УДК 004.056.5
DOI: 10.15593/2224-9397/2020.4.12

А.С. Шабуров, А.И. Шлыков

Пермский национальный исследовательский политехнический университет,
Пермь, Россия

РАЗРАБОТКА МЕТОДА ОЦЕНКИ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ КОММЕРЧЕСКИХ ПРЕДПРИЯТИЙ

Современные информационные системы подвергаются угрозам при недостаточной оценке эффективности защиты информации. Эта проблема характеризует нарушение процесса управления информационной безопасностью. Очевидно, что нехватка научной базы методов и алгоритмов оценки приводит к нарушению эффективности защиты. С позиции влияния на бизнес при оценке экономической эффективности выявляются уязвимые показатели. Поэтому научной задачей является обеспечение процесса функционирования системы защиты информации методом оценки экономической эффективности. **Цель исследования:** разработка актуального метода оценки экономической эффективности системы защиты информации на основе модели экономически эффективного функционирования системы. **Методы:** оценка экономической эффективности определяется аналитической и математической моделями лингвистического описания эффективной системы защиты. На их основе строится метод из 9 последовательных этапов оценивания. Он реализует организационный и математический алгоритм, основанный на методе анализа иерархий. **Результаты:** в статье приводятся результаты проектирования лингвистической модели в виде неориентированного графа подбора подсистем, требований и средств защиты информации для обеспечения максимальной экономической эффективности системы. Новизна подхода заключается в осуществлении предварительного расчёта результатов метода оценки экономической эффективности. Совместно с моделью, проведено проектирование метода оценки. Разработанный метод получил апробацию на реальном объекте защиты, с его помощью были получены достоверные показатели эффективности системы защиты информации. Результатами моделирования являются данные экономической эффективности, степени риска для информационной системы, а также параметры модели, дающие словесное описания параметров эффективной системы защиты, в том числе коэффициент защищенности. **Практическая значимость:** разработанный метод испытан и применен в рамках улучшения показателей системы защиты на объекте – коммерческом предприятии Пермского края. Также в статье даны рекомендации по применению метода в организационных мероприятиях по защите информации. Более того, авторами обозначены пути развития метода оценки экономической эффективности в виде многокритериального подхода.

Ключевые слова: эффективность защиты информации, экономическая эффективность, модели и методы оценки, многокритериальная оценка, метод парных сравнений, риск информационной безопасности.

A.S. Shaburov, A.I. Shlykov

Perm National Research Polytechnic University, Perm, Russian Federation

DEVELOPMENT OF METHOD FOR ASSESSING THE ECONOMIC EFFICIENCY OF THE INFORMATION SECUTITY SYSTEM FOR COMMERCIAL ENTERPRISES

Modern systems are vulnerable to threats because of insufficient assessment of the information security effectiveness. This problem characterizes a breach of the information security management process. It is obvious that the lack of a scientific base of methods and assessment algorithms leads to a violation of protection effectiveness. From the standpoint of business impact, the cost-benefit assessment identifies vulnerable indicators, ensuring the reliability of business processes. Therefore, the scientific task is to ensure the process of information security system functioning by assessing economic efficiency. **Purpose:** development of an up-to-date method for assessing the economic efficiency of an information security system based on model of economically efficient functioning of the system. **Methods:** analytical and mathematical models of the linguistic description of an effective protection system determine the assessment of economic efficiency. The method based on it consists 9 consecutive stages of assessment. It implements an organizational and mathematical algorithm based on the hierarchy analysis method. **Results:** the article presents the results of designing a linguistic model in the form of an undirected graph. It selects subsystems, requirements and information security tools to ensure the maximal economic efficiency of the system. Graph carries out a preliminary calculation of the assessing economic efficiency results. Article provides the development of the assessment method connected with economical model. The developed method tested on a real protected object. Economical method calculated indicators of the information security system efficiency. As a result, method calculates economic efficiency data, the degree of risk for information system, as well as model parameters. It gives a verbal description of the effective security system parameters including the protection coefficient. **Practical relevance:** the developed method tested and applied in the framework of improving the performance of the security system at the facility based on commercial enterprise in Perm Krai. The article also provides recommendations of using the method in organizational measures for information security. Moreover, the authors offered the ways of implementation an economic efficiency assessment in the form of a multi-criteria approach.

Keywords: information security efficiency, economic efficiency, models and methods of assessment, multi-criteria assessment, method of paired comparison, information security risk.

Введение. Коммерческие компании в непростой мировой обстановке всё больше подвергаются угрозам безопасности информации. Согласно отчётам компаний Eset и Anti-Malware [1], этот факт обоснован неграмотным построением системы информационной безопасности на предприятии. Ввиду того, что её недостатки можно оценить только в ходе аудита информационной безопасности, возникает проблема достаточности оценки эффективности системы защиты информации (далее – СЗИ), корректное проведение которой даёт предприятию подробные знания о недостатках. С точки зрения бизнеса именно экономический параметр эффективности актуален для возможности

переоценки качества СЗИ. На законодательном уровне и на уровне подзаконных нормативно-правовых актов не определяется, насколько эффективной должна быть система защиты информации. Помимо того действующие решения представлены в виде экспертных методов, зависящих от качества оценивающего, знаний информационной системы, а также умений внедрять алгоритмы информационной безопасности (далее – ИБ). В таком случае трудность задачи качественной оценки экономической эффективности в моделях и методах представляется необходимостью при решении. Подход к моделированию экономической оценки представлен в труде Е.В. Бережной и В.И. Бережного [2], а конкретные методы эффективности были представлены в работе Д.А. Полянского [3]. Кроме того, при моделировании экономической эффективности было принято ссылаться на баесовские модели А. Мотцека [4] и Парето-эффективные модели [5–6]. Эти источники содержат частные подходы, но не предполагают систематизации знаний об оценке эффективности, как и не несут общего подхода к оценке в ходе аудита безопасности. Рассматриваемая проблема актуальна для обширной сферы бизнеса предприятий и организаций в Российской Федерации, а необходимость решения определила тематику работы.

