МРНТИ 27.35.33

10.51889/2959-5894.2024.87.3.013

Д.Д. Жаксыгулова[1*], С.Ж. Рахметуллина[1], С.А Гнатюк[2]

[1]Восточно-Казахстанский технический университет им. Д. Серикбаева, г. Усть-Каменогорск, Казахстан
[2]Национальный авиационный университет, г. Киев, Украина
[*]e-mail: daurija_zd@mail.ru

ИССЛЕДОВАНИЕ МОДЕЛИ РАСЧЕТА КОЛИЧЕСТВЕННОГО КРИТЕРИЯ ОЦЕНКИ УСТОЙЧИВОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФРАСТРУКТУРЫ

Аннотация

С учетом глобальных тенденций к увеличению числа и сложности кибератак возникает неотложная необходимость в обеспечении устойчивости информационно-технических систем (ИТС), особенно отраслевых, играющих критическую роль в общественном функционировании, социально-экономическом развитии и национальной безопасности. В связи с этим, на уровне государства решение проблемы обеспечения безопасности критической инфраструктуры становится приоритетом в процессе реформирования сектора обороны и безопасности Республики Казахстан. В данном контексте возникает неотложная необходимость разработки методов и моделей для отнесения ИС к критическим объектам инфраструктуры с целью обеспечения национальной безопасности Казахстана. В настоящем исследовании представлена модель расчета количественного критерия устойчивости информационных систем, основанная на методе анализа иерархий. Этот подход позволяет получить количественные показатели устойчивости ИС путем обработки экспертных оценок. Применение данной модели упрощает процедуру подбора экспертов, избегает сложностей обработки экспертных данных и обеспечивает оценку ИС при ограниченных статистических данных. Разработанная модель позволяет перейти от качественной оценки, представленной упорядоченным рядом буквенно-числовых комбинаций, отражающих уровни реализованных услуг, к количественной оценке в виде отношения функциональных профилей защищенности.

Ключевые слова: информационные системы, критический объект инфраструктуры, кибербезопасность, количественный критерий, критерий оценки защищенности, функциональный профиль защищенности.

Д.Д. Жаксыгулова[1], С.Ж. Рахметуллина[1], С.А. Гнатюк[2]
[1]Д. Серікбаев атындағы Шығыс Қазақстан техникалық университеті, Өскемен, Қазақстан
[2]Ұлттық авиация университеті, Киев, Украина

ИНФРАҚҰРЫЛЫМНЫҢ АСА МАҢЫЗДЫ ОБЪЕКТІЛЕРІНІҢ АҚПАРАТТЫҚ-ТЕЛЕКОММУНИКАЦИЯЛЫҚ ЖҮЙЕЛЕРІНІҢ ТҰРАҚТЫЛЫҒЫН БАҒАЛАУДЫҢ САНДЫҚ КРИТЕРИЙІН ЕСЕПТЕУ МОДЕЛІН ЗЕРТТЕУ

Аңдатпа

Кибершабуылдардың саны мен күрделілігінің артуының жаһандық тенденцияларын ескере отырып, ақпараттық-техникалық жүйелердің (АТЖ), әсіресе қоғамдық қызметте, әлеуметтік-экономикалық дамуда және Ұлттық қауіпсіздікте маңызды рөл атқаратын салалық жүйелердің тұрақтылығын қамтамасыз етудің шұғыл қажеттілігі туындайды. Осыған байланысты, маңызды инфрақұрылымның қауіпсіздігін мемлекет деңгейінде қамтамасыз ету проблемасын шешу Қазақстан Республикасының Қорғаныс және қауіпсіздік секторын реформалау процесінде басымдыққа айналады. Осы тұрғыда Қазақстанның ұлттық қауіпсіздігін қамтамасыз ету мақсатында ақпараттық жүйені (АЖ) инфрақұрылымның маңызды объектілеріне жатқызу үшін әдістер мен модельдерді әзірлеудің шұғыл қажеттілігі туындайды. Бұл зерттеу иерархияларды талдау әдісіне негізделген ақпараттық жүйелердің тұрақтылығының сандық критерийін есептеу моделін ұсынады. Бұл тәсіл сараптамалық бағалауды өңдеу арқылы АЖ тұрақтылығының сандық көрсеткіштерін алуға мүмкіндік береді. Бұл модельді қолдану сарапшыларды таңдау процедурасын жеңілдетеді, сараптамалық деректерді өңдеудегі

қиындықтардан аулақ болады және шектеулі статистикалық мәліметтермен АЖ бағалауды қамтамасыз етеді. Әзірленген модель іске асырылған қызметтердің деңгейлерін көрсететін әріптік-сандық комбинациялардың реттелген сериясымен ұсынылған сапалық бағалаудан функционалдық қауіпсіздік профильдерінің қатынасы түріндегі сандық бағалауға көшуге мүмкіндік береді.

