УДК 004.056.5
DOI: 10.26102/2310-6018/2026.57.6.015

Оценка киберживучести информационной системы «Умный дом» на основе применения нечетких когнитивных карт

А.С. Ожгибесова

Пермский национальный исследовательский политехнический университет, Пермь, Российская Федерация

Резюме. В статье рассматривается задача оценки киберживучести информационной системы «Умный дом», функционирующей в условиях роста числа киберугроз и уязвимостей устройств интернета вещей. Целью исследования является оценка метода анализа устойчивости таких систем на основе применения нечетких когнитивных карт. Предлагаемый подход позволяет моделировать причинно-следственные связи между компонентами системы, включая сетевую инфраструктуру, интеллектуальные устройства, факторы безопасности и внешние киберугрозы. В рамках работы сформирована когнитивная модель информационной системы, включающая ключевые элементы архитектуры, определены причинно-следственные зависимости между факторами, влияющими на уровень киберживучести системы, и сформирована матрица весов для последующего вычислительного моделирования. На основе разработанной модели проведен экспериментальный анализ сценария кибератаки, связанной с компрометацией сетевой инфраструктуры. Результаты моделирования демонстрируют влияние кибератак на уровень киберживучести системы и позволяют количественно оценить воздействие различных факторов безопасности на функционирование системы. Также показана динамика восстановления системы после устранения последствий атаки. Предложенный метод позволяет учитывать неопределенность и взаимосвязь факторов безопасности, обеспечивая наглядное представление структуры угроз и их влияния на систему. Полученные результаты подтверждают возможность применения нечетких когнитивных карт для оценки киберживучести и повышения устойчивости информационных систем «Умный дом».

Ключевые слова: риск информационной безопасности, киберживучесть информационных систем, система «Умный дом», кибератака, нечеткое моделирование.

Для цитирования: Ожгибесова А.С. Оценка киберживучести информационной системы «Умный дом» на основе применения нечетких когнитивных карт. *Моделирование, оптимизация и информационные технологии.* 2026;14(6). URL: https://moitvivt.ru/ru/journal/article?id=2330
DOI: 10.26102/2310-6018/2026.57.6.015

Assessment of cyber survivability of the Smart Home information system based on the use of fuzzy cognitive maps

A.S. Ozhgibesova

Perm National Research Polytechnic University, Perm, the Russian Federation

Abstract. The article considers the task of assessing the cyber-survivability of a Smart Home information system operating in the context of an increasing number of cyber threats and vulnerabilities of Internet of Things devices. The aim of the study is to develop a method for analyzing the stability of such systems based on the use of fuzzy cognitive maps. The proposed approach makes it possible to model causal relationships between system components, including network infrastructure, intelligent devices, security factors, and external cyber threats. As part of the work, a cognitive model of the information system was formed, including key elements of the architecture, the causal relationships between the factors influencing the level of cyber survivability of the system were determined, and a matrix of weights was formed for subsequent computational modeling. Based on the developed model, an experimental

analysis of the cyberattack scenario related to the compromise of the network infrastructure was carried out. The simulation results demonstrate the impact of cyber-attacks on the level of cyber survivability of the system and allow us to quantify the impact of various security factors on the functioning of the system. The dynamics of system recovery after the elimination of the consequences of the attack is also shown. The proposed method allows to take into account the uncertainty and interrelation of security factors, providing a visual representation of the structure of threats and their impact on the system. The results obtained confirm the possibility of using fuzzy cognitive maps to assess cyber survivability and increase the stability of Smart Home information systems.

Keywords: information security risk, cyber survivability of information systems, Smart Home system, cyberattack, fuzzy modeling.

For citation: Ozhgibesova A.S. Assessment of cyber survivability of the Smart Home information system based on the use of fuzzy cognitive maps. *Modeling, Optimization and Information Technology.* 2026;14(6). (In Russ.). URL: https://moitvivt.ru/ru/journal/article?id=2330 DOI: 10.26102/2310-6018/2026.57.6.015

Введение

Интеллектуальные жилые системы или «Умные дома» – это сложные распределенные информационные системы, которые объединяют различные устройства Интернета вещей, сетевую инфраструктуру и облачные сервисы. С их широким внедрением увеличивается и число угроз информационной безопасности, такие как несанкционированный доступ, компрометация данных и отказ в обслуживании [1]. Кибератаки на такие системы могут привести не только к потере конфиденциальной информации, но и к реальным физическим последствиям, включая угрозы здоровью и жизни людей. В связи с этим обеспечение живучести является критическим аспектом проектирования и эксплуатации этих систем. Существующие методы оценки рисков, такие как ISO/IEC 27005, демонстрируют ограниченную эффективность при рассмотрении сложных взаимосвязей между компонентами системы и динамикой современных угроз [2].

В контексте современного развития информационных систем, в частности, среды Интернета вещей, полное предотвращение угроз информационной безопасности становится невыполнимой задачей. Это приводит к смене парадигмы с оценки вероятности угроз на оценку способности системы поддерживать функциональность в свете их возникновения. Традиционное определение «живучесть» подразумевает свойство системы сохранять способность выполнять свои основные функции под воздействием неблагоприятных факторов (отказов, внешних воздействий, чрезвычайных ситуаций) и восстанавливать работоспособность после их устранения. Однако в отношении информационных систем в контексте киберугроз используется технический термин «киберживучесть» (КЖ). КЖ определяется как способность информационной системы противостоять кибератакам, поддерживать критически важные функции в условиях киберинцидентов и восстанавливать функциональность после их реализации [3]. В отличие от традиционных моделей оценки рисков, КЖ учитывает динамическое поведение системы и влияние защитных механизмов. Это позволяет более адекватно охарактеризовать уровень безопасности системы и является необходимым дополнением к классическим методам оценки рисков информационной безопасности (РИБ) [4].

