ISSN 2658-5014 (Print) СИИТ ISSN 2686-7044 (Online)
http://siit.ugatu.su 2025. Т. 7, № 5(24)
СИСТЕМНАЯ ИНЖЕНЕРИЯ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
Научная статья

УДК 004.056 DOI: 10.54708/2658-5014-SIIT-2025-no5-p157 EDN: DTYMGZ

О совершенствовании подхода к оценке рисков безопасности информации в контексте обеспечения живучести информационных систем

А. С. Ожгибесова • А. С. Шабуров • А. А. Южаков

Обозначены недостатки традиционных методов оценки рисков информационной безопасности. Приводится анализ методов оценки рисков информационной безопасности, ориентированных на сохранение живучести и кибер-устойчивости информационных систем. Перечислены их особенности, преимущества и недостатки, полученные данные представлены в сравнительной таблице. Предлагается подход по совершенствованию методов оценки рисков, ориентированный на сохранение живучести информационных систем по принципу построения нечетких когнитивных карт. Представлена математическая постановка задачи оценки рисков на основе применения методов нечеткой логики. Приведен пример реализации разработанного метода на примере приложения «Умный дом». Продемонстрирован вариант оценки множественных рисков информационной безопасности на основе нечеткой когнитивной карты. Выведены преимущества разработанного метода оценки рисков безопасности информации в контексте обеспечения живучести информационных систем над существующими

Риск информационной безопасности; защита информации; живучесть информационных систем; нечеткая когнитивная карта.

Введение

В условиях увеличения количества и сложности кибератак оценка рисков безопасности информации (ИБ) становится важнейшим инструментом для защиты данных, инфраструктуры и бизнес-процессов. Традиционные методы оценки рисков ИБ имеют общие недостатки, ограничивающие эффективность их применения [Пле11]. Как правило, реализация традиционных подходов либо требует значительного количества вычислительных ресурсов, либо имеет ограничения по применению (CRAMM, OCTAVE). Кроме того, часть методов являются недостаточно гибкими и сложно адаптируются к применению современных технологий (COBIT for Risk). Другие субъективны, узконаправленны и игнорируют устойчивость и возможность восстановления (FRAP, OCTAVE), акцентируя оценку на сохранении традиционных критериев обеспечения безопасности информации (конфиденциальности, целостности, доступности).

В то же время в современных условиях особое значение приобретает способность информационной системы адаптироваться к новым непредсказуемым условиям функционирования, противостоять неблагоприятным воздействиям и достигать цели за счёт изменения поведения и структуры, таким образом, сохраняя свою устойчивость и живучесть. При этом традиционными аспектами сохранения живучести систем являются:

- проявление данного свойства в нештатных условиях функционирования, при возникновении отказов элементов, неблагоприятных воздействиях и т. п.;

Ожгибесова А. С., Шабуров А. С., Южаков А. А. О совершенствовании подхода к оценке рисков безопасности информации в контексте обеспечения живучести информационных систем // СИИТ. 2025. Т. 7, № 5(24). С. 157-169. DOI: 10.54708/2658-5014-SIIT-2025-no5-p157. EDN: DTYMGZ.

Ozhgibesova A. S., Shaburov A. S., Yuzhakov A. A. “On improving the approach to assessing information security risks in the context of ensuring the survivability of information systems” // SIIT. 2025. Vol. 7, no. 5(24), pp. 157-169. DOI: 10.54708/2658-5014-SIIT-2025-no5-p157. EDN: DTYMGZ (In Russian).

- сохранение наиболее критичных функций системы с возможным понижением качества их выполнения;
- обеспечение механизмов распознавания, противодействия, восстановления, а также специальными средствами адаптации, реконструкции, реконфигурации и реорганизации системы.

Сохранение живучести системы в условиях информационного воздействия обеспечивается следующими основными факторами:

- механизмы распознавания, позволяющие выявлять информационные атаки, успешные вторжения, повышение риска выхода из строя жизненно важных компонентов системы, а также риска потери или искажения информации;
- механизмы противодействия, ориентированные на поддержку заданных условий функционирования и минимизацию потерь при переходе системы в нештатный режим функционирования;
- механизмы восстановления, обеспечивающие восстановление функциональности и работоспособности отдельных компонентов системы и всей системы в целом как в условиях сохранения неблагоприятных воздействий, так и после их прекращения.

Термин «живучесть» для характеристики информационной системы зачастую подразумевает сохранение ее киберустойчивости как способности организации противостоять, адаптироваться и восстанавливаться после кибератак и других киберугроз при условии минимизации ущерба и обеспечения непрерывности бизнес-процессов [Max09].

Совершенствование подходов к оценке рисков информационной безопасности, с учетом сохранения живучести информационных систем, предполагает как анализ уже известных, традиционных подходов, так и разработку новых подходов и методов оценки с учетом современных и высокотехнологичных угроз безопасности информации, а также возможности применения технологий ML, AI и т. п.

1. Анализ традиционных подходов оценки рисков, ориентированных на сохранение живучести ИС

Традиционные подходы, реализованные в методиках оценки рисков ИБ, ориентированные на сохранение живучести ИС, фокусируются на анализе устойчивости систем к воздействиям и ее способности восстанавливаться после инцидентов. Существуют множество методов оценки живучести ИС, рассмотрим несколько наиболее распространенных в данной области:

Survivability Analysis Framework (SAF)

Метод разработан CERT/SEI (Computer Emergency Response Team at the Software Engineering Institute) для военных и космических систем (DARPA, NASA) [Ell10] и предполагает системный подход, анализируя как отдельные уязвимости, так и ИС в целом. Данный метод основан на трех ключевых аспектах живучести:

- сопротивление (resistance) – возможность системы предотвращать атаки и сбои;
- обнаружение (recognition) – способность системы выявлять вторжения, ошибки и аномалии;
- восстановление (recovery) – возможность системы минимизировать ущерб и быстро восстанавливаться после атак и отказов.