Түйін сөздер: ақпараттық жүйелер, маңызды инфрақұрылым объектісі, киберқауіпсіздік, сандық критерий, қауіпсіздікті бағалау критерийі, функционалдық қауіпсіздік профилі.

D.D. Zhaxsygulova[1], S.Zh. Rakhmetullina[1], S.O. Gnatyuk[2]
[1]D. Serikbayev East Kazakhstan Technical University, Ust`-Kamenogorsk, Kazakhstan,
[2]National Aviation University, Kyiv, Ukraine

STUDY OF A MODEL FOR CALCULATING A QUANTITATIVE CRITERION FOR ASSESSING THE STABILITY OF INFORMATION AND TELECOMMUNICATION SYSTEMS OF CRITICAL INFRASTRUCTURE FACILITIES

Abstract

Given the global trends towards an increase in the number and complexity of cyberattacks, there is an urgent need to ensure the resilience of information technology systems (ITS), especially sectoral systems that play a critical role in public functioning, socio-economic development and national security. In this regard, at the level of the state, the solution of the problem of ensuring the security of critical infrastructure becomes a priority in the process of reforming the defense and security sector of the Republic of Kazakhstan. In this context, there is an urgent need to develop methods and models for attributing IS to critical infrastructure objects in order to ensure national security of Kazakhstan. This study presents a model for calculating the quantitative criterion of information systems sustainability based on the method of hierarchy analysis. This approach allows us to obtain quantitative indicators of IS sustainability by processing expert evaluations. The application of this model simplifies the procedure of expert selection, avoids the complexities of expert data processing and provides IS assessment with limited statistical data. The developed model allows us to move from a qualitative assessment, represented by an ordered series of alphanumeric combinations reflecting the levels of realized services, to a quantitative assessment in the form of a ratio of functional profiles of security.

Keywords: information systems, critical infrastructure object, cybersecurity, quantitative criterion, security assessment criterion, functional security profile.

Основные положения

В данной статье представлена модель расчета количественного критерия оценки устойчивости информационно-телекоммуникационных систем (ИТС), основанная на методе анализа иерархий. Исследование акцентирует внимание на критически важных критериях защищенности, таких как конфиденциальность, наблюдаемость, доступность и целостность. Составленная матрица сравнений продемонстрировала значимость каждого из этих критериев для общей оценки устойчивости систем к различным угрозам. Результаты подтверждают необходимость дальнейшего анализа взаимосвязей между критериями и их влияния на защиту информационно-технических систем. Это открывает перспективы для разработки более эффективных методов и стратегий защиты, критически важных для национальной безопасности.

Введение

Сегодня информационно-коммуникационные технологии (ИКТ) критически важны для обеспечения ключевых функций общества и государства, таких как предоставление государственных, финансовых и медицинских услуг, обеспечение безопасности, связи и функционирование жизнеобеспечивающих объектов. Надежность этих технологий, включая серверы, системы управления, центры обработки данных и информационные системы, существенно влияет на обеспечение жизненных потребностей населения.

Учитывая, что нарушение работы этих систем может привести к серьезным последствиям, включая незаконный доступ к личным данным и сведениям охраняемой законом тайны, а также создание чрезвычайных ситуаций, в настоящее время во многих странах

разрабатываются перечни критически важных объектов и информационных систем (КВОИКИ). Эти перечни предназначены для эффективного управления чрезвычайными ситуациями социального, техногенного и других характеров, а также для обеспечения безопасности, обороны и экономической стабильности.