Таким образом, возникает настоятельная потребность в разработке новых методов, способных моделировать поведение системы с учетом множества взаимосвязанных динамических факторов, объединяющих оценку РИБ и живучести информационных систем. Целью данного исследования является оценка разработанной модели и метода автоматизированной оценки КЖ информационных систем, основанных на нечетких когнитивных картах [5].

Материалы и методы

Разработанный авторский метод основан на использовании нечетких когнитивных карт (НКК), представляющих систему в виде ориентированного графа [6]:

$$\text{НКК} = (C, W), \quad (1)$$

где $C = \{C_1, C_2, \ldots, C_n\}$ – множество концептов (факторов системы); $W = [w_{ij}]$ – матрица весов причинно-следственных связей со значениями $w_{ij} \in [1,1]$, которые отражают степень влияния C_i на C_j.

Состояние системы в момент времени описывается выражением:

$$A(t) = [a_1(t), a_2(t), \ldots, a_n(t)], \quad (2)$$

где $a_i(t) \in [0,1]$ – уровень активации концепта C_i.

Например, уровень угроз, эффективность мониторинга, доступность сервиса и скорость восстановления.

Эволюция системы описывается итерационным уравнением:

$$A(t+1) = f(A(t) \cdot W), \quad (3)$$

где W – матрица весов; $f(x)$ – функция активации.

Часто используется сигмоидальная функция:

$$f(x) = \frac{1}{1+e^{-\lambda x1}}, \quad (4)$$

обеспечивающая ограничение значений в диапазоне [0,1].

Факторы модели можно разделить на три группы:

1) Факторы угроз:

$$T = \{T_1, T_2, \ldots, T_k\}, \quad (5)$$

такие, как интенсивность атак, количество уязвимостей, сложность атак.

2) Факторы защиты:

$$S = \{S_1, S_2, \ldots, S_m\}, \quad (6)$$

например, эффективность обнаружения атак, эффективность обнаружения атак, уровень мониторинга.

3) Факторы функционирования системы:

$$F = \{F_1, F_2, \ldots, F_p\}, \quad (7)$$

то есть доступность сервисов, целостность данных, время восстановления.

Интегральный показатель КЖ (Cyber Resilience):

$$CR = C_r, \quad (8)$$

где C_r – концепт «киберустойчивость».

Либо можно задать агрегированную метрику:

$$CR = \alpha A + \beta I + \gamma R, \quad (9)$$

где A – доступность системы; I – целостность данных; R – способность к восстановлению; α, β, γ – весовые коэффициенты.

Матрица W может формироваться:

1) Экспертным методом по формуле:

$$w_{ij} = \frac{1}{k} \sum_{e=1}^{k} w_{ij}^{(e)}, \quad (10)$$

где k – число экспертов.

2) Методами обучения, такими как генетические алгоритмы или градиентное обучение [7].

Разработанный алгоритм оценки КЖ состоит из следующих пунктов:

1) формирование множества концептов;
2) построение матрицы влияния W;
3) инициализация вектора состояния $A(0)$;
4) итерационный расчет состояния системы;
5) вычисление показателя КЖ CR.

По результатам моделирования можно провести анализ влияния атак на систему устойчивости архитектуры, эффективности защитных мер и определить критические факторы системы. Завершающий этап включает анализ полученных результатов, в том числе проведение чувствительного анализа по весам, моделирование различных сценариев атак и оценку влияния факторов КЖ.

Результаты

Внедрение разработанного метода было выполнено на примере системы «Умный дом», реализованной в г. Перми компанией ООО «ЮНИКОРН».

Система «Умный дом» – это технологичный комплекс бытовых подсистем, функционирующих на базе IT-решений как тип систем автоматизации, а также класс систем в зависимости от уровня цифровой зрелости [8]. Основное целевое назначение внедрения подобных систем, автоматизированное поддержание комфортного и безопасного микроклимата в помещении через удаленное управление сервисами. В основе архитектуры лежат компьютерные технологии и системы телеметрии, объединяющие различные устройства в единую сеть для централизованного контроля. Текущий функционал системы включает более ста задач, среди которых приоритетными являются:

- управление энергоресурсами и водопотреблением;
- мониторинг аварийных систем жилья;
- комплексное повышение удобства и безопасности быта.

Реализация перечисленных сценариев становится возможной благодаря внутренней и внешней коммуникационной инфраструктуре, обеспечивающей стабильный обмен данными между всеми элементами системы. Архитектура такой системы, как правило, состоит из центрального управляющего узла (шлюза умного дома), сетевой инфраструктуры и набора интеллектуальных устройств и представлена на Рисунке 1.

Функционирование системы основано на постоянном обмене данными между устройствами через локальную сеть и облачные сервисы. Это обеспечивает автоматизацию различных сценариев, например, управление освещением, климатом и системами безопасности.