SAF реализуется в четыре этапа. Сначала производится идентификация критических для системы бизнес-процессов, затем анализируются потенциальные угрозы и уязвимости системы, затрагивающие критические функции. После оцениваются последствия от нарушения работы этих функций и, наконец, разрабатываются стратегии и планы по повышению живучести системы.

Mission-Oriented Risk and Design Analysis (MORDA)

MORDA – метод, разработанный MITRE Corporation для критической инфраструктуры, который фокусируется на оценке рисков с точки зрения выполнения миссии системы [Buc05]. Предполагает, что угрозы и уязвимости должны анализироваться в контексте их влияния на ключевые задачи системы. В основе идеи лежит отличие от традиционных методов оценки рисков, которые фокусируются на активах (серверах, базах данных, ПО). MORDA анализирует миссию или бизнес-функцию и определяет, какие угрозы могут помешать ее выполнению. Система считается живучей, если она способна продолжать выполнение критически важных задач, даже если она частично скомпрометирована или работает в условиях атаки/сбоя.

MORDA строится на следующих аспектах:

- гарантия выполнения миссии (mission assurance) – оценивается, насколько миссия или бизнес-задача защищена от сбоев и атак;
- принятие решений на основе рисков (risk-based decision making) – риски оцениваются не с точки зрения отдельных активов, а с точки зрения их влияния на миссию;
- компромисс между безопасностью и функциональностью (trade-offs between security and functionality) – повышение безопасности не должно мешать выполнению миссии.

Реализация MORDA начинается с определения миссии и ключевых функций системы – критически важных процессов, без которых миссия не может быть выполнена. За этим следуют анализ подсистем и ресурсов, поддерживающих выполнение миссии, и актуальные угрозы, которые могут помешать их работе. Далее производится расчет влияния угрозы на реализацию миссии по средствам сценарного анализа, метода дерева отказов и оценки последствий.

На основе полученных данных предлагаются конкретные меры, которые не только повышают безопасность, но и не мешают выполнению миссии. Методика фокусируется на выполнении миссии, а не только на технических уязвимостях. Оценивается реальное влияние угроз, а не абстрактных рисков, учитывается баланс между безопасностью и функциональностью.

Resilience-Based Risk Management (RBRM)

Метод разработан университетом Карнеги–Меллона для финансового сектора, основан на концепции живучести системы [Gal21]. В отличие от традиционных подходов к управлению рисками, которые фокусируются на предотвращении угроз, данный метод ориентирован на способность системы адаптироваться, выдерживать и восстанавливаться после сбоев и атак. Этот подход особенно важен для критических инфраструктур финансовых систем, облачных сервисов и военных технологий, где сбои неизбежны, но система должна оставаться работоспособной. RBRM опирается на четыре ключевых компонента живучести:

- подготовка (prepare) – оценка возможных угроз и уязвимостей, разработка резервных планов и сценариев реагирования, обучение персонала для работы в условиях кризиса;
- сопротивление (resist) – реализация механизмов защиты, позволяющих снизить вероятность и влияние атак, использование кибербезопасности, отказоустойчивых архитектур, мониторинга;
- восстановление (recover) – минимизация ущерба и быстрое восстановление после атак или сбоев, использование автоматизированных механизмов восстановления, разработка стратегии "degraded mode" (режим пониженной функциональности, если основная система недоступна);
- адаптация (adapt) – постоянный анализ инцидентов и улучшение защитных мер, автоматизация защиты на основе искусственного интеллекта и машинного обучения.

Первоначально в RBRM выявляются ключевые бизнес-процессы, которые должны продолжать работать при любых условиях, после чего анализируются основные угрозы и риски. Затем проводится оценка устойчивости ИС с использованием стандартных метрик устойчивости (среднее время восстановления, показатель живучести системы, возможность системы работать в урезанном режиме). По итогу разрабатывается стратегия управления рисками,

учитывающая меры защиты, восстановления и адаптации. Оцениваются стоимость внедрения защитных мер и их экономическая целесообразность.

Cyber Resilience Review (CRR)

CRR – это метод оценки киберустойчивости, разработанный Министерством внутренней безопасности США (DHS) совместно с CERT Division of the Software Engineering Institute (SEI) при Carnegie Mellon University [Cyb20]. Реализуется в виде структурированного интервью с ключевыми специалистами компании, такими как ИТ-директора, специалисты по кибербезопасности, менеджеры по непрерывности бизнеса, технические руководители. Процесс занимает 5–6 часов и включает 9 ключевых областей оценки, называемых доменами. По итогам анализа CRR не дается количественная оценка в баллах, а формируется развернутый отчет по каждому домену, представляющийся одним из 5 уровней зрелости киберустойчивости системы:

1. Начальный (initial) – нет формализованных процессов, реагирование хаотично.
2. Повторяющийся (repeatable) – есть базовые процедуры, но они не документированы и зависят от отдельных сотрудников.
3. Определенный (defined) – процессы формализованы, но не всегда соблюдаются.
4. Управляемый (managed) – контролируется выполнение процессов, ведется документация, анализируются инциденты.
5. Оптимизированный (optimized) – киберустойчивость встроена в бизнес-процессы, есть проактивный анализ угроз.

Таким образом, CRR фокусируется не только на технических аспектах безопасности, но и на бизнес-цели. Подходит для компаний любых сфер и отраслей, опирается на лучшие практики NIST, ISO 27001.

Каждая методика имеет свои уникальные особенности, цели и подходы к оценке рисков и устойчивости. Проанализировав информацию о вышеперечисленных методиках, можно выделить наиболее важные критерии анализа, представленные в табл. 1.

