.

7. Покусов В.В. Оценка эффективности системы обеспечения ИБ. Часть 2. Методика и результаты // Защита информации. Инсайд. 2019. № 3 (87). С. 64–72.

8. Основные принципы проектирования архитектуры современных систем защиты / М.В. Буйневич [и др.] // Национальная безопасность и стратегическое планирование. 2020. № 3 (31). С. 51–58. DOI: 10.37468/2307-1400-2020-3-51-58.

9. Eryshov V.G., Ilina D.V. Model of the Integrated System of Protection of Information Systems of the Organization // The proceedings of Wave Electronics and its Application in Information and Telecommunication Systems. Saint-Petersburg, 2021. P. 1–4. DOI: 10.1109/WECONF51603.2021.9470711.

10. Буйневич М.В., Моисеенко Г.Ю. Комбинирование разнородных деструктивных воздействий на информационную систему и противодействие атакам (на примере инсайдерской деятельности и DDOS-атаки) // Информационные технологии и телекоммуникации. 2023. Т. 11. № 3. С. 27–36. DOI: 10.31854/2307-1303-2023-11-3-27-36.

11. Леонов Н.В. Противодействие уязвимостям программного обеспечения. Часть 1. Онтологическая модель // Вопросы кибербезопасности. 2024. № 2 (60). С. 87–92. DOI: 10.21681/2311-3456-2024-2-87-92.

12. Леонов Н.В. Противодействие уязвимостям программного обеспечения. Часть 2. Аналитическая модель и концептуальные решения // Вопросы кибербезопасности. 2024. № 3 (61). С. 90–95. DOI: 10.21681/2311-3456-2024-3-90-95.

13. Yuan Q., Ma W. Research on Computer Network Information Security Strategy under the Background of Big Data // Networking, informatics and computing: the proceedings of international conference. Palermo, 2023. P. 214–218. DOI: 10.1109/ICNETIC59568.2023.00051.

14. Власов Д.С. К вопросу о признаках инсайдерской деятельности // Национальная безопасность и стратегическое планирование. 2024. № 1 (45). С. 35–45. DOI: 10.37468/2307-1400-2024-1-35-45.

15. White E.F.R., Dhillon G. Synthesizing Information System Design Ideals to Overcome Developmental Duality in Securing Information Systems // System Sciences: the proceedings of 38th annual hawaii international conference. Big Island, USA, 2005. P. 186a–186a. DOI: 10.1109/HICSS.2005.572.

16. Некрасов А.В., Калач А.В., Исаев А.А. Идеальное моделирование – основа совершенствования системы противопожарной защиты предприятий // Пожаровзрывобезопасность. 2011. Т. 20. № 9. С. 31–34.

17. Курта П.А. Эффективностная модель интерфейса взаимодействия пользователя с информационным сервисом запросного типа // Труды учебных заведений связи. 2023. Т. 9. № 6. С. 102–115. DOI: 10.31854/1813-324X-2023-9-6-102-115.

18. Аристова Д.А., Макеева Е.З., Федорова О.В. Интегральный показатель эффективности при оценке проектов в транспортной отрасли // Экономика железных дорог. 2022. № 4. С. 38–44.

19. Критерий построения и стратегия функционирования информационно-телекоммуникационной системы с защитой от деструктивных воздействий / М.В. Кныш [и др.] // Наукоемкие технологии. 2024. Т. 25. № 5. С. 5–15. DOI: 10.18127/j19998465-202405-01.

20. Будаков В.И., Кальченко Д.В., Королева Т.М. К вопросу об оперативности реагирования на чрезвычайные ситуации // Проблемы безопасности и чрезвычайных ситуаций. 2013. № 6. С. 130–135.

21. Макаров О.Ю., Рогозин Е.А., Хвостов В.А. Математическая модель обоснования требований к показателю ресурсоемкости систем защиты информации от несанкционированного доступа // Вестник Воронежского государственного технического университета. 2007. Т. 3. № 4. С. 102–104.

22. Хубаев Г.Н. Экспертная оценка весов показателей: вариант реализации // Вопросы экономических наук. 2008. № 5 (33). С. 134–136.

23. Информационная безопасность информационных систем с элементами централизации и децентрализации / С.В. Кругликов [и др.] // Вопросы кибербезопасности. 2020. № 1 (35). С. 2–7. DOI: 10.21681/2311-3456-2020-01-02-07.