Каналы передачи данных для большинства устройств включают протокол Wi-Fi с подключением напрямую к домашней сети, для расширенных систем с датчиками используется энергоэффективный протокол ZigBee. Управление может происходить голосом с помощью умной колонки, вручную физическим нажатием на клавиши выключателей и сенсорных панелей или средствами мобильного приложения.

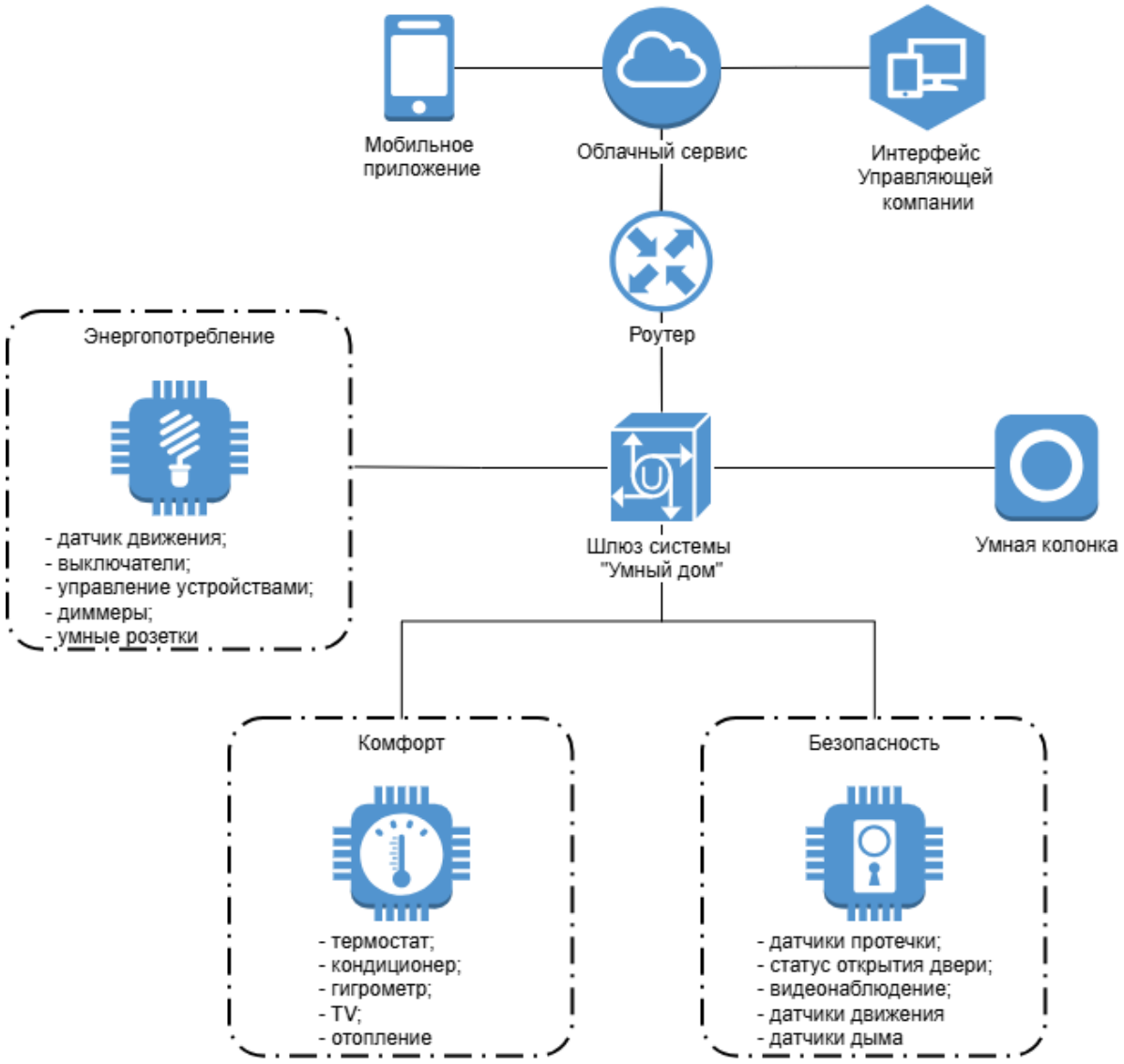

Рисунок 1 – Инфраструктура жилого помещения
Figure 1 – Residential infrastructure

В качестве объекта оценки выбран жилой квартал «SMART City» – высокотехнологичный комплекс домов переменной этажности с подземным паркингом и закрытой дворовой территорией в Индустриальном районе г. Перми по адресу ул. Стахановская, дом 52А. Комплекс состоит из трех домов переменной этажности (9, 16 и 25 этажей), 3 подъездов и 331 квартиры. В доме представлены студии, 1-, 2- и 3-комнатные квартиры площадью 31–73 м².

Всего в системе используется более 7200 датчиков, на каждом этаже расположены 2 конвертера для шлюзования с проводной IP-сетью дома (Gigabit Ethernet). В рамках настоящего исследования рассмотрен фрагмент описанной инфраструктуры, ограниченной двухкомнатной квартирой. Общее количество беспроводных датчиков в рассматриваемом фрагменте сети составляет около 30 штук (Рисунок 2).