Таблица 1

Сравнительные характеристики методов оценки рисков ИБ

Критерий	SAF	MORDA	RBRM	CRR
Основная цель	Оценка способности системы сохранять функциональность при атаках/сбоях	Оптимизация архитектуры под миссию с учетом рисков	Повышение живучести и восстановления	Оценка киберустойчивости по стандартам (NIST)
Область применения	Военные/критические системы	Космос, оборонная инфраструктура	Бизнес-процессы, ИТ-системы	Кибербезопасность (CIKR)
Методология	Анализ сценариев отказа + FTA	Моделирование угроз + стоимостной анализ рисков	Интеграция риск-менеджмента и живучести	Анкетирование + модель зрелости
Ключевые метрики	Вероятность выживания, время восстановления	Риск миссии, вероятность успеха	Индексы живучести	Уровень зрелости
Преимущества	•Высокая точность для сложных технических систем • Выявление «узких мест» в архитектуре • Интеграция с инструментами моделирования	• Четкая экономическая обоснованность решений • Учет человеческого фактора через STPA • Подходит для сложных гетерогенных систем	• Баланс между профилактикой и адаптацией • Подходит для быстро меняющихся угроз • Учитывает организационные аспекты	• Быстрое внедрение • Соответствие NIST CSF • Бесплатные инструменты от CISA

Продолжение табл. 1

Недостатки	• Требует глубоких экспертных знаний • Сложна в адаптации для бизнес-процессов • Длительность расчетов для распределенных систем	•Требует точных данных о стоимости простоев • Сложность в определении вероятностей редких событий	• Субъективность оценок • Требует зрелых процессов управления	• Формальный подход • Не учитывает специфику новых угроз (AI) • Ориентация на формальное соответствие требованиям, а не реальную безопасность
Ресурсоемкость	Высокая	Высокая	Средняя	Низкая
Результаты	• Детализированная модель жизненно важных функций ИС • Перечень критических компонентов, от которых зависит функционирование систем • Стратегия повышения живучести • Анализ возможных сценариев атак и их влияния на ключевые функции	•Анализ соответствия системы целям и задачам миссии •Ранжирование угроз по степени воздействия на миссионные функции • Сценарии, приводящие к срыву миссии •Рекомендации по переосмыслению архитектуры или процессов, если текущие не обеспечивают выполнение миссии в условиях угроз	•Оценка способности системы к устойчивому функционированию и восстановлению •Планы реагирования и восстановления после инцидентов •Индикаторы живучести •Рекомендации по усилению участков, где система не способна быстро восстановиться	•Самооценка зрелости процессов киберустойчивости •Индивидуальный отчет с рекомендациями по повышению живучести •Карта зрелости системы защиты •Список уязвимостей системы в плане процессов

Анализ сравнительных характеристик базовых методов оценки рисков ИБ позволяет сделать следующие выводы:

- SAF подходит для глубокого анализа критических функций системы, но требует значительных затрат ресурсов;
- MORDA ориентирован на системы, где важно выполнение конкретных миссий, но менее применим для систем общего назначения;
- RBRM фокусируется на восстановлении после инцидентов, что делает ее полезной для систем с высокой важностью непрерывности, но требует значительных ресурсов для анализа рисков;
- CRR – простой и доступный инструмент для оценки киберустойчивости, но не обеспечивающий глубокий анализ данных.

Таким образом, необходимость совершенствования подходов к оценке рисков ИБ в настоящее время может быть обусловлена ориентированностью данной оценки на сохранении живучести ИС в условиях риска ИБ путем нахождения оптимального баланса между универсальностью применения, необходимой глубиной анализа, оптимальной ресурсоёмкостью и простотой применения технологий оценки [Ожг24]. При этом оценку целесообразно осуществлять на основе построения современных, риск-ориентированных моделей, например, на основе нечетких когнитивных карт (НКК), что неоднократно подтверждено теорией и практикой [Ожг24].

2. Математическая модель оценки рисков ИБ

Постановка задачи

Для постановки задачи нахождения приемлемого уровня риска ИБ с учетом ориентированности на сохранении живучести ИС рассмотрим параметры для расчета риска и живучести.

В общем случае риск R определяется как средний потенциальный ущерб от реализации возможных угроз информационным активам и описывается факторами:

$A=\{a_1,a_2,\dots a_n\}$ – множество ключевых активов;

$T=\{t_1,t_2,\dots t_p\}$ – множество угроз;

$V=\{v_1,v_2,\dots v_q\}$ – множество уязвимостей;

При этом связь формализуется как:

$$R = \{(a_i, t_j, v_k) | a_i \in A_i, t_j \in T_i, v_k \in V_i\}. \quad (1)$$

В свою очередь живучесть – вероятность того, что после нанесения системе локального повреждения она сохранит свою функциональность, то есть не придет в состояние отказа, или, иначе говоря, она придет в конечное состояние, находящееся в допустимой области (рис. 1).

Определим множество функциональных состояний ИС $S = \{S_1, S_2, \dots, S_m\}$, где каждое состояние s_k характеризует степень работоспособности при частичных отказах ИС.

Разнообразие состояний ИС целесообразно представить набором множеств, как на рис. 1, среди которых F – множество состояний ИС; δ – множество допустимых состояний ИС; НС – начальное состояние системы; N – дестабилизирующее воздействие; КС – конечное состояние системы.

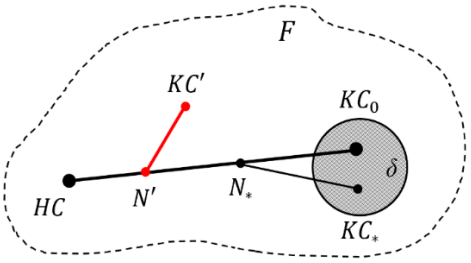

Рис. 1 Интерпретация множества состояний информационной системы

Таким образом, под живучестью системы понимается условная вероятность невыхода конечного состояния системы КС* за границы заданной области допустимых (безопасных) состояний δ пространства F в случае локального повреждения системы N.

Живучесть информационных систем можно описать факторами:

$H = \{h_1,h_2,\dots h_q\}$ – устойчивость элементов ИС (вероятность безотказной работы отдельных узлов);

$D = \{d_1,d_2,\dots d_q\}$ – киберустойчивость (способность противостоять кибератакам без значительной потери функциональности системы);

$Y = \{y_1,y_2,\dots y_q\}$ – восстанавливаемость (способность системы возвращаться к нормальной работе после сбоя);

$G = \{g_1,g_2,\dots g_q\}$ – адаптивность (возможность системы автоматически перестраивать маршруты, перераспределять потоки, балансировать нагрузку).