Понятие экономической эффективности СЗИ. Эффективность системы защиты информации – степень соответствия достигнутых результатов поставленным целям по защите информации. Методики расчёта показателя различны и зависят от того, с какой целью и на каком этапе функционирования СЗИ проводится оценка. Оценка эффективности может осуществляться в процессе создания, приемки и эксплуатации СЗИ. Ключевым понятием является критерий оценки – признак, основание принятия решения по оценке эффективности на соответствие предъявленным требованиям. Критериев эффективности системы защиты информации может быть много, однако выбор конкретных зависит от специфики проводимой оценки. На практике выделяют следующие типы критериев оценки эффективности работоспособной СЗИ [7]:

1) критерий «эффект–затраты», позволяющий оценивать достижение СЗИ целей функционирования при заданных затратах;

2) критерии качества СЗИ по определённым показателям, исключая варианты, не удовлетворяющие заданным ограничениям. Используются методы многокритериальной оптимизации (задается одна или несколько целевых функций – таким образом, решается задача оптимизации);

3) искусственные критерии, позволяющие оценивать интегральный эффект («линейная свертка» частных показателей, нечеткие множества).

Всего существует несколько основных подходов к оцениванию эффективности защиты информации, каждый из которых предполагает требования по его обеспечению: опытный, экономический и т.д. В данной работе будет применяться экономический подход с точки зрения задач, связанных с решением проблемы экономического обоснования функционирования СЗИ на предприятии.

Экономическая эффективность системы защиты информации – это эффективность СЗИ, рассчитанная экономическим методом, т.е. затраты на СЗИ должны эффективно обеспечивать функционирование системы в рамках правовых документов и административных регламентов. Или иначе, это мера минимизации риска за счёт функционирования СЗИ [8].

При этом требования, а также применение методов функциональной стандартизации в области ИБ изложены в стандарте ГОСТ ИСО/МЭК 15408-02, а также в ГОСТ Р ИСО/МЭК 27002-2012, в связи с которыми определены метрики оценки эффективности КСЗИ. Исходя из требований заказчика, для оценки подбираются измеряемые критерии и метрики экономической эффективности. В разрабатываемом методе решено придерживаться следующих метрик эффективности [9]:

– показатели риска для защищенной и незащищенной системы;

– показатель экономической эффективности системы защиты информации;

– коэффициент защищенности от актуальных угроз для СЗИ.

Из этих параметров следует, что результатом модели и метода будет являться многокритериальная оценка. Этот факт позволяет взглянуть на функционирование СЗИ под разными ракурсами, произвести комплексную оценку, а также определить корреляцию между критериями. Для проектирования модели оценки экономической эффективности СЗИ будет применяться ситуационный анализ в предметной области экономических параметров информационной безопасности. Достоинство способа – сочетание субъективных оценок экспертов, косвенным образом влияющие на результаты оценки (вычисление весовых коэффициентов), и объективных данных о СЗИ: актуальные угрозы и уязвимости, информационные ресурсы, статистические данные.

Проектирование модели оценки экономической эффективности системы защиты информации. В рамках моделирования применяется следующая семиотическая цепочка (последовательность нескольких параметров системы безопасности), состоящая из 4 взаимосвязанных единиц функционирования СЗИ компании: множество подсистем системы защиты (P_i) – множество требований по защите (T_j) – множество средств защиты (M_k) – задаваемый параметр экономической эффективности системы (E). Эта цепочка и взаимодействие между её звеньями представлена на рис. 1

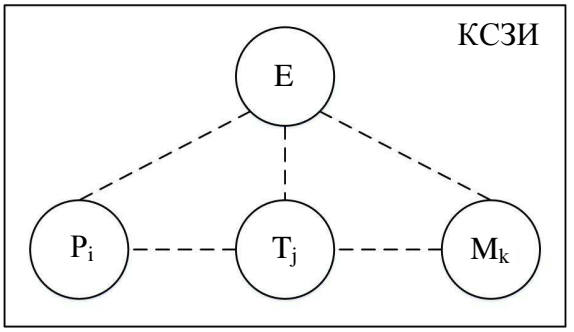

Рис. 1. Цепочка единиц функционирования КСЗИ

С точки зрения моделирования экономической эффективности используется математическая модель (1), представляющая собой сочетание вероятностной и многокритериальной методик оценки. В общем виде она будет выглядеть так:

$$\text{ЭФ}_{\text{СЗИ}} = \frac{\Delta R}{S_{\text{сзи}}}, \quad (1)$$

где ΔR – устраненный риск, $S_{\text{сзи}}$ – стоимость системы защиты информации.

Задача моделирования сводится к нахождению оптимального состава множества подсистем системы защиты (P_i), множества требований по защите (T_j), множества средств защиты (M_k) и параметра экономической эффективности системы защиты информации (E). Образ СЗИ, исходя из условий экономической эффективности, собирается из элементов системы. Модель демонстрирует структурно-функциональную схему СЗИ в совокупности средств защиты, требований и подсистем, из чего видно, будет или не будет обеспечивать она эффективное функционирование.