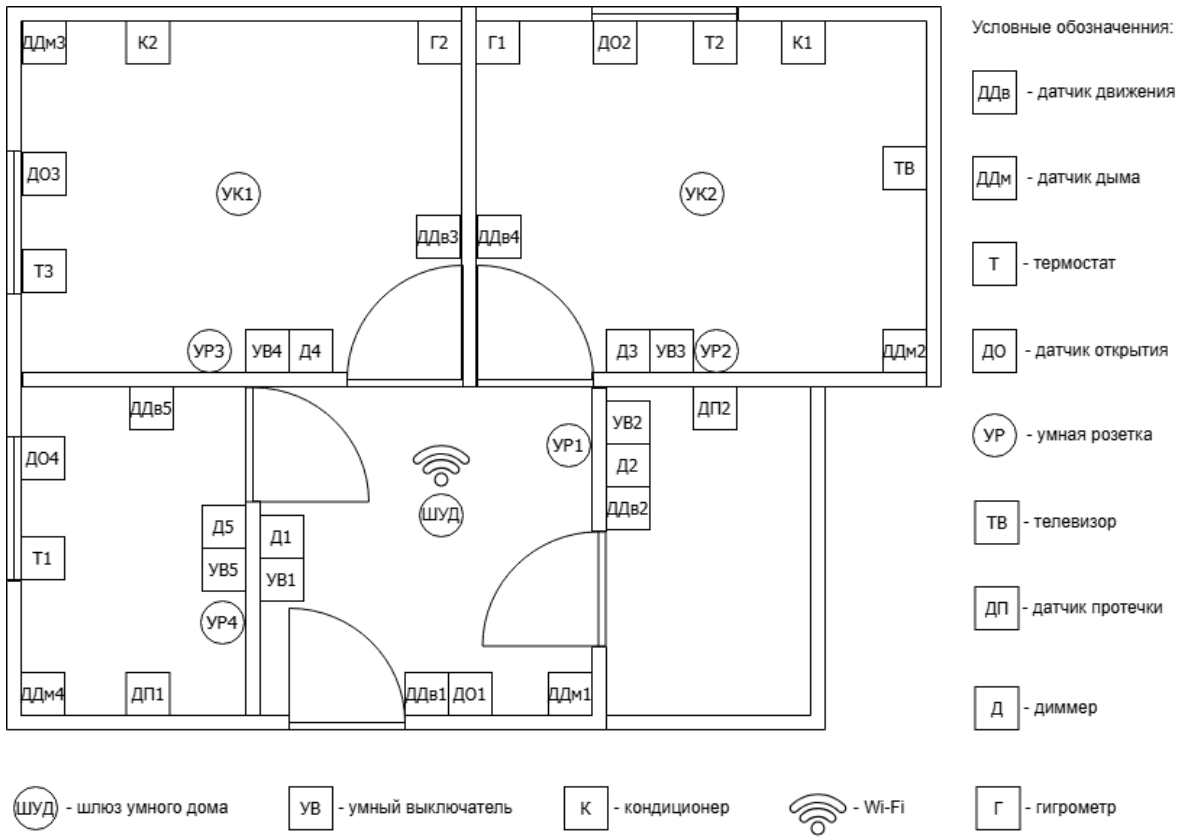

Рисунок 2 – Расположение устройств в жилом помещении
Figure 2 – Device location in the residential apartment

Оценку живучести будем проводить на примере указанного выше объекта – двухкомнатной квартиры. Расчеты производятся средствами специализированного программного обеспечения[1].

Оценка КЖ методом на основе НКК. В качестве концептов НКК были выбраны факторы, обозначенные в Таблице 1. Значения начальных состояний задаются экспертным методом.

Таблица 1 – Описание концептов НКК
Table 1 – Description of the FCM concepts

Группа факторов	Концепт	Фактор	Начальное состояние
Сетевые компоненты	C1	Wi-Fi роутер	0,9
	C2	шлюз умного дома	0,8
	C3	мобильное приложение	0,7
	C4	мобильное устройство с удаленным доступом	0,6
IoT-устройства	C5	умная колонка	0,7
	C6	датчики движения	0,8
	C7	датчики открытия дверей и окон	0,8
	C8	датчики протечки	0,8
	C9	датчики дыма	0,8

[1] Ожгибесова А.С., Южаков А.А., Шабуров А.С. Программа оценки рисков информационной безопасности и живучести информационных систем на основе нечетких когнитивных карт «Когнитивная модель управления рисками и живучестью». Свидетельство о государственной регистрации программ для ЭВМ №2026618681 Российская Федерация: заявл. 27.03.2026; опубл. 27.03.2026.

Таблица 1 (продолжение)
Table 1 (continued)

Исполнительные устройства	C10	диммеры	0,7
	C11	умные розетки	0,8
	C12	система кондиционирования	0,7
Факторы безопасности	C13	уровень сетевых атак	0,3
	C14	уязвимости IoT-устройств	0,4
	C15	компрометация устройств	0,2
	C16	безопасность IoT-сети	0,8
Факторы функционирования	C17	доступность системы	0,9
	C18	целостность данных	0,8
	C19	способность восстановления	0,7
Целевой фактор	C20	уровень КЖ	0,8

После определения концептов и их начальных значений строится НКК, представленная на Рисунке 3.