В условиях мировых тенденций, связанных с увеличением частоты и усложнением кибератак, вопрос устойчивости информационных систем отраслевого уровня становится все более актуальным. Особенно это касается тех систем, которые играют ключевую роль в обеспечении стабильного функционирования общества, поддержке социально-экономического развития страны и защите информационной составляющей национальной безопасности [1]. С учетом национальных потребностей в обеспечении безопасности и важности системного подхода к защите критической инфраструктуры на государственном уровне, создание эффективной системы защиты таких объектов становится одним из приоритетных направлений в процессе реформирования оборонного и безопасного сектора любой страны, включая Казахстан (Постановление Правительства РК № 559 от 13.07.2023 г.) [2]. В данном контексте основными проблемами, требующими решения, являются отсутствие унифицированных критериев и методологии отнесения ИС, являющихся частью объектов инфраструктуры, к категории критически важной инфраструктуры; отсутствие единой методологии оценки угроз безопасности ИС, являющихся критически важными объектами инфраструктуры.

Принципы классификации объектов информационно-коммуникационной инфраструктуры как критически важных соответствуют положениям Закона Республики Казахстан «Об информатизации» и регламентируют процесс их отнесения к этой категории в рамках информационно-коммуникационной инфраструктуры.

Важно отметить, что Закон Республики Казахстан «Об информатизации» №141-VII от 14.07.2022 года устанавливает правила составления перечня критической информационной инфраструктуры [1], а также разработку критериев и процедур, по которым объекты информационно-коммуникационной инфраструктуры признаются критически важными. Согласно Указу Президента Казахстана, для обеспечения киберзащиты критической инфраструктуры первоочередной задачей является установление критериев, позволяющих классифицировать информационные (автоматизированные), телекоммуникационные и информационно-технические системы как критическую информационную инфраструктуру.

Необходимо подчеркнуть, что в 13.07.2023 года был приняты изменения закона в данной области [3]. Этот закон определяет юридические и организационные основы создания и функционирования национальной системы защиты критической инфраструктуры.

Таким образом, упомянутые нормативно-правовые акты Казахстана подчеркивают необходимость разработки единых критериев и методологии для классификации информационно-технических систем (ИТС) как составляющих критической инфраструктуры государства. Следует отметить, что использование качественных оценок вместо количественных объясняется сложностью их сопоставления и воспроизведения. Это связано, в первую очередь, с трудностями в подборе экспертов и спецификой обработки экспертных данных. Указанные ограничения подчеркивают наличие важной научной задачи — установления критериев для определения отнесения ИТС к критической информационной инфраструктуре.

В 2023 году 514 объектов информационно-коммуникационной инфраструктуры были классифицированы как критически важные объекты информационно-коммуникационной инфраструктуры (далее - КВОИКИ) в соответствии с определенными критериями. Эти критерии включают:

1. Воздействие объекта информационно-коммуникационной инфраструктуры на бесперебойное функционирование особо важных государственных объектов. Нарушение работы этого объекта может привести к прекращению деятельности таких государственных объектов.

2. Воздействие объекта на непрерывное и безопасное функционирование стратегических объектов. Нарушение работы этого объекта может вызвать остановку деятельности стратегических объектов или угрозу техногенной чрезвычайной ситуации.

3. Воздействие объекта на беспрепятственное функционирование объектов отраслей экономики, имеющих стратегическое значение. Нарушение работы этого объекта может привести к прекращению деятельности таких объектов или угрозе техногенной чрезвычайной ситуации.

4. Воздействие объекта на обеспечение устойчивого функционирования «электронного правительства» и других информационно-коммуникационных услуг. Полное или частичное прекращение работы этого объекта может привести к незаконному сбору и обработке ограниченного доступа персональных данных и сведений, содержащих охраняемую законом тайну, а также к чрезвычайным ситуациям социального характера.

Методология исследования

Для анализа и моделирования использовались данные реальных информационно-телекоммуникационных систем, включая автоматизированные, телекоммуникационные и информационно-технические системы, относящиеся к критическим объектам инфраструктуры Казахстана. Эти данные были собраны через взаимодействие с профильными организациями и государственными структурами, ответственными за обеспечение информационной безопасности и киберзащиты. Выборка объектов исследования включала в себя:

1. Информационные системы государственного сектора, используемые для управления критической инфраструктурой.

2. Телекоммуникационные системы, обеспечивающие связь и передачу данных на критических объектах.

3. Автоматизированные системы, задействованные в управлении процессами на таких объектах, как энергосети, водоснабжение и транспортные узлы.