Весовые коэффициенты P, T, M обозначают лингвистические величины подсистем, требований и средств защиты и определяются

согласно следующим правилам. К примеру, P_3 – подсистема управления информационной безопасностью, T_{11} – требование Приказа ФСТЭК № 17 по аутентификации в системе защиты, M_{42} – система виброакустической защиты «Шторм-2». Коэффициенты модели зависят от среды моделирования и выбора эксперта, основанного на результатах аудита на объекте. Средства защиты информации M выбираются из баз данных средств защиты информации (например, Государственный реестр сертифицированных средств защиты ФСТЭК, другие базы данных) или среди доступных предприятию средств – в случае, когда необходимо провести оценку экономической эффективности СЗИ предприятия. Множество T собирается в модель из требований, распространяющихся на систему защиты нормативно-правовыми или локальными актами по защите информации. Подсистемы защиты информации P определяются в процессе формирования на объекте базы требований T и средств защиты информации M, а также исходя из требований к составу подсистем заказчика оценки или нормативно-правовых актов.

Стоимость $S_{\text{сзи}}$ моделируется средствами защиты информации (далее – СрЗИ), а ΔR формируется, исходя из того, перекрывают ли требования T_j и подсистемы P_i актуальные угрозы и уязвимости. Модель дополняется экспертной или статистической оценкой параметров, представляющих собой субъективную оценку подмножества методом анализа иерархий. Оценка лежит в пределах {1,9}, где 1 означает «элемент не функционирует», 9 – «элемент удовлетворяет параметру эффективности». Так, оценки модели принимают значения, показывающие, достаточно ли эффективен элемент. Модель представляет собой граф множества состояний, в котором отражены элементы, представленные в табл. 1.

Таблица 1

Соответствие модели реальным показателям КСЗИ

Обозначение в модели	Значения диапазона	Интерпретация на КСЗИ
P	$\{P_1, P_2, ..., P_n\}$	Множество подсистем КСЗИ
T	$\{T_1, T_2, ..., T_m\}$	Множество требований по защите
M	$\{M_1, M_2, ..., M_q\}$	Множество средств защиты
E	Функциональный	Параметр экон. эффект-ти
b_{EP}, b_{PT}, b_{TM}	{1;9}	Множество состояния переходов

В качестве интерпретации формальной модели представления СЗИ (рис. 1) была построена модель экономически-эффективного функционирования КСЗИ, представленная на рис. 2.

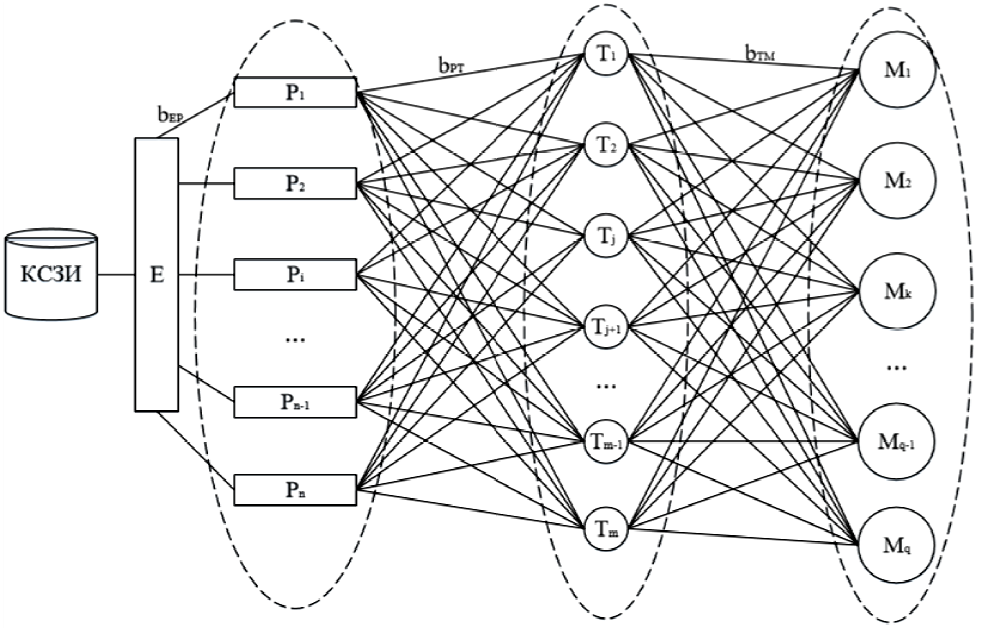

Рис. 2. Модель экономически эффективного функционирования СЗИ

Поскольку модель оперирует лингвистическими величинами, это позволяет проследить связь между исполнением требований с помощью средств защиты информации внутри подсистем защиты. Необходимо обозначить числовое выражение, которое выражает модель. Учитывая, что моделирование экономической эффективности сводится к устранению рисков СЗИ путём поиска оптимальных связей между весовыми коэффициентами, результат моделирования будет представлен коэффициентом защищённости ($K_з$), принимая факт, что произведение требований и подсистем моделируют устранение риска, а произведение СрЗИ моделируют стоимость СЗИ [10]:

$$E = K_з = 1 - \frac{R_з}{R_{НЗ}}, \quad (2)$$

где $R_{НЗ}$ – риск для незащищенной системы, $R_з$ – риск для защищенной системы.

Данный коэффициент показывает, насколько защищена информационная система от рисков ИБ, т.е. перекрывают ли подсистемы системы защиты (P_i) множества требований по защите (T_j) множества

средств защиты (M_k) угрозы и уязвимости. Соответственно, если перекрывают – смоделированная система экономически эффективна и пригодна к эксплуатации. Если этого не происходит ($K_э = 0$) или происходит недостаточно эффективно ($K_э \leq 0{,}5$), то параметры системы в виде СрЗИ и подсистем пересматриваются, пока СЗИ не достигнет достаточной эффективности.