Общая живучесть ИС L каждого состояния s_k может быть рассчитана как взвешенное сочетание параметров:

$$L(s_k) = \alpha_1 H + \alpha_1 D + \alpha_1 Y + \alpha_1 G, \quad (2)$$

где α_i – весовые коэффициенты важности (сумма равна 1).

Построение НКК

Построение НКК для оценки рисков ИБ предполагает реализовать в виде графа $G = (C,E,W)$, где $C = \{c_1, c_2, \ldots, c_l\}$ – концепты (факторы риска, уязвимости, угрозы, факторы живучести, средства защиты); $E \in C \times C$ – множество направленных связей; $W = \{w_{ij}\}$, $w_{ij} \in [-1; 1]$ – веса влияния концепта c_j на концепт c_i.

Нечеткие значения концептов $A = \{a_1, a_2, \ldots, a_n\}$ задаются в виде чисел в интервале [0, 1] и обновляются по формуле

$$a_i^{(t+1)} = f\left(\sum_{j=1}^{l} w_{ij}\, a_i^{(t)}\right), . \tag{3}$$

где $f(x)$ – функция активации, например,

$$f(x) = \frac{1}{1+e^{-x}}, \text{ или } f(x) = \min(1, \max(0, x)).$$

Для каждого пути P_{ij} между концептами $c_j \rightarrow c_i$ можно вычислить агрегированное влияние с учетом длины пути и затухания:

$$\mathrm{Imp}(c_j, c_i) = \sum_{k=1}^{K} \lambda^k \cdot \prod_{(u,v)\in P_{ij}^{(k)}} w_{uv}, . \tag{4}$$

где $\lambda \in [0, 1]$ – коэффициент затухания; K – максимальная длина пути; $P^{(k)}_{ij}$ – пути длины k между c_j и c_i.

Обычно коэффициент затухания λ и веса влияния одного концепта на другой w_{ij} задаются экспертным методом, однако данный процесс можно автоматизировать с помощью машинного обучения (МО) [Куч24], например, методом обратного распространения ошибки и градиентного спуска, как это представлено в статье [Пал18].

Методы МО необходимо применять для автоматической настройки весов при большом количестве концептов в НКК (> 1000) [Хай25], тогда количество связей растет как n^2, то есть может возрасти до 1 млн. Также для сохранения устойчивости модели необходимо объединять концепты в подсистемы – иерархические кластеры (подсети, домены, службы) и использовать методы стабилизации.

Расчет уровня риска для актива a_i, связанного с угрозой t_j и уязвимостью v_k, определяется как нечеткая функция

$$R_{ijk} = \mu T(t_j) \otimes \mu V(v_k) \otimes \mu C(c_m), \tag{5}$$

где $\mu T(t_j), \mu V(v_k), \mu C(c_m) \in [0,1]$ – степени принадлежности соответствующих концептов; $\otimes$ – нечеткая операция агрегации (например, минимум, произведение или правило Мамдани [Гол18]).

Тогда общий риск для ИС будет определяться, как

$$R_{\text{общ}} = \sum_{(a_i,t_j,v_k)\in R} \beta_{ijk} R_{ijk}, \tag{6}$$

где β_{ijk} – весовая значимость тройки (a_i, t_j, v_k).

Итоговый риск корректируется коэффициентом живучести ИС

$$R_{\text{кор}} = R_{\text{общ}}(1 - L(s_{\text{тек}})), \tag{7}$$

где $L(s_{\text{тек}})$ – живучесть в текущем состоянии системы.

В контексте НКК живучесть – это целевая обратная метрика риска. То есть

$$L(s_k) = 1 - R_{\text{общ}}, \tag{8}$$

но, чтобы учесть влияние внутренних факторов устойчивости (резервирование, отказоустойчивость, адаптивность), необходимо включить L как отдельный концепт в когнитивную карту.

Живучесть обозначим дополнительным концептом C_L, который:

- получает входящие связи с угроз, уязвимостей и активов;
- имеет отрицательные веса от угроз (ослабляет живучесть);

- имеет положительные веса от факторов живучести (резервирование, избыточность, мониторинг, защита).

Пусть вектор концептов $C(t)$ включает живучесть $C_L(t)$:

$$C(t) = [C_1, C_2 \ldots, C_n, C_L]. \quad (9)$$

Динамика НКК описывается уравнением:

$$C(t+1) = f((1-\varphi_L)C(t) + W\,C(t)). \quad (10)$$

Тогда уровень живучести изменяется как

$$C_L(t+1) = f_L((1-\varphi_L)C_L(t) + \sum_{i=1}^{n} W_{i,L}\,C_i(t)), \quad (11)$$

где $W_{i,L}$ – вес влияния концепта i на живучесть; $f_L(x)$ – функция активации, нормирующая в [0,1]; φ_L – коэффициент инерции живучести (0.1–0.5 для адаптивных систем, 0.7–0.9 для инертных).

Живучесть затем корректирует итоговый риск

$$R_{\text{кор}} = R_{\text{общ}}(1 - C_L). \quad (12)$$

Таким образом, при высокой живучести ($C_L \to 1$) риск снижается, а при низкой ($C_L \to 0$) увеличивается.

Разработанная математическая модель оценки рисков ИБ, ориентированная на сохранение живучести ИС, позволяет произвести численную оценку требуемых параметров как для наступления одной рисковой ситуации, так и для случая одновременного их наступления.

3. Пример реализации метода

Для наглядности рассмотрим реализацию метода на примере информационной системы «Умный дом».