Методы, использованные в исследовании, включают: анализ нормативно-правовой базы Казахстана в области информационной безопасности, в том числе Закона Республики Казахстан «Об информатизации» и соответствующих постановлений правительства, математическое моделирование, направленное на разработку количественного критерия устойчивости информационных систем. В качестве модели использовались методы анализа надежности, а также имитационные и вероятностные модели для прогнозирования устойчивости системы к внешним и внутренним угрозам. Сравнительный анализ, который включал сопоставление устойчивости систем в разных отраслях (энергетика, транспорт, связь) с целью выявления закономерностей и общих факторов риска.

Анализ исследований и публикаций

Для выбора наиболее эффективного метода расчета количественного критерия защищенности информационно-технических систем (ИТС), в работе [3] был проведен анализ существующих методов принятия решений. Авторы отмечают, что общий принцип классификации этих методов базируется на их содержании и типе экспертной информации, получаемой в ходе оценки [4-8]. Рассмотренные методы делятся на те, которые применяются в условиях определенности, и те, которые актуальны при неопределенности или нечеткости данных. По мнению [4], наибольший потенциал имеют следующие подходы:

1. Методы теории ожидаемой полезности предполагают, что каждое действие приводит к определенным последствиям, которые описываются набором характеристик, факторов или показателей. Выбор осуществляется в пользу той альтернативы, чьи последствия наиболее предпочтительны. Для применения данного метода требуется количественная оценка всех возможных результатов, возникающих при принятии решений, после чего на основе этих оценок выбирается оптимальный результат [4, 8].

2. Метод анализа иерархий представляет собой математический инструмент системного подхода к решению сложных задач принятия решений. Он предусматривает синтез приоритетов на основе субъективных экспертных оценок. Этот метод помогает эксперту выбрать вариант решения, который наиболее соответствует его пониманию проблемы и предъявляемым к ней требованиям.

3. Методы теории нечетких множеств направлены на формализацию исходных параметров в виде вектора интервальных значений, где каждый интервал характеризуется степенью неопределенности. Допустимые границы параметров и наиболее вероятные области их значений определяются на основе исходных данных, опыта и интуиции. Основной характеристикой этих методов является функция принадлежности параметра к интервалу [9]. Существуют различные современные способы определения функций принадлежности, такие как методы попарных сравнений, экспертные оценки, использование лингвистических терминов со статистическими данными, а также параметрические и интервальные оценки [10].

Проведенный в данном исследовании анализ выявил, что наибольшую эффективность проявляют методы, основанные на правилах. Учитывая как преимущества, так и недостатки указанных методов, было принято решение использовать метод анализа иерархий для расчета количественного критерия оценки защищенности. В работе [4], авторами представлена модель расчета количественного критерия оценки защищенности информационно-технических систем (ИТС) критической инфраструктуры государства. Однако данная работа ограничивается теоретическим обоснованием предложенной модели, не предоставляя экспериментального исследования в конкретной области критической инфраструктуры. Учитывая этот аспект, основной целью настоящей статьи является проведение экспериментального исследования модели расчета количественного критерия оценки защищенности ИТС.

Теоретические основы исследования

Предложенная модель, основанная на методе анализа иерархий, позволяет преобразовать качественную оценку, выраженную через упорядоченные буквенно-числовые комбинации [11], характеризующие уровни предоставляемых услуг, в количественную оценку, отражающую соотношение между базовым и экспертно определенным профилем защищенности. Исходные данные для этой модели включают базовый функциональный профиль защищенности, также называемый $ФПЗ_Б$, и профиль, скорректированный экспертом ($ФПЗ_Э$). Согласно стандарту НД ТЗИ 2.5-005-99, который регламентирует требования по защите информации от несанкционированного доступа, ФПЗ устанавливает меры для защиты информации от определенных угроз и применяет актуальные функциональные сервисы для их предотвращения [13]. Модель расчета количественного критерия оценки защищенности информационно-технических систем (ИТС), основанная на методе анализа иерархий, показана на рисунке 1 [4].

Метод анализа иерархий для определения отношения между альтернативами ($ФПЗ_Б$ и $ФПЗ_Э$) реализуется в последовательности шагов:

1. Сначала создаются матрицы попарных сравнений для каждого уровня критериев (где критерии защищенности составляют 1 уровень, критерии услуг безопасности – 2 уровень, а критерии уровней услуг безопасности – 3 уровень):

$$A = \left\| a_{ij} \right\|_{nxn}, \tag{1}$$

где $a_{ij} = w_i / w_j$, а w_i -«вес» i – того критерия

при этом, то есть, матрица положительной, обратно симметричным