В результате параметры подсистем, требований и экономической эффективности системы задаются в соответствии с нормативными актами, стандартами, условиями функционирования СЗИ компании, а параметры СЗИ необходимо подобрать с учётом актуальных уязвимостей и угроз, а также согласно требованию по эффективности системы.

Разработка метода оценки экономической эффективности СЗИ. На основе предложенной модели создается метод расчёта экономической эффективности СЗИ, основанный на методике парных сравнений. Он представляет собой поэтапное оценивание параметров системы защиты с учётом угроз и уязвимостей ИБ, а также стоимости активов организации и рисков, связанных с возможной реализацией угроз.

Сущность метода сводится к выполнению 9 этапов оценки, каждый из которых представляет тот или иной процесс оценки экономической эффективности. Расчёты в методе производились согласно формулам методики [11], однако процесс оценки был изменен в соответствии с поэтапным оцениванием и переоцениванием результатов моделирования СЗИ (см. рис. 2). Научная новизна по отношению к используемой методике заключается в применении к ней разработанной модели оценки экономической эффективности для формирования первичных данных о СЗИ, а также в возможности переоценки результатов при получении нежелательных исходов в виде неэффективной системы защиты. Таким образом, решается научная задача совершенствования используемых подходов к моделированию оценки экономической эффективности.

Стоит отметить, что метод [11] не позволяет обнаружить связь между общей неэффективностью СЗИ и неэффективностью отдельного её элемента, а также степень его влияния на экономическую эффективность. Применение модели оценки, благодаря первичной оценке с помощью лингвистических параметров, позволяет обнаружить неэффективный элемент на графе экономической эффективности. Кроме того, в подход к оцениванию также заложены механизмы организационного обеспечения информационной безопасности (в виде создания постоянно

действующей системы оценки экономической эффективности, определяющей оценку во время аудита ИБ в строгой организационной форме в несколько этапов), что позволяет рекомендовать метод для использования на реальных объектах защиты информации. Включаемые в метод параметры, с учётом требований по оценке экономической эффективности, представлены на рис. 3.

Рис. 3. Параметры безопасности при оценивании экономической эффективности

Содержание проводимых при оценке экономической эффективности этапов:

Этап 1. Создание комиссии и проведение её оценки. Метод предполагает, что будет проведена вероятностная оценка в сочетании с экспертным оцениванием. Поэтому на первом этапе создается комиссия в составе нескольких человек в зависимости от сложности расчётов и получения данных об объекте информатизации (далее – ОИ). К работе привлекаются специализированные работники сторонних организаций по защите информации, деятели науки в области ИБ, работники кафедр, осуществляющих подготовку студентов по программе «Информационная безопасность», и студенты смежных программ подготовки.

Если эксперт по каким-то условиям не подходит для осуществления оценочной деятельности, то состав комиссии пересматривается с учётом соответствия требованиям. В результате выбора в рамках этапа составляется акт о создании комиссии по оценке.

Этап 2. Получение комиссией исходных данных об объекте и действующей СЗИ. В ходе внутреннего или внешнего аудита эксперты по-

лучают данные об информационной системе (далее – ИС) для оценки активов и рисков. Исходными данными считаются знания об ОИ, подлежащие защите. Эта информация отражает стоимость информационных активов организации, потенциальные угрозы и уязвимости для ОИ, требования законодательства и принятые меры по защите информации.

Этап 3. Формализация полученных данных. В методе будет использоваться шкала относительной значимости для сравнения двух качественных отношений (метод Саати) [12]. Так решается задача анализа иерархий на основе выбора из нескольких критериев. В случае предлагаемого метода критериями выступят уязвимости СЗИ, а также угрозы безопасности информации, которые считаются актуальными для ИС. Поскольку критерии имеют свойство неоднородновсти, то применять их для построения рабочей модели можно в случае выполнения условий:

– преобразование качественных описаний в количественные;
– нормирование количественных описаний с учетом значимости.

Для решения задачи преобразования качественных описаний в количественные строятся таблица парных сравнений оценки уязвимостей и угроз, а также таблица оценки ценности информации. Общий вид таблиц, представляющих собой лингвистическое сравнение двух параметров, показан в табл. 2.

Таблица 2

Парные сравнения двух параметров

Лингвистическая оценка сравнения 1-го и 2-го параметра	Значение
При наличии 1-го 2-й можно не учитывать	9
Существенное превосходство 1-го над 2-й	7
Использование 1-го предпочтительнее, чем 2-го	5
Чуть более высокая значимость 1-го против 2-го	3
Одинаковая значимость сравниваемых параметров	1

Описание множества сравниваемых параметров с использованием шкалы относительной значимости представлено в виде матрицы парных сравнений [11]:

$$M_B^i = \begin{bmatrix} b_{11}^i & \cdots & b_{in}^i \\ \vdots & \ddots & \vdots \\ b_{n1}^i & \cdots & b_{nn}^i \end{bmatrix}, \quad (3)$$

где $B = \{b_1, b_1 \ldots b_n\}$ – множество уязвимостей, $i = \{1,2 \ldots n\}$ – номер эксперта.