Система реализована в жилом доме с четырьмя подъездами по 40 квартир. В инфраструктуре задействовано более 2400 датчиков, включая около 500 беспроводных в одном подъезде (рассматриваемый фрагмент), причем некоторые из них работают на автономных источниках питания. На каждом этаже размещаются по два конвертера, подключённых к проводной IP-сети (Gigabit Ethernet), через которые агрегированные данные от беспроводных датчиков передаются в сеть.

Информационная система «Умный дом» обеспечивает:

- учёт ресурсов ЖКХ (электроэнергии, воды, тепла, газа);
- охранно-пожарную сигнализацию (датчики дыма, движения, открытия дверей);
- контроль микроклимата (температура, влажность, вентиляция, кондиционирование);
- взаимодействие с пользователем (микрофоны, камеры, ИК/радио-ретрансляторы, динамики).

Основные типы трафика: телеметрия от сенсоров, голосовой и видеотрафик, мультимедиа-потоки. Реализация метода предполагает этапы:

1) Определение нескольких основных активов, угроз и уязвимостей, а также факторов киберустойчивости для системы «Умный дом».

Активы (A):

- система учета энергии;
- система охранной сигнализации;
- система контроля микроклимата;
- сетевое оборудование;
- видеонаблюдение.

Уязвимости (V):

- отсутствие шифрования передачи данных;
- слабые пароли доступа;
- устаревшее ПО;
- отсутствие резервного копирования.

Угрозы (T):

- несанкционированный доступ;
- утечка конфиденциальных данных;
- повреждение конфигурации сети;
- отказ центрального модуля.

Факторы киберустойчивости (D):

- многофакторная аутентификация;
- шифрование данных;
- резервные каналы связи;
- SIEM система.

2) Построение НКК, для которой в качестве концептов используются ранее определенные активы, уязвимости, угрозы и факторы киберустойчивости. При этом целевыми концептами будут являться значение «общего риска» R и живучесть в текущем состоянии системы $L(s_{тек})$.

Матрица весов влияния между концептами (НКК) представлена в табл. 2.

Таблица 2

Матрица весов НКК

От / к	V1	V2	V3	V4	T1	T2	T3	T4	R	L
A1	+0.25	0	0	0	0	0	0	0	0	+0.05
A2	0	+0.20	0	0	+0.40	0	0	0	0	+0.08
A3	0	0	0	0	0	0	0	+0.30	0	0
A4	0	0	+0.30	0	0	0	+0.60	0	0	0
A5	0	0	0	0	0	+0.35	0	0	0	0
V1	0	0	0	0	+0.50	+0.70	+0.20	+0.10	+0.30	0
V2	0	0	0	0	+0.90	+0.30	+0.25		+0.25	0
V3	0	0	0	0	+0.25	0	+0.60	+0.50	+0.20	0
V4	0	0	0	0	0	+0.25	0	+0.70	+0.15	0
T1	0	0	0	0	0	0	0	0	+0.60	0
T2	0	0	0	0	0	0	0	0	+0.70	0
T3	0	0	0	0	0	0	0	0	+0.60	0
T4	0	0	0	0	0	0	0	0	+0.80	0
D1	0	0	0	0	-0.80	0	0	0	0	+0.25
D2	0	0	0	0	0	-0.90	0	0	0	+0.30
D3	0	0	0	0	0	0	0	-0.60	0	+0.20
D4	0	0	0	0	-0.50	-0.30	-0.40	0	0	+0.25

Разработанная НКК представлена на рис. 2.

3) Произведя расчет НКК, получаем значения $R_{общ} \approx 0.730$ – в текущей конфигурации уязвимости и угрозы дают заметный вклад в риск, $L(s_{тек}) = 0.500$ – система обладает только средней способностью сохранять/восстанавливать функции.

Итоговый риск корректируется коэффициентом живучести ИС:

$$R_{кор} = R_{общ} \cdot \left(1 - L(s_{тек})\right) = 0.730 \cdot (1 - 0.500) \approx 0.365.$$

Выводы:

- итоговый совокупный риск нарушения безопасности для системы «Умный дом» составляет 0.365 (средний риск);

- коэффициент живучесть системы оценивается на уровне 0.500, что соответствует допустимому уровню киберустойчивости, однако требует усиления защиты в зонах, связанных с НСД и отказами центрального модуля;
- система способна частично компенсировать угрозы, поэтому с учетом ее живучести итоговый риск снижается до 0.365.