24. Ярошенко А.Ю. Интеллектуальный метод решения задачи ранжирования требованийпо информационной безопасности в организационной системе ее обеспечения // Автоматизация в промышленности. 2024. № 12. С. 47–52. DOI: 10.25728/avtprom.2024.12.10.

25. Vitenburg E., Nikishova A. Project of Automated System's Information Security System Selection // EastConf: the proceedings of international science and technology conference. Vladivostok, 2019. P. 1–5. DOI: 10.1109/EastConf.2019.8725345.

References

1. Cifrovye tekhnologii i problemy informacionnoj bezopasnosti / T.I. Abdullin [i dr.]. SPb.: Sankt-Peterburgskij gosudarstvennyj ekonomicheskij universitet, 2021. 163 s.

2. Bujnevich M.V., Pokusov V.V., Izrailov K.E. Model' ugroz informacionno-tekhnicheskogo vzaimodejstviya v integrirovannoj sisteme zashchity informacii // Informatizaciya i svyaz'. 2021. № 4. S. 66–73. DOI: 10.34219/2078-8320-2021-12-4-66-73.

3. Assessment of Information Security in Integrated Systems / T.Yu. Khashirova [et al.] // Quality management, transport and information security, information technologies: the proceedings of international conference. Yaroslavl, 2021. P. 201–205. DOI: 10.1109/ITQMIS53292.2021.9642824.

4. Pokusov V.V. Formalizaciya i opredelenie korrektnosti protokola informacionno-tekhnicheskogo vzaimodejstviya (na primere integrirovannoj sistemy zashchity informacii) // Informatizaciya i svyaz'. 2021. № 2. S. 55–68. DOI: 10.34219/2078-8320-2021-12-2-55-68.

5. Bujnevich M.V., Lozhkina O.V., Yaroshenko A.Yu. Arhitekturnye modeli kompleksnoj i integrirovannoj bezopasnosti informacionnyh sistem: sravnitel'nyj analiz podhodov // Nauch.-analit. zhurn. «Vestnik S.-Peterb. un-ta GPS MChS Rossii». 2021. № 1. S. 100–108.

6. Pokusov V.V. Ocenka effektivnosti sistemy obespecheniya IB. Chast' 1. Pokazateli i modeli predstavleniya // Zashchita informacii. Insajd. 2019. № 2 (86). S. 54–60.

7. Pokusov V.V. Ocenka effektivnosti sistemy obespecheniya IB. Chast' 2. Metodika i rezul'taty // Zashchita informacii. Insajd. 2019. № 3 (87). S. 64–72.

8. Osnovnye principy proektirovaniya arhitektury sovremennyh sistem zashchity / M.V. Bujnevich [i dr.] // Nacional'naya bezopasnost' i strategicheskoe planirovanie. 2020. № 3 (31). S. 51–58. DOI: 10.37468/2307-1400-2020-3-51-58.

9. Eryshov V.G., Ilina D.V. Model of the Integrated System of Protection of Information Systems of the Organization // The proceedings of Wave Electronics and its Application in Information and Telecommunication Systems. Saint-Petersburg, 2021. P. 1–4. DOI: 10.1109/WECONF51603.2021.9470711.

10. Bujnevich M.V., Moiseenko G.Yu. Kombinirovanie raznorodnyh destruktivnyh vozdejstvij na informacionnuyu sistemu i protivodejstvie atakam (na primere insajderskoj deyatel'nosti i DDOS-ataki) // Informacionnye tekhnologii i telekommunikacii. 2023. T. 11. № 3. S. 27–36. DOI: 10.31854/2307-1303-2023-11-3-27-36.

11. Leonov N.V. Protivodejstvie uyazvimostyam programmnogo obespecheniya. Chast' 1. Ontologicheskaya model' // Voprosy kiberbezopasnosti. 2024. № 2 (60). S. 87–92. DOI: 10.21681/2311-3456-2024-2-87-92.

12. Leonov N.V. Protivodejstvie uyazvimostyam programmnogo obespecheniya. Chast' 2. Analiticheskaya model' i konceptual'nye resheniya // Voprosy kiberbezopasnosti. 2024. № 3 (61). S. 90–95. DOI: 10.21681/2311-3456-2024-3-90-95.

13. Yuan Q., Ma W. Research on Computer Network Information Security Strategy under the Background of Big Data // Networking, informatics and computing: the proceedings of international conference. Palermo, 2023. P. 214–218. DOI: 10.1109/ICNETIC59568.2023.00051.