Условие относительности означает, что матрица (3) обратносимметрична [13]:

$$b^i_{xy}=\frac{1}{b^i_{yx}}. \tag{4}$$

Каждым экспертом строится матрица парных сравнений уязвимостей на основании табл. 2. Следующим шагом, по ранговой шкале каждый эксперт должен составить вектор доступности уязвимостей для злоумышленника:

$$V=(v^i_1,v^i_2\dots\ v^i_S). \tag{5}$$

Взаимосвязь между угрозами и уязвимостями определяется матрицей причинно-следственных связей, её строит каждый эксперт. Матрица выглядит так:

$$M^i_{\text{УУ}}=\begin{bmatrix} c^i_{11} & \cdots & c^i_{1S} \\ \vdots & \ddots & \vdots \\ c^i_{n1} & \cdots & c^i_{nS} \end{bmatrix}. \tag{6}$$

Этап 4. Расчёт вероятности возникновения угроз. В ходе этапа рассчитываются вероятности возникновения угроз на основании матриц, полученных в предыдущем этапе. Это необходимо для выявления зависимости между существующими уязвимостями и возникающими угрозами. Для текущего этапа перемножаются матрицы относительной значимости уязвимостей и причинно-следственных связей уязвимостей и угроз. Таким образом, получится единственная матрица показателей значимости уязвимостей для возникновения угроз:

$$M^i_{\text{ПЗ}} = M^i_{\text{УУ}}\cdot M^i_{\text{В}}. \tag{7}$$

Далее нужно дополнить матрицу (7) вектором (8) и определить интегральный показатель влияния всех уязвимостей на возникновение *k*-й угрозы:

$$w^i_k=\sum\nolimits_{r=1}^{S} w^i_{kr}\ ,\ i=0,\dots,\ n. \tag{8}$$

Нормализация вектора W проводится так: максимальному значению соответствует величина 9, а минимальному – 1. Далее необходимо получить матрицу отношений элементов:

$$M^i_W=\begin{bmatrix} 1 & \cdots & 1/w^i_{1n} \\ \vdots & \ddots & \vdots \\ w^i_{n1} & \cdots & 1 \end{bmatrix}. \tag{9}$$

Нахождение вероятностей возникновения угроз безопасности по оценкам i-го эксперта P_{bji} сводится к поиску собственных чисел матрицы (9) и собственного вектора P_{bi} – максимальному собственному значению вероятности. Впоследствии производится расчёт ущерба от i-й угрозы незащищенной ИС. Ущерб U_i рассчитывают как относительную величину стоимости ИС – h_i. Степень воздействия i-й угрозы на информационную систему h_i оценивается экспертами при наличии двух условий:

$$0 \le h_i \le 1, \quad \sum_{i=1}^{n} h_i = 1. \tag{10}$$

При этом ущерб от i-й угрозы для незащищенной ИС определяется как [6]:

$$U_i = h_i(S_{\text{и}} + S_{\text{ои}} + S_{\text{сзи}}). \tag{11}$$

Матрица парных сравнений степени вреда, наносимого угрозами, строится экспертами на основе матрицы (6) с учетом (7)–(9) и табл. 2:

$$M_H^i = \begin{bmatrix} h_{11}^i & \cdots & 1/w_{1n}^i \\ \vdots & \ddots & \vdots \\ w_{n1}^i & \cdots & 1 \end{bmatrix}, \tag{12}$$

где $h_{\alpha\beta}^i = (\alpha,\beta = 1,\ldots, n)$ показывает, насколько вред, наносимый α-й угрозой, существеннее вреда, наносимого β-й угрозой.

Этап 5. Определение стоимости информационных ресурсов. Следующим шагом группа экспертов вычисляет ценность информационных ресурсов ОИ методом парных сравнений по формулам (7)–(9) и табл. 2:

$$M_C^i = \begin{bmatrix} 1 & \cdots & 1/C_{k1}^i \\ \vdots & \ddots & \vdots \\ C_{k1}^i & \cdots & 1 \end{bmatrix} \tag{13}$$

и определить вектор относительной ценности:

$$\overline{C}_j = \{C_j^i\},\ i = 0,\ldots, k. \tag{14}$$

Стоимость каждого отдельно взятого информационного ресурса определяется на основе вектора ценности после выделения элемента по формуле:

$$S_{\text{И}i} = \frac{\overline{C}_j}{\overline{C}_0} S_{\text{ИО}}, \tag{15}$$

где $\overline{C}_0$ – относительная ценность ресурса; $S_{\text{ИО}}$ – его стоимость.

Этап 6. Расчёт стоимости объектов, подверженных угрозам. На этом этапе считается стоимость тех объектов, которые являются

уязвимыми для угроз безопасности информации, они непосредственно защищаются СЗИ. Стоимость элементов объекта, подверженных воздействию угроз, определяется их суммированием:

$$S_{\text{ОИ}} = \sum_{j=1}^{m} S_{\text{ОИ}j}, \tag{16}$$

где $S_{\text{ОИ}j}$ – стоимость j-го элемента; m – количество элементов объекта.

Стоимость элементов КСЗИ $S_{\text{СЗИ}}$ определяется как сумма всех затрат на информационную безопасность по всем позициям и считается аналогично формуле (16).

Этап 7. Расчёт вероятности устранения угроз информации. Далее эксперты должны оценить вероятность устранения угроз безопасности. Вероятность устранения j-й угрозы P_{yj} определяется тем, насколько полно учтены качественные и количественные требования к КСЗИ при ее проектировании. Вероятность устранения j-й угрозы по оценкам i-го эксперта определяется из выражения:

$$P_{yj}^{i} = \sum_{q=1}^{l} k_{jq}^{i} \cdot x_{jq}^{i}, \tag{17}$$

где k_{jq}^{i}– весовой коэффициент значимости q-го требования для устранения j-й угрозы по оценке i-го эксперта; x_{jq}^{i} – степень выполнения количественного и качественного требования к СЗИ для устранения j-й угрозы. Весовые коэффициенты проставляются непосредственно экспертами по правилам, установленным *этапом 3*.