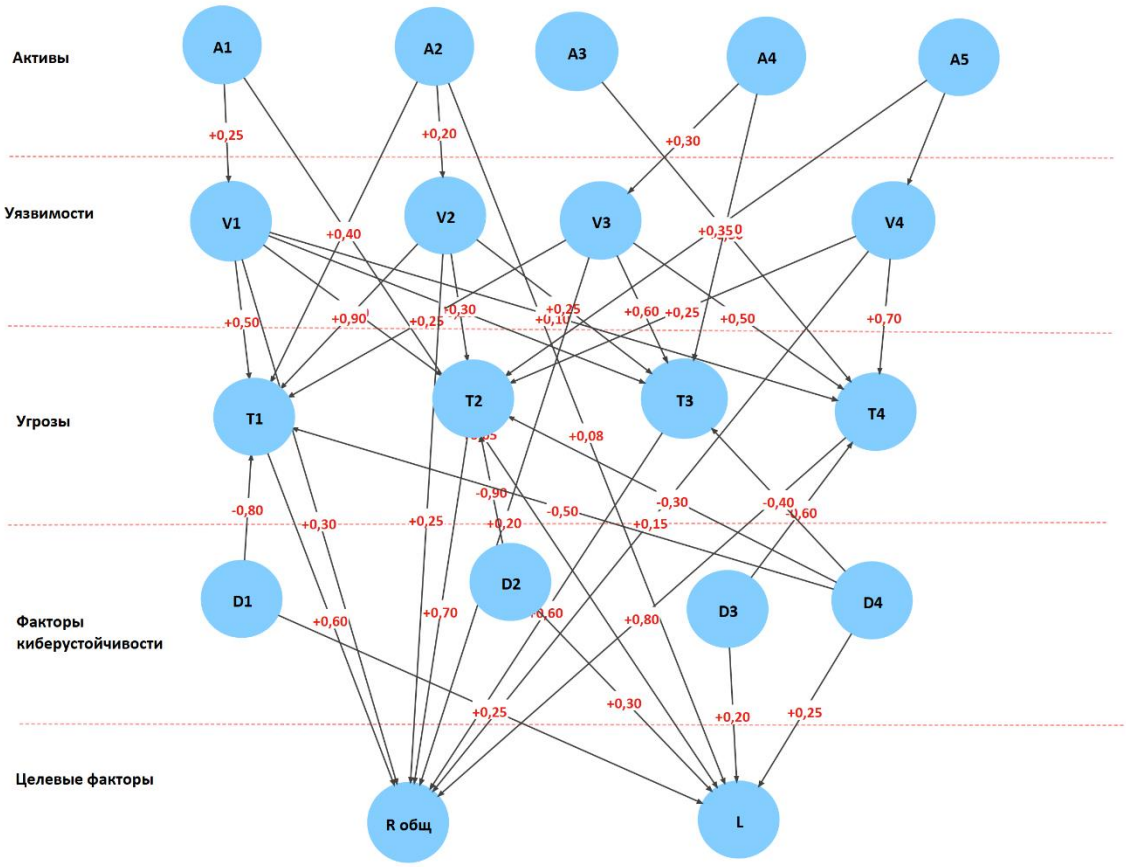

Рис. 2 НКК для системы типа «Умный дом»

4) Для учета множественных рисков можно рассмотреть несколько комбинаций одновременного наступления рисков в системе «Умный дом», используя НКК и подход к моделированию множественных сценариев. При этом можно определить количество всех возможных комбинаций одновременного наступления рисков с использованием числа сочетаний без наступления повторений рисковых ситуаций:

$$C(n,k) = \frac{n!}{k!(n-k)!}, \tag{8}$$

где n – количество рисков; k – количество одновременно наступающих рисков.

Для приведенного примера существует всего 15 уникальных комбинаций одновременного наступления рисковых ситуаций (от 1 до 4) при учете условия, что каждый риск рассматривается как независимое событие. При переходе на оценку множественных рисков отбрасываются сценарии с одиночными рисками, так как этот вариант уже рассмотрен в ранее построенной НКК. Тогда в соответствии с ранее принятыми ограничениями получается 10 сценариев для наступления от 2 до 3 одновременно проявляющихся угроз безопасности. При этом из всех оставшихся сценариев наиболее опасными будут считаться сценарии с наибольшим полученным значением общего риска.

Рассмотрим несколько вариантов комбинаций множественного и одновременного наступления рисков от 2 до 3 угроз информационной безопасности (табл. 3).

Таблица 3

Сценарии наступления множественных рисков

№	Концепты	Общий риск	Живучесть	Риск с корректировкой
S1	T1, T2	0.650	0.477	0.340
S2	T2, T3	0.650	0.477	0.340
S3	T1, T3, T4	0.667	0.470	0.353
S4	T2, T3, T4	0.700	0.459	0.379

Анализ различных комбинаций угроз также удобно визуализировать с помощью НКК путем отбрасывания незадействованных концептов.

Выводы

Анализ уязвимостей системы при различных комбинациях рисков позволяет выбрать приоритетные области для усиления защиты и предложить рекомендации по снижению рисков. Предложенный метод оценки рисков ИБ в контексте живучести ИС обладает рядом преимуществ относительно существующих методов:

- гибкость подхода обуславливается использованием НКК, так как существует возможность ее адаптации для различных по назначению информационных систем с дополнением необходимого количества концептов, позволяющих учесть особенности конкретной системы;
- использование нечеткой логики, позволяющее произвести оценку рисков информационной безопасности даже в условиях неопределенности и неточности данных;
- рассмотрение всех возможных комбинаций одновременного наступления множественных рисков, что дает наиболее полную и подробную оценку поведения системы при реализации подобных сценариев;
- определение наиболее разрушительных сценариев для информационной системы при реализации множественных угроз ИБ, что позволяет осуществить разработку плана по снижению рисков;
- возможность автоматизации построения и расчета параметров НКК, позволяющая значительно ускорить процесс оценки рисков ИБ [Bac14].

Таким образом, научная новизна исследования заключается в следующем:

1. На основе анализа существующих методов оценки рисков ИБ предложены метод и новая модель автоматизированной оценки рисков ИБ с учетом ориентированности данной оценки на сохранении живучести ИС.
2. Разработан метод количественной оценки рисков ИБ на основе моделирования сценариев атак в контексте сохранения живучести ИС с использованием технологии построения НКК и методов машинного обучения.

Заключение

Совершенствование подходов к оценке рисков ИБ предполагает поиск новых, более гибких подходов к оценке рисков, ориентированных на противодействии современным киберугрозам, а также позволяющим автоматизировать процессы управления рисками ИБ в режиме «реального времени». Кроме того, для отдельных типов объектов при невозможности исключить риски ИБ предполагается получение их оценки с учетом сохранения живучести объекта даже в условиях реализации стратегии принятия рисков ИБ. Сохранение живучести ИС в условиях риска может достигаться путем нахождения оптимального баланса между универсальностью применения, необходимой глубиной анализа, оптимальной ресурсоёмкостью и простотой применения технологий оценки. Разработка новых математических подходов оценки рисков позволит находить резервы информационных систем даже в условиях множественных информационных воздействий и кибернетических атак.

СПИСОК ЛИТЕРАТУРЫ | REFERENCES

[Buc05] Buckshaw D. L., Parnell G. S. et al. Mission Oriented Risk and Design Analysis of Critical Information Systems // Military Operat. Research. 2005. V. 10, Iss. 10 (2). P. 19-38.

Buckshaw D. L., Parnell G. S. et al. “Mission Oriented Risk and Design Analysis of Critical Information Systems” // Military Operat. Research. 2005. V. 10, Iss. 10(2). P. 19-38.