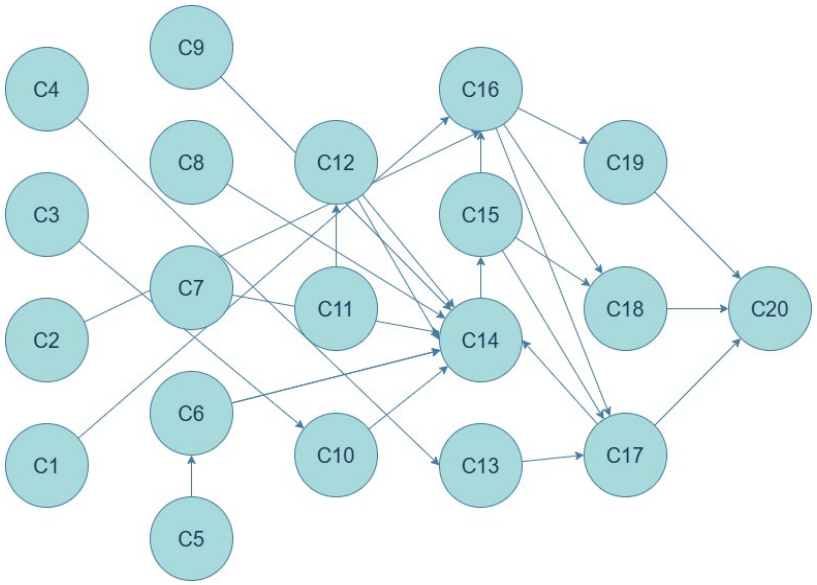

Рисунок 3 – Граф НКК
Figure 3 – FCM graph

Веса связей НКК, определенные экспертным методом, представлены в Таблице 2.

Таблица 2 – Веса связи НКК
Table 2 – FCM connection weights

№	Причина (концепт C_i)	Следствие (концепт C_j)	Вес	№	Причина (концепт C_i)	Следствие (концепт C_j)	Вес
1	C1	C16	+0,7	13	C13	C14	+0,7
2	C2	C16	+0,8	14	C14	C15	+0,6
3	C3	C14	+0,5	15	C14	C15	+0,8
4	C4	C13	+0,6	16	C15	C16	−0,7
5	C5	C14	+0,3	17	C15	C17	−0,6
6	C6	C14	+0,2	18	C15	C18	−0,6
7	C7	C14	+0,2	19	C16	C17	+0,6
8	C8	C14	+0,2	20	C16	C18	+0,5
9	C9	C14	+0,2	21	C16	C19	+0,5

Таблица 2 (продолжение)
Table 2 (continued)

10	C10	C14	+0,2	22	C17	C20	+0,9
11	C11	C14	+0,2	23	C18	C20	+0,8
12	C12	C14	+0,2	24	C19	C20	+0,7

Расчетные значения критических концептов приведены в Таблице 3.

Таблица 3 – Итоговые значения факторов
Table 3 – Summary values of the factors

Концепт	**Фактор**	**Итоговое значение (с учетом нормирования)**
C13	уровень сетевых атак	0,3
C14	уязвимости IoT-устройств	0,71
C15	компрометация устройств	0,75
C16	безопасность IoT-сети	0,75
C17	доступность системы	0,90
C18	целостность данных	0,78
C19	способность восстановления	1
C20	уровень КЖ	**0,71**

Система показывает уровень КЖ выше среднего, основной риск создают уязвимости IoT устройств, компрометация устройств сильно влияет на доступность, защита Wi-Fi сети и шлюза повышает устойчивость.

Для проверки адекватности модели была проведена оценка корреляции между наблюдаемыми значениями КЖ, полученными от экспериментов на тестовом стенде, развернутом на базе ООО «ЮНИКОРН» и результатами моделирования на основе НКК для 10 вариантов квартир по формуле:

$$r = \frac{\sum(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum(x_i - \bar{x})^2 \sum(y_i - \bar{y})}}, \quad (10)$$

где x_i – наблюдаемые значения; y_i – значение модели.

Полученные значения представлены в Таблице 4.

Таблица 4 – Киберживучесть различных вариантов квартир
Table 4 – Cyber survivability of various apartment options

	Наблюдаемые значения	**Модель НКК**
Квартира 1	0,91	0,90
Квартира 2	0,87	0,85
Квартира 3	0,79	0,80
Квартира 4	0,83	0,82
Квартира 5	0,76	0,75
Квартира 6	0,88	0,89
Квартира 7	0,81	0,82
Квартира 8	0,84	0,83
Квартира 9	0,89	0,87
Квартира 10	0,85	0,88

Расчет коэффициента Пирсона показал значение r=0,97 при уровне значимости p<0,01, что свидетельствует о высокой степени согласованности модели с

наблюдаемыми данными. Таким образом, модель на основе НКК очень хорошо воспроизводит реальные значения КЖ, что говорит об ее адекватности.

Моделирование сценариев атак. Реализуем кибератаки на инфраструктуру сети жилого помещения для оценки изменения уровня КЖ. Атаки имитируются путем добавления концептов в НКК, а также задания причинно-следственных связей и их весов.

Расчет значений КЖ после реализации кибератак и их ранжирование по степени влияния на систему представлен в Таблице 5.