14. Vlasov D.S. K voprosu o priznakah insajderskoj deyatel'nosti // Nacional'naya bezopasnost' i strategicheskoe planirovanie. 2024. № 1 (45). S. 35–45. DOI: 10.37468/2307-1400-2024-1-35-45.

15. White E.F.R., Dhillon G. Synthesizing Information System Design Ideals to Overcome Developmental Duality in Securing Information Systems // System Sciences: the proceedings of 38th annual hawaii international conference. Big Island, USA, 2005. P. 186a–186a. DOI: 10.1109/HICSS.2005.572.

16. Nekrasov A.V., Kalach A.V., Isaev A.A. Ideal'noe modelirovanie – osnova sovershenstvovaniya sistemy protivopozharnoj zashchity predpriyatij // Pozharovzryvobezopasnost'. 2011. T. 20. № 9. S. 31–34.

17. Kurta P.A. Effektivnostnaya model' interfejsa vzaimodejstviya pol'zovatelya s informacionnym servisom zaprosnogo tipa // Trudy uchebnyh zavedenij svyazi. 2023. T. 9. № 6. S. 102–115. DOI: 10.31854/1813-324X-2023-9-6-102-115.

18. Aristova D.A., Makeeva E.Z., Fedorova O.V. Integral'nyj pokazatel' effektivnosti pri ocenke proektov v transportnoj otrasli // Ekonomika zheleznyh dorog. 2022. № 4. S. 38–44.

19. Kriterij postroeniya i strategiya funkcionirovaniya informacionno-telekommunikacionnoj sistemy s zashchitoj ot destruktivnyh vozdejstvij / M.V. Knysh [i dr.] // Naukoemkie tekhnologii. 2024. T. 25. № 5. S. 5–15. DOI: 10.18127/j19998465-202405-01.

20. Budakov V.I., Kal'chenko D.V., Koroleva T.M. K voprosu ob operativnosti reagirovaniya na chrezvychajnye situacii // Problemy bezopasnosti i chrezvychajnyh situacij. 2013. № 6. S. 130–135.

21. Makarov O.Yu., Rogozin E.A., Hvostov V.A. Matematicheskaya model' obosnovaniya trebovanij k pokazatelyu resursoemkosti sistem zashchity informacii ot nesankcionirovannogo dostupa // Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta. 2007. T. 3. № 4. S. 102–104.

22. Hubaev G.N. Ekspertnaya ocenka vesov pokazatelej: variant realizacii // Voprosy ekonomicheskih nauk. 2008. № 5 (33). S. 134–136.

23. Informacionnaya bezopasnost' informacionnyh sistem s elementami centralizacii i decentralizacii / S.V. Kruglikov [i dr.] // Voprosy kiberbezopasnosti. 2020. № 1 (35). S. 2–7. DOI: 10.21681/2311-3456-2020-01-02-07.

24. Yaroshenko A.Yu. Intellektual'nyj metod resheniya zadachi ranzhirovaniya trebovanijpo informacionnoj bezopasnosti v organizacionnoj sisteme ee obespecheniya // Avtomatizaciya v promyshlennosti. 2024. № 12. S. 47–52. DOI: 10.25728/avtprom.2024.12.10.

25. Vitenburg E., Nikishova A. Project of Automated System\'s Information Security System Selection // EastConf: the proceedings of international science and technology conference. Vladivostok, 2019. P. 1–5. DOI: 10.1109/EastConf.2019.8725345.

Информация о статье:
Статья поступила в редакцию: 05.08.2025; одобрена после рецензирования: 16.09.2025;
принята к публикации: 18.09.2025
Information about the article:
The article was submitted to the editorial office: 05.08.2025; approved after review: 16.09.2025;
accepted for publication: 18.09.2025

Сведения об авторах:
Покусов Виктор Владимирович, исследователь-преподаватель Института проблем информационной безопасности (050000, Республика Казахстан, г. Алматы, ул. Мынбаева, 46/48), e-mail: v@victor.kz, https://orcid.org/0000-0002-5251-3452, SPIN-код: 5308-7334

Information about authors:
Pokusov Viktor V., researcher and lecturer at the Institute of information security problems (050000, Republic of Kazakhstan, Almaty, Mynbaev st., 46/48), e-mail: v@victor.kz, https://orcid.org/0000-0002-5251-3452, SPIN: 5308-7334