[Cyb20] Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide, cisa.gov, apr., 2020. URL: www.cisa.gov/sites/default/files/publications/2_CRR%25204.0_Self-Assessment_User_Guide_April_2020.pdf.

Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide, cisa.gov, apr., 2020. URL: www.cisa.gov/sites/default/files/publications/2_CRR%25204.0_Self-Assessment_User_Guide_April_2020.pdf.

[Ell10] Ellison R., Woody C. Survivability Analysis Framework. // Carnegie Mellon University, Software Engineering Institute's Digital Library. Software Engineering Institute, Technical Note CMU/SEI-2010-TN-013, 1-Jun-2010. DOI: 10.1184/R1/6584474.v1.

Ellison R., Woody C. "Survivability Analysis Framework," Carnegie Mellon University, Soft-ware Engineering Institute's Digital Library. Software Engineering Institute, Technical Note CMU/SEI-2010-TN-013, 1-Jun-2010. DOI: 10.1184/R1/6584474.v1.

[Gal21] Galderisi A., Altay-Kaya A. A New Framework for a Resilience-Based Disaster Risk Management // Eslamian, S., Eslamian, F. (eds) Handbook of Disaster Risk Reduction for Resilience. Springer, Cham. 2021. 15. DOI: 10.1007/978-3-030-61278-8_6.

Galderisi A., Altay-Kaya A. “A New Framework for a Resilience-Based Disaster Risk Management” // Eslamian, S., Eslamian, F. (eds) Handbook of Disaster Risk Reduction for Resilience. Springer, Cham. 15, 2021, 2021. DOI: 10.1007/978-3-030-61278-8_6.

[Вас14] Васильев В. И., Кудрявцева Р. Т., Юдинцев В. А. Автоматизация процесса оценки информационных рисков с использованием нечетких когнитивных карт // Вестник УГАТУ. 2014. Т. 18, № 3 (64). С. 253–260. EDN: REMWKM.

Vasiliev V.I., Kudryavtseva R.T., Yudintsev V.A. Automation of the process of assessing information risks using fuzzy cognitive maps // Vestnik UGATU. 2014. Vol. 18, No. 3 (64). P. 253-260. EDN AQLGLE. (In Russian). EDN: REMWKM.

[Гол18] Голосовский М. С., Богомолов А. В., Теребов Д. С., Евтушенко Е. В. Алгоритм настройки системы нечёткого логического вывода типа Мамдани // Вестник ЮУрГУ. Серия: Математика. Механика. Физика. 2018. № 3. DOI: 10.14529/mmph180303. EDN: UTSRWO.

Golosovsky M. S., Bogomolov A. V., Terebov D. S., Evtushenko E. V. Algorithm for setting up a Mamdani-type fuzzy logical inference system // Bulletin of SUSU. Series: Mathematics. Mechanics. Physics. 2018. No. 3. (In Russian). DOI: 10.14529/mmph180303. EDN: UTSRWO.

[Куч24] Кучкарова Н. В. Оценка актуальных угроз и уязвимостей объектов критической информационной инфраструктуры с использованием технологий интеллектуального анализа текстов // СИИТ. 2024. Т. 6, № 2(17). С. 50–65. DOI: 10.54708/2658-5014-SIIT-2024-no2-p50. EDN: NLDWBE.

Kuchkarova N.V. Assessment of current threats and vulnerabilities of critical information infrastructure objects using text mining technologies // SIIT. 2024. Vol. 6, No. 2(17). P. 50-65. (In Russian). DOI: 10.54708/2658-5014-SIIT-2024-no2-p50. EDN: NLDWBE.

[Мах09] Махутов Н. А., Петров В. П., Резников Д. О. Оценка живучести сложных технических систем // Проблемы безопасности и чрезвычайных ситуаций. 2009. № 3. С. 47–66. EDN: MEGOYJ.

Makhutov N.A., Petrov V.P., Reznikov D.O. Assessment of survivability of com-plex technical systems // Problems of safety and emergencies. 2009. No. 3. P. 47–66. (In Russian). EDN: MEGOYJ.

[Ожг24] Ожгибесова А. С., Шабуров А. С., Южаков А. А. Об оценке рисков информационной безопасности на основе применения нечетких когнитивных карт в интеллектуальных транспортных системах управления дорожным движением // Вестник УрФО. 2024. № 2(52). С. 56–67. DOI: 10.14529/secur240206. EDN: OYVETG.

Ozhgibesova A. S., Shaburov A. S., Yuzhakov A. A. On the level of information security risk based on the use of fuzzy cognitive maps in intelligent methods of integrated traffic management // Bulletin of the Ural Federal District. - 2024. No. 2 (52). P. 56-67. EDN AQLGLE. (In Russian). DOI: 10.14529/secur240206. EDN: OYVETG.

[Пал18] Палютина Г. Н. О применении нейронных сетей для оценки весов связей между концептами нечеткой когнитивной карты в адаптивной оценке рисков информационной безопасности // Вестник УрФО. 2023. № 4(50). С. 60–69. DOI: 10.14529/secur230406. EDN: OVSDNY.

Palyutina G.N. On the use of neural networks for assessing the weights of connections between concepts of a fuzzy cognitive map in adaptive assessment of information security risks // Bulletin of the Ural Federal District. 2023. No. 4 (50). P. 60-69. (In Russian). DOI: 10.14529/secur230406. EDN: OVSDNY.

[Пле11] Плетнёв П. В., Белов В. М. Сравнительный анализ существующих методов определения рисков информационной безопасности // Ползуновский вестник. 2011. № 3–1. EDN: OHFZML.

Pletnev P. V., Belov V. M. Comparative analysis of existing methods for determining information security risks // Polzunovsky Vestnik. 2011. No. 3-1. (In Russian). OHFZML.

[Хай25] Хайруллин Э. Р. и др. Нейросетевая система обнаружения сетевых атак // СИИТ. 2025. Т. 7, № 1 (20). С. 105–112. DOI: 10.54708/2658-5014-SIIT-2025-no1-p105. EDN: GVIQLO.