Таблица 5 – Влияние атак на киберживучесть жилого помещения
Table 5 – The impact of cyber attacks on residential survivability

Концепт	Сценарий атаки	Основные последствия	Вес связи	КЖ
C21	Атака на шлюз умного дома	потеря координации устройств	−0,90	0,43
C22	Атака на IoT-устройства (ботнет)	заражение датчиков	−0,55	0,45
C23	Компрометация Wi-Fi роутера	перехват трафика, распространение атаки на устройства	−0,80	0,49
C24	DDoS-атака на сеть	перегрузка канала связи	−0,76	0,51
C25	Взлом мобильного приложения	удалённое управление системой	−0,65	0,56
C21+C23+ +C25	Шлюз + Wi-Fi + мобильное приложение	потеря централизованного управления устройствами	–	0,41
C21+C23+ +C22+C24	Шлюз + Wi-Fi + +IoT-устройства + DDoS	отказ сетевой инфраструктуры	–	0,36
C21–C25	Одновременная реализация атак	риск здоровью и жизни людей	–	0,33

По результатам моделирования видно, что наиболее критическими узлами системы являются шлюз умного дома, IoT-устройства и Wi-Fi роутер, компрометация этих устройств вызывает каскадное распространение угроз на остальные компоненты системы. При одновременном наступлении рассматриваемых кибератак уровень КЖ падает до критически низкого значения 0,33. По сравнению с нормальным режимом функционирования наблюдается снижение на 54 %.

Моделирование динамики системы показало, что при снижении уровня КЖ до 0,33 восстановление системы происходит в течение 7–8 итераций обновления модели НКК, после чего показатель стабилизируется на уровне 0,71, соответствующем нормальному функционированию системы.

Применение мер по обеспечению информационной безопасности и повторная реализация КА. Для восстановления и/или повышения уровня КЖ введем необходимые меры защиты в граф НКК и зададим их веса влияния на целевой концепт (Таблица 6).

Таблица 6 – Влияние мер на киберживучесть жилого помещения
Table 6 – The impact of protective measures on the cyber survivability of residential premises

№	Фактор	Вес влияния	КЖ
C26	Сегментация Wi-Fi сети	0,18	0,50
C27	Шифрование сетевого трафика	0,16	0,49
C28	Регулярные обновления IoT устройств	0,14	0,48
C29	Система аутентификации пользователей	0,09	0,46
C30	Мониторинг сетевой активности	0,08	0,45

В рамках рассматриваемого объекта сегментацию Wi-Fi-сети предлагается произвести путем размещения датчиков, умных розеток и исполнительных устройств в отдельный IoT-сегмент, не имеющий прямого доступа к пользовательским устройствам и внешним сетевым устройствам. Такая архитектура позволяет локализовать распространение атаки и снизить вероятность компрометации всей инфраструктуры при заражении отдельного устройства.

По возможности шифрование сетевого трафика обеспечивается современными протоколами защищенной передачи данных, включая WPA3 для Wi-Fi-сети, TLS для обмена данными мобильным приложением и шлюзом умного дома, а также VPN-туннель для удаленного доступа пользователей. В случае, если устройства не поддерживают встроенное шифрование, предлагается реализовать защищенное взаимодействие на уровне шлюза умного дома путем настройки маршрутизации и дополнительного шифрования передаваемого трафика.

Многофакторная аутентификация пользователей для входа в мобильное приложение по средствам пароля и дополнительного подтверждения, например, через СМС, а также регистрация IoT-устройств через шлюз умного дома и использование уникальных идентификаторов, ключей доступа или сертификатов позволит ограничить подключение неавторизованных устройств к системе и снизить риск подмены компонентов инфраструктуры.

Мониторинг сетевой активности – непрерывный анализ состояния сети и поведения устройств, направленный на обнаружение аномальной сетевой активности, резкого увеличения трафика, повторяющихся попыток авторизации и нетипичного поведения IoT-устройств. При выявлении подозрительной активности система может инициировать автоматическую изоляцию устройства, ограничение сетевого взаимодействия или уведомление пользователя о возможной атаке.

Таким образом, формируется многоуровневая система обеспечения безопасности.

После добавления в НКК концептов защитных мер снова проведем КА, чтобы отследить динамику КЖ.

Таблица 7 – Сравнение уровня киберживучести при различных сценариях атак
Table 7 – Comparison of cyber survivability levels under different attack scenarios

Сценарий атаки	КЖ до введения МЗ	КЖ после введения МЗ
Атака на шлюз умного дома	0,58	0,66
Компрометация Wi-Fi роутера	0,55	0,64
Взлом мобильного приложения	0,60	0,68
DDoS-атака на сеть	0,57	0,65
Атака на IoT-устройства (ботнет)	0,59	0,67
Шлюз + Wi-Fi + мобильное приложение	0,41	0,54
Шлюз + Wi-Fi + IoT-устройства + DDoS	0,36	0,50
Одновременная реализация атак	0,33	0,47

Введенные МЗ в совокупности снижают влияние атак примерно на 35 %, что приводит к повышению КЖ на 42 % даже при реализации сложных сценариев кибератак (Таблица 7). Результаты моделирования показывают, что внедрение комплекса защитных мер позволяет существенно повысить уровень КЖ системы. Даже при реализации пяти одновременных атак уровень устойчивости системы увеличивается с низкого 0,33 до среднего 0,47, что подтверждает эффективность предложенного подхода и возможность его применения для оценки защищенности IoT-инфраструктур.

Благодаря введению факторов защиты увеличивается значение фактора C19 – способность восстановления. Система восстанавливается с уровня 0,47 до устойчивого

значения 0,71 в течение 6–7 итераций обновления НКК, что свидетельствует о достаточно высокой скорости восстановления системы.

Обсуждение

Для оценки живучести традиционно используются Байесовские сети (БС) и Марковские цепи (МЦ) [9, 10]. Проведем оценку КЖ с помощью этих методов по сценарию, описанному выше, и сравним полученные значения с методом на основе НКК и реальными данными (РД), полученными от экспериментов на тестовом стенде, развернутом на базе ООО «ЮНИКОРН».