Этап 8. Расчёт итоговых показателей экономической эффективности системы защиты информации на объекте информатизации

При работе организации существует определенное количество угроз безопасности ($i = 1, \ldots, n$), которые характеризуются вероятностями возникновения P_{bi} и ущербом, наносимым каждой угрозой U_i. Задачей СЗИ является устранение i-й угрозы. Полный ущерб незащищенному ОИ можно представить как сумму возможных ущербов:

$$U = \sum_{i=1}^{n} P_{bi} U_i. \tag{18}$$

Риск для незащищенного ОИ [14] представляет собой произведение вероятностей возникновения угроз и ущерба в случае их реализации и показывает, какой вероятный ущерб понесёт предприятие при реализации угрозы информационной безопасности в условиях, когда СЗИ на объекте моделируется с неработающими функциями:

$$R_{\text{НЗ}} = \sum_{i=1}^{n} P_{bi} U_i. \tag{19}$$

Риск же для защищенного ОИ зависит от вероятности устранения i-й угрозы P_{yi}:

$$R_з = \sum_{i=1}^{n} P_{bi} U_i (1 - P_{yi}). \quad (20)$$

Чем выше будет вероятность устранения угрозы СЗИ предприятия, тем меньший риск понесет компания в случае реализации угроз. Экономическая эффективность применения системы защиты информации через риски рассчитывается по формуле (1). Через риски выразим коэффициент защищенности ОИ – получим коэффициент экономической эффективности системы защиты информации из формулы (2).

Для расчета экономической эффективности и коэффициента защищенности нужно провести все вышеперечисленные этапы. Система считается тем больше экономически эффективной, чем выше показатель устранения рисков на предприятии за счёт суммарной стоимости системы защиты информации [15]. Если отношение 1:1, то система не перекрывает риски информационной безопасности, об эффективности речь также не идёт, т.е. данная разность должна быть меньше, чем 1.

Этап 9. Принятие решения об экономической эффективности СЗИ. В результате расчётов экспертной группой принимается решение, является ли СЗИ экономически эффективной. Если она эффективна, то принимается решение о её внедрении (модификации) на ОИ, создается проект по внедрению СЗИ на ОИ [16–17]. Если СЗИ признается неэффективной или её эффективность недостаточна для принятия решения о внедрении, то такая СЗИ отправляется на доработку по параметрам, которые в ходе расчёта негативно влияют на общую экономическую эффективность системы.

Апробация модели и метода на объекте защиты. Для проверки работоспособности модели и метода на реальном объекте защиты было выбрано коммерческое предприятие ООО «Компания» (реальное название предприятия не указывается), которое осуществляет свою деятельность на территории Пермского края. Для моделирования эффективной системы защиты информации использовались данные СЗИ на предприятии, а также Государственный реестр сертифицированных средств защиты информации ФСТЭК [18]. Требования к СЗИ предъявлялись, исходя из бизнес-процессов организации (обработка персональных данных, ведение конфиденциальных переговоров, наличие коммерческой тайны). Состав подсистем защиты моделировался, исходя из потребностей организации в защите критичных ресурсов.

Результаты моделирования графической модели (см. рис. 2) были визуализированы в системе Gephi. В результате визуализации на графе были выделены оптимальные пути решения, т.е. наилучшие параметры системы защиты информации в лингвистической форме. Вершины и рёбра в графе, отмеченные красным цветом, обеспечивают максимальную экономическую эффективность, тогда как серые вершины неэффективны. Модель экономически эффективной системы защиты информации на объекте показана на рис. 4.

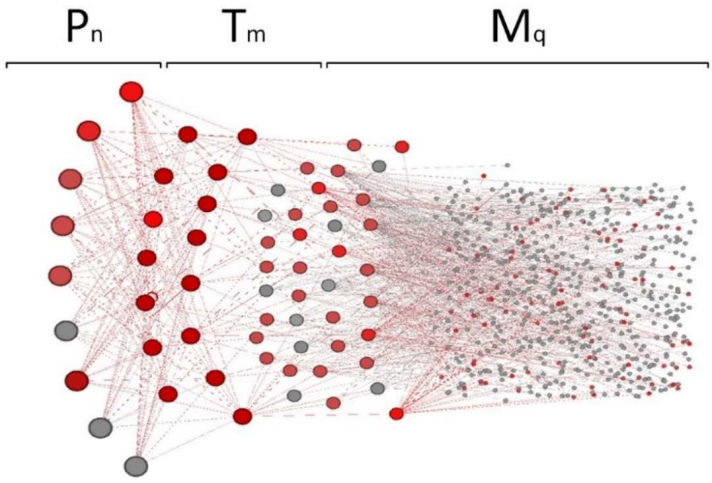

Рис. 4. Визуализация экономически-эффективной СЗИ на объекте защиты

В результате моделирования экономически эффективной СЗИ на объекте защиты были оценены параметры эффективности модели с помощью описанного метода парных сравнений. Полученные показатели оценки экономической эффективности системы защиты информации «Компания» отражены в табл. 3.

Таблица 3

Результаты расчёта итоговых показателей экономической эффективности

Показатель	Значение
Стоимость средств защиты информации, тыс. руб.	174
Риск для незащищенной системы, тыс. руб.	1 809
Риск для защищенной системы, тыс. руб.	648,5
Экономическая эффективность, относительная единица	6,67
Коэффициент защищенности, относительная единица	0,64

Результаты моделирования экономически эффективной СЗИ на объекте, а также оценка этих результатов по методу показали эффективность модели. Показатели составляют 6,67, что означает эффективность работы СЗИ по устранению выявленных рисков ИБ [19]. Содержание СЗИ позволяет снизить стоимость рисков в рублях в 3 раза, при этом обеспечивая отличный коэффициент защищенности ресурсов в 0,64.