Khairullin E. R. et al. Neural network system for detecting network attacks // SIIT. 2025. Vol. 7, No. 1(20). P. 105-112. (In Russian). DOI: 10.54708/2658-5014-SIIT-2025-no1-p105. EDN: GVIQLO.

[Шам24] Шамсутдинов Р. Р. и др. Интеллектуальная система мониторинга информационной безопасности промышленного интернета вещей с использованием механизмов искусственных иммунных систем // СИИТ. 2024. Т. 6, № 4 (19). С. 14–31. DOI: 10.54708/2658-5014-SIIT-2024-no4-p14. EDN: LTXBSG.

Shamsutdinov R. R. et al. Intelligent system for monitoring information security of the Industrial Internet of Things using mechanisms of artificial immune systems // SIIT. 2024. Vol. 6, No. 4(19). P. 14-31. (In Russian). DOI: 10.54708/2658-5014-SIIT-2024-no4-p14. EDN: LTXBSG.

ОБ АВТОРАХ | ABOUT THE AUTHORS

ОЖГИБЕСОВА Анна Сергеевна
Пермский национальный исследовательский политехнический университет, Россия.
aozgibesova@pstu.ru.
Аспирантка каф. автоматики и телемеханики. Готовит дис. в обл. управления информационной безопасностью, автоматизации процесса оценки рисков. Магистр по информационной безопасности (Пермск. нац. иссл. политехн. ун-т, 2023).

ШАБУРОВ Андрей Сергеевич
Пермский национальный исследовательский политехнический университет, Россия.
shans@at.pstu.ru.
Доц. каф. автоматики и телемеханики. Дипл. (ПВВКИКУ РВ, 1993, проф. переподготовка: «информационная безопасность», РТУ МИРЭА, 2020). Канд. техн. наук (Пермск. военн. ин-т ракетных войск, 2001). Иссл. в обл. информ. безоп. информационно-управляющих систем.

ЮЖАКОВ Александр Анатольевич
Пермский национальный исследовательский политехнический университет, Россия.
uz@at.pstu.ru ORCID: 0000-0003-1865-2448.
Зав. каф. автоматики и телемеханики. Проф., д-р техн. наук по информационным измерительным системам (Пермск. гос. техн. ин-т, 1997) Иссл. в области информационно-измерительных, управляющих систем и устройств на основе нейронной технологии, распознавание образов.

OZHGIBESOVA Anna Sergeevna
Perm National Research Polytechnic University,
Russia.
aozgibesova@pstu.ru.
Postgraduate student of the Department of Automation and Telemechanics. Preparing a dissertation in the field of information security management, automation of the risk assessment process. Master of Information Security (Perm National Research Polytechnic University, 2023).

SHABUROV Andrey Sergeevich
Perm National Research Polytechnic University,
Russia.
shans@at.pstu.ru.
Assoc. Prof., Department of Automation and Telemechanics. Dipl. (PVVKIKU RV, 1993, professional retraining: Information Security, RTU MIREA, 2020). Cand. of Technical Sciences (Perm Military Institute of Missile Forces, 2001). Research in the field of information security of information and control systems.

YUZHAKOV Alexander Anatolyevich
Perm National Research Polytechnic University,
Russia.
uz@at.pstu.ru ORCID: 0000-0003-1865-2448.
Head of the Department of Automation and Telemechanics. Professor, Doctor of Technical Sciences in Information Measur-ing Systems (Perm State Technical Institute, 1997). Research in the field of information-measuring, control systems and devices based on neural technology that recognize patterns.

МЕТАДАННЫЕ | METADATA

Заглавие: О совершенствовании подхода к оценке рисков безопасности информации в контексте обеспечения живучести информационных систем.

Авторы: Ожгибесова А. С., Шабуров А. С., Южаков А. А.

Аннотация: Обозначены недостатки традиционных методов оценки рисков информационной безопасности. Приводится анализ методов оценки рисков информационной безопасности, ориентированных на сохранение живучести и киберустойчивости информационных систем. Перечислены их особенности, преимущества и недостатки, полученные данные представлены в сравнительной таблице. Предлагается подход по совершенствованию методов оценки рисков, ориентированный на сохранение живучести информационных систем по принципу построения нечетких когнитивных карт. Представлена математическая постановка задачи оценки рисков на основе применения методов нечеткой логики. Приведен пример реализации разработанного метода на примере приложения «Умный дом». Продемонстрирован вариант оценки множественных рисков информационной безопасности на основе нечеткой когнитивной карты. Выведены преимущества разработанного метода оценки рисков безопасности информации в контексте обеспечения живучести информационных систем над существующими.

Ключевые слова: Риск информационной безопасности; защита информации; живучесть информационных систем; нечеткая когнитивная карта.

Язык: Русский.

Статья поступила в редакцию 18 июля 2025 г.

Title: On improving the approach to assessing information security risks in the context of ensuring the survivability of information systems.

Authors: Ozhgibesova A. S., Shaburov A. S., Yuzhakov A. A.

Abstract: The article outlines the shortcomings of traditional methods for assessing information security risks. It provides an analysis of methods for assessing information security risks aimed at maintaining the survivability and cyberstability of information systems. Their features, advantages and disadvantages are listed, and the obtained data are presented in a comparative table. An approach is proposed to improve the risk assessment methods aimed at maintaining the survivability of information systems based on the principle of constructing fuzzy cognitive maps. A mathematical formulation of the risk assessment problem based on the application of fuzzy logic methods is presented. An example of implementing the developed method is given using the example of the Smart Home application. A variant of assessing multiple information security risks based on a fuzzy cognitive map is demonstrated. The advantages of the developed method for assessing information security risks in the context of ensuring the survivability of information systems over existing ones are derived.

Key words: Information security risk; information protection; survivability of information systems; fuzzy cognitive map.

Language: Russian.

The article was received by the editors on 18 July 2025.