Произведем расчет показателя средней абсолютной ошибки (MAE) по формуле:

$$MAE = \frac{1}{n}\sum_{i=1}^{n}|CR_{real} - CR_{model}|, \quad (11)$$

где CR_{real} – реальный уровень КЖ системы; CR_{model} – значения, полученные при моделировании; n – число экспериментальных сценариев.

Реальные данные, полученные со стенда, примем за идеал, то есть средняя ошибка равна нулю, а точность оценки берем за единицу.

Сравним прогнозируемые моделями значения КЖ после реализации атак с реальными данными (Таблицы 8, 9).

Таблица 8 – Сравнение методов по точности оценки КЖ после реализации кибератак
Table 8 – Comparison of methods for assessing cyber survivability after cyber attacks

	Реальные данные	**Байесовские сети**		**Марковские цепи**		**Нечеткие когнитивные карты**	
Название атаки	Значение	Прогноз	Ошибка	Прогноз	Ошибка	Прогноз	Ошибка
Атака на Wi-Fi роутер	0,50	0,61	0,11	0,56	0,06	0,48	0,02
Атака ботнета на IoT устройства	0,45	0,58	0,13	0,52	0,07	0,46	0,01
Компрометация мобильного приложения	0,55	0,67	0,12	0,61	0,06	0,51	0,09
DDoS атака сети	0,52	0,63	0,11	0,58	0,06	0,54	0,02
Атака на шлюз умного дома	0,44	0,57	0,13	0,50	0,06	0,45	0,01
Средняя ошибка ~	0	**0,10**		**0,05**		**0,02**	
Точность оценки ~	1	**0,90**		**0,95**		**0,98**	

Таблица 9 – Сравнение методов по точности оценки
Table 9 – Comparison of methods by estimation accuracy

	РД	**БС**		**МЦ**		**НКК**	
КЖ в различных условиях	Значение	Прогноз	Ошибка	Прогноз	Ошибка	Прогноз	Ошибка
Базовая КЖ	0,74	0,83	0,11	0,81	0,07	0,71	0,03
КЖ до внедрения ЗМ	0,30	0,40	0,10	0,36	0,06	0,33	0,03
КЖ после введения ЗМ	0,45	0,57	0,12	0,52	0,07	0,47	0,02
Средняя ошибка ~	0	**0,11**		**0,07**		**0,03**	
Точность оценки ~	1	**0,89**		**0,93**		**0,97**	

Базовая КЖ – это исходный уровень КЖ системы, характеризующий её способность функционировать в штатном режиме при отсутствии кибератак и дополнительных защитных воздействий.

КЖ до внедрения защитных мер – это уровень КЖ системы в условиях реализации кибератак при отсутствии или недостаточности механизмов защиты, отражающий степень уязвимости системы к внешним угрозам.

КЖ после внедрения защитных мер – это уровень КЖ системы при реализации кибератак с учетом функционирования защитных механизмов, характеризующий способность системы противостоять атакам, сохранять работоспособность и восстанавливаться после нарушений.

Рассчитаем итоговые значения ошибки прогнозов моделей и их точность оценки (Таблица 10).

Таблица 10 – Итоговые значения ошибок и точности методов
Table 10 – Final values of errors and accuracy of methods

БС		**МЦ**		**НКК**	
Ошибка	Точность	Ошибка	Точность	Ошибка	Точность
0,11	0,89	0,06	0,94	0,03	0,97

Таким образом, при использовании метода на основе НКК КЖ системы увеличивается на 42 %, в то время как Байесовские сети повышают ее на 32 % (меньше НКК на 29 %), а Марковские цепи на 30 % (меньше НКК на 24 %). В то же время точность оценки КЖ повышается до 8,2 % в сравнении с Байесовскими сетями и на 3,1 % по сравнению с цепями Маркова.

Заключение

Предлагаемый подход имеет преимущества количественно измерять КЖ систем «Умного дома» и анализировать влияние факторов безопасности на их функционирование. Адекватность оценки киберустойчивости по средствам разработанной НКК подтверждается результатами проведенных экспериментов. Практическая ценность этого метода заключается в повышении уровня КЖ к кибератакам и сбоям за счет определения наиболее уязвимых компонентов. Кроме того, метод позволяет моделировать различные сценарии кибератак и оценивать их влияние на ключевые показатели системы. Благодаря этому появляется возможность прогнозирования поведения системы при реализации угроз и РИБ, определения оптимальных стратегий реагирования и восстановления. Исследование показало превосходство метода, основанного на НКК, над моделями, использующими цепи Маркова и Байесовские сети, и продемонстрировало более точную оценку КЖ, а также более адекватное отражение снижения КЖ и восстановления системы.