Перспективы использования модели и метода оценки экономической эффективности систем защиты информации. В результате проектирования модели и реализующего её оценку метода можно определить не только рекомендации по практическому применению моделей и методов оценки экономической эффективности, но также и сделать вывод по перспективам развития оценки эффективности СЗИ. Результатом проектирования стала модель экономически эффективного функционирования системы защиты информации, с помощью которой можно представить СЗИ предприятия в качестве совокупности подсистем защиты, требований и СрЗИ. Это позволяет увидеть закономерности между действующей системой и её экономической эффективностью, но также приводит СЗИ к формализации для оценки экономической эффективности разработанным методом. Применение метода на реальном объекте продемонстрировало, что модель и метод оценки позволяют провести качественную оценку экономической её эффективности, показывая понятный и конкретный результат. Положительный результат апробации метода позволяет рекомендовать научную работу к применению на действующих объектах защиты информации коммерческих предприятий. Показатели оценки помогут сформировать рекомендации по модернизации СЗИ объекта для увеличения эффективности защиты информации, а также исправить недочёты, уменьшающие эффективность СЗИ.

Кроме того, приведенный случай многокритериальной и комплексной оценки экономической эффективности СЗИ является оптимальным и рекомендуется к применению в модели, отраженной в формулах (1)–(3). Закономерным следствием из рекомендаций являются резюмированные перспективы оценки экономической эффективности в СЗИ. Поскольку оценка в модели и методе осуществляется многокритериально [20], появляется возможность использования новых критериев оценки внутри них, основанных на вероятностных, эко-

номических и оперативных (рисковых) показателях. Это позволит расширить возможности оценки экономической эффективности, включая возможность оценки эффективности через разные показатели.

Библиографический список

1. Анализ рынка ИБ в России. Ч. 1 [Электронный ресурс]. – URL: https://www.anti-malware.ru/analytics/Market_Analysis/analysis-information-security-market-russia-part-1 (дата обращения: 17.10.20).

2. Бережная Е.В. Математические методы моделирования систем. – М.: Финансы и статистика, 2006. – 432 с.

3. Полянский Д.А. Экономика защиты информации. – Владимир: Изд-во ВлГУ, 2009. – 592 с.

4. Motzek A., Möller R. Context- and bias-free probabilistic mission impact assessment // Computers & Security. – 2017. – № 65. – P. 166–186. DOI: https://doi.org/10.1016/j.cose.2016.11.005

5. Selection of Pareto-efficient response plans based on financial and operational assessments / A. Motzek, R. Möller, H. Debar, J. Garcia-Alfaro, G.G. Granadillo // EURASIP Journal on Information Security. – 2017. – № 1. – P. 1–22. DOI: https://doi.org/10.1186/s13635-017-0063-6

6. Aslanyan Z., Nielson F. Pareto Efficient Solutions of Attack-Defence Trees // International Conference on Principles of Security and Trust. – 2015. – P. 95–114. DOI: https://doi.org/10.1007/978-3-662-46666-7_6

7. Маслова Н.А. Методы оценки эффективности систем защиты информационных систем // Искусственный интеллект. – 2008. – № 4. – С. 253–264.

8. Anderson R., Moore T. The Economics of Information Security // Science. – 2006. – № 314. – P. 610–613. DOI: https://doi.org/10.1126/science.1130992

9. Wheeler E. Security Risk Management: Building Information Security Risk Management Program from the Ground Up // Syngress Publishing. – 2011.

10. Economics of Information Security and Privacy III [Электронный ресурс]. – URL: https://ru.scribd.com/document/379404173/Economics-of-Information-Security-and-Privacy-III/ (дата обращения: 15.10.2020).

11. Голиков Ю.А. Экономическая эффективность системы защиты информации. – Новосибирск: СГГА, 2012. – 41 с.

12. Баранова Е.К. Методики анализа и оценки рисков ИБ // Образовательные ресурсы и технологии. – 2015. – № 1(9). – С. 73–79.

13. Цуканова О.А. Экономика защиты информации. – СПб.: Изд-во НИУ ИТМО, 2014. – 79 с.

14. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности // Доступ из справ.-правовой системы КонсультантПлюс.

15. Шлыков А.И., Шабуров А.С. О формализации подходов к разработке моделей многокритериальной оценки эффективности систем защиты информации // Автоматизированные системы управления и информационные технологии: материалы всерос. науч.-техн. конф. (г. Пермь 9–11 июня 2020 г.). – Пермь: Изд-во Перм. нац. исслед. политехн. ун-та, 2020. – Т. 2. – С. 408–414.

16. Положение Гостехкомиссии от 25 ноября 1994 г. по аттестации объектов информатизации по требованиям безопасности информации // Доступ из справ.-правовой системы КонсультантПлюс.

17. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью // Доступ из справ.-правовой системы КонсультантПлюс.

18. Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 [Электронный ресурс]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00 (дата обращения: 22.10.2020).

19. Актуальные киберугрозы – 2019 [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-q1-2019/ (дата обращения: 17.10.20).

20. Шлыков А.И. Разработка модели определения критичных ресурсов и связанных с ними рисков информационной безопасности // Инновационные технологии: теория, инструменты, практика: материалы XI Междунар. интернет-конф. молодых ученых, аспирантов, студентов (15 ноября – 31 декабря 2019 г.). – Пермь: Изд-во Перм. нац. исследов. политехн. ун-та. – 2019. – С. 244–248.

References

1. Analiz rynka IB v Rossii. Chast' 1 [Analysis of the IB market in Russia. Part 1], available at: https://www.anti-malware.ru/analytics/Market_Analysis/analysis-information-security-market-russia-part-1 (accessed 17 October 2020).

2. Berezhnaia E.V. Matematicheskie metody modelirovaniia sistem [Mathematical methods for modeling economic systems]. Moscow: Finansy i statistika, 2006, 432 p.