Возможность масштабируемости модели, основанной на НКК, позволит в дальнейшем оценивать киберустойчивость не только отдельного помещения, но и более сложных инфраструктур Интернета вещей, сохранив при этом целостность причинно-следственных связей.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Вольвач А.В., Поддубная Н.С. Уязвимости системы «Умный дом». *Вестник Пермского университета. Математика. Механика. Информатика.* 2021;(1):49–52. https://doi.org/10.17072/1993-0550-2021-1-49-52

Volvach A.V., Poddubnaya N.S. Vulnerabilities in Smart Home system. *Bulletin of Perm University. Mathematics. Mechanics. Computer Science.* 2021;(1):49–52. (In Russ.). https://doi.org/10.17072/1993-0550-2021-1-49-52

2. Аникин И.В. Методы и алгоритмы количественной оценки и управления рисками безопасности в корпоративных информационных сетях на основе нечеткой логики. *Системная инженерия и информационные технологии.* 2023;5(3):93–113.
   Anikin I.V. Methods and algorithms for quantitative assessment and management of security risks in corporate information networks based on fuzzy logic. *Systems Engineering and Information Technologies.* 2023;5(3):93–113. (In Russ.).
3. Якшин А.А., Демяненко А.Н. Живучесть системы управления и информации, передаваемой по радиолиниям робототехнических комплексов. *Актуальные исследования.* 2025;(14-1):52–55.
   Yakshin A.A., Demyanenko A.N. Survivability of the control system and information transmitted over the radio lines of robotic complexes. *Current Research.* 2025;(14-1):52–55. (In Russ.).
4. Васильев В.И., Вульфин А.М., Герасимова И.Б. и др. Анализ рисков кибербезопасности с помощью нечетких когнитивных карт. *Вопросы кибербезопасности.* 2020;(2):11–21.
   Vasilyev V., Vulfin A., Gerasimova I., et al. Analysis of cybersecurity risk with use of fuzzy cognitive maps. *Voprosy kiberbezopasnosti.* 2020;(2):11–21. (In Russ.).
5. Ожгибесова А.С., Шабуров А.С., Капгер И.В. О разработке метода автоматизированной оценки рисков в контексте обеспечения живучести информационных систем. *Вопросы защиты информации.* 2025;(1):40–45.
   Ozhgibesova A.S., Shaburov A.S., Kapger I.V. On the development of a method for automated risk assessment in the context of ensuring the survivability of information systems. *Information Security Questions.* 2025;(1):40–45. (In Russ.).
6. Ожгибесова А.С., Шабуров А.С., Южаков А.А. О совершенствовании подхода к оценке рисков безопасности информации в контексте обеспечения живучести информационных систем. *Системная инженерия и информационные технологии.* 2025;7(5):157–169. https://doi.org/10.54708/2658-5014-SIIT-2025-no5-p157
   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. *Systems Engineering and Information Technologies.* 2025;7(5):157–169. (In Russ.). https://doi.org/10.54708/2658-5014-SIIT-2025-no5-p157
7. Палютина Г.Н. О применении нейронных сетей для оценки весов связей между концептами нечеткой когнитивной карты в адаптивной оценке рисков информационной безопасности. *Вестник УрФО. Безопасность в информационной сфере.* 2023;(4):60–69. https://doi.org/10.14529/secur230406
   Palyutina G.N. On the application of neural networks for estimating the weights of connections between the concepts of a fuzzy cognitive map. *Journal of the Ural Federal District. Information Security.* 2023;(4):60–69. (In Russ.). https://doi.org/10.14529/secur230406
8. Шаев Ю.М., Самойлова Е.О. Технология «умного дома» и тенденции трансформаций жизненного пространства. *Философские проблемы информационных технологий и киберпространства.* 2020;(1):45–53. https://doi.org/10.17726/philIT.2020.1.4
   Shaev Y.M., Samoylova E.O. Smart house technology and tendencies of life space transformations. *Philosophical Problems of IT & Cyberspace (PhilIT&C).* 2020;(1):45–53. (In Russ.). https://doi.org/10.17726/philIT.2020.1.4

9. Капитонова Т.А., Стручкова Г.П., Слепцов О.И. Использование байесовских сетей для выработки рекомендаций при отказах северного магистрального газопровода Мастах-Берге-Якутск. *Вычислительные технологии.* 2023;28(4):35–44. https://doi.org/10.25743/ICT.2023.28.4.004
Kapitonova T.A., Struchkova G.P., Sleptsov O.I. Using Bayesian networks to establish recommendations for the case of failure of the northern main gas pipeline. *Computational Technologies.* 2023;28(4):35–44. (In Russ.). https://doi.org/10.25743/ICT.2023.28.4.004
10. Бабкин А.Н., Акчурина Л.В., Алексеенко С.П. Практическая реализация цепей Маркова в исследовании телекоммуникационных сетей при воздействии угроз информационной безопасности. *Вестник Воронежского института МВД России.* 2022;(1):18–23.
Babkin A.N., Akchurina L.V., Alekseenko S.P. Practical implementation of Markov chains in the study of telecommunication networks under the influence of information security threats. *Vestnik of Voronezh Institute of the Ministry of the Interior of Russia.* 2022;(1):18–23. (In Russ.).

ИНФОРМАЦИЯОБАВТОРЕ / INFORMATION ABOUT THE AUTHOR

Ожгибесова Анна Сергеевна, аспирантка кафедры «Автоматика и телемеханика», Пермский национальный исследовательский политехнический университет, Пермь, Российская Федерация.
e-mail: aozgibesova@pstu.ru

Anna S. Ozhgibesova, Postgraduate at the Department of Automation and Telemechanics, Perm National Research Polytechnic University, Perm, the Russian Federation.

Статья поступила в редакцию 13.04.2026; одобрена после рецензирования 10.06.2026; принята к публикации 24.06.2026.

The article was submitted 13.04.2026; approved after reviewing 10.06.2026; accepted for publication 24.06.2026.