3. Polianskii D.A. Ekonomika zashchity informatsii [Information security economics]. Vladimir: Vladimirskii gosudarstvennyi universitet, 2009, 592 p.

4. Motzek A., Möller R. Context- and bias-free probabilistic mission impact assessment. *Computers & Security*, 2017, no. 65, pp. 166-186. DOI: https://doi.org/10.1016/j.cose.2016.11.005

5. Motzek A., Möller R., Debar H., Garcia-Alfaro J., Granadillo G.G. Selection of Pareto-efficient response plans based on financial and operational assessments. *EURASIP Journal on Information Security*, 2017, no. 1, pp. 1-22. DOI: https://doi.org/10.1186/s13635-017-0063-6

6. Aslanyan Z., Nielson F. Pareto Efficient Solutions of Attack-Defence Trees. *International Conference on Principles of Security and Trust*, 2015, pp. 95-114. DOI: https://doi.org/10.1007/978-3-662-46666-7_6

7. Maslova N.A. Metody otsenki effektivnosti sistem zashchity informatsionnykh sistem [Methods for assessing the effectiveness of information systems protection systems]. *Iskusstvennyi intellekt*, 2008, no. 4, pp. 253-264.

8. Anderson R., Moore T. The Economics of Information Security. *Science*, 2006, no. 314, pp. 610-613. DOI: https://doi.org/10.1126/science.1130992

9. Wheeler E. Security Risk Management: Building Information Security Risk Management Program from the Ground Up. *Syngress Publishing*, 2011.

10. Economics of Information Security and Privacy III, available at: https://ru.scribd.com/document/379404173/Economics-of-Information-Security-and-Privacy-III/ (accessed 15 October 2020).

11. Golikov Iu.A. Ekonomicheskaia effektivnost' sistemy zashchity informatsii [Economic efficiency of information security systems]. Novosibirsk: Sibirskii gosudarstvennyi universitet geosistem i tekhnologii, 2012, 41 p.

12. Baranova E.K. Metodiki analiza i otsenki riskov IB [Methods of analysis and assessment of information security risks]. *Obrazovatel'nye resursy i tekhnologii*, 2015, no. 1(9), pp. 73-79.

13. Tsukanova O.A. Ekonomika zashchity informatsii [Economics of information security]. Saint Petersburg: Sankt-Peterburgskii natsional'nyi issledovatel'skii universitet informatsionnykh tekhnologii, mekhaniki i optiki, 2014, 79 p.

14. GOST R ISO/MEK 27005-2010. Informatsionnaia tekhnologiia. Metody i sredstva obespecheniia bezopasnosti. Menedzhment riska informatsionnoi bezopasn [GOST R ISO/MEK 27005-2010. Information technology. Security techniques. Information security risk management]. Dostup iz spravochno-pravovoi sistemy Konsul'tantPlius.

15. Shlykov A.I., Shaburov A.S. O formalizatsii podkhodov k razrabotke modelei mnogokriterial'noi otsenki effektivnosti sistem zashchity informatsii [On the formalization of approaches to the development of models of multi-criteria evaluation of the effectiveness of information security systems]. *Avtomatizirovannye sistemy upravleniia i informatsionnye tekhnologii: materialy vserossiiskoi nauchno-tekhnicheskoi konferentsii (Perm 9-11 June 2020)*. Perm': Permskii natsional'nyi issledovatel'skii politekhnicheskii universitet, 2020, vol. 2, pp. 408–414.

16. Polozhenie Gostekhkomissii ot 25 noiabria 1994 goda po attestatsii ob"ektov informatizatsii po trebovaniiam bezopasnosti informatsii [Regulations of Gostekhkomissii dated 25 november 1994 on certification of information objects for information security requirements]. Dostup iz spravochno-pravovoi sistemy Konsul'tantPlius.

17. GOST R ISO/MEK 17799-2005. Informatsionnaia tekhnologiia. Prakticheskie pravila upravleniia informatsionnoi bezopasnost'iu [GOST R ISO/MEK 17799-2005. Information technology. Code of practice for information security management]. Dostup iz spravochno-pravovoi sistemy Konsul'tantPlius.

18. Gosudarstvennyi reestr sertifitsirovannykh sredstv zashchity informatsii N ROSS RU.0001.01BI00 [State register of certified protection equipment N ROSS RU.0001.01BI00], available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00 (accessed 22 October 2020).

19. Aktual'nye kiberugrozy - 2019 [Topical Cyber Threats - 2019], available at: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-q1-2019/ (accessed 17 October 2020).

20. Shlykov A.I. Razrabotka modeli opredeleniia kritichnykh resursov i sviazannykh s nimi riskov informatsionnoi bezopasnosti [Development of a model for determining critical resources and the related risks of information security]. *Innovatsionnye tekhnologii: teoriia, instrumenty, praktika. Materialy XI Mezhdunarodnoi internet-konferentsii molodykh uchenykh, aspirantov, studentov (15 November - 31 December 2019)*. Perm': Permskii natsional'nyi issledovatel'skii politekhnicheskii universitet, 2019, pp. 244-248.

Сведения об авторах

Шабуров Андрей Сергеевич (Пермь, Россия) – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: shans@at.pstu.ru).

Шлыков Алексей Игоревич (Пермь, Россия) – магистрант кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: thekingofthedas@gmail.com).

About the authors

Shaburov Andrey Sergeevich (Perm, Russian Federation) is a Ph. D in Technical Sciences, Associate Professor of the Department of Automation and Telemechanics Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: shans@at.pstu.ru).

Shlykov Alexey Igorevich (Perm, Russian Federation) is a Master Student Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: thekingofthedas@gmail.com).

Получено 07.10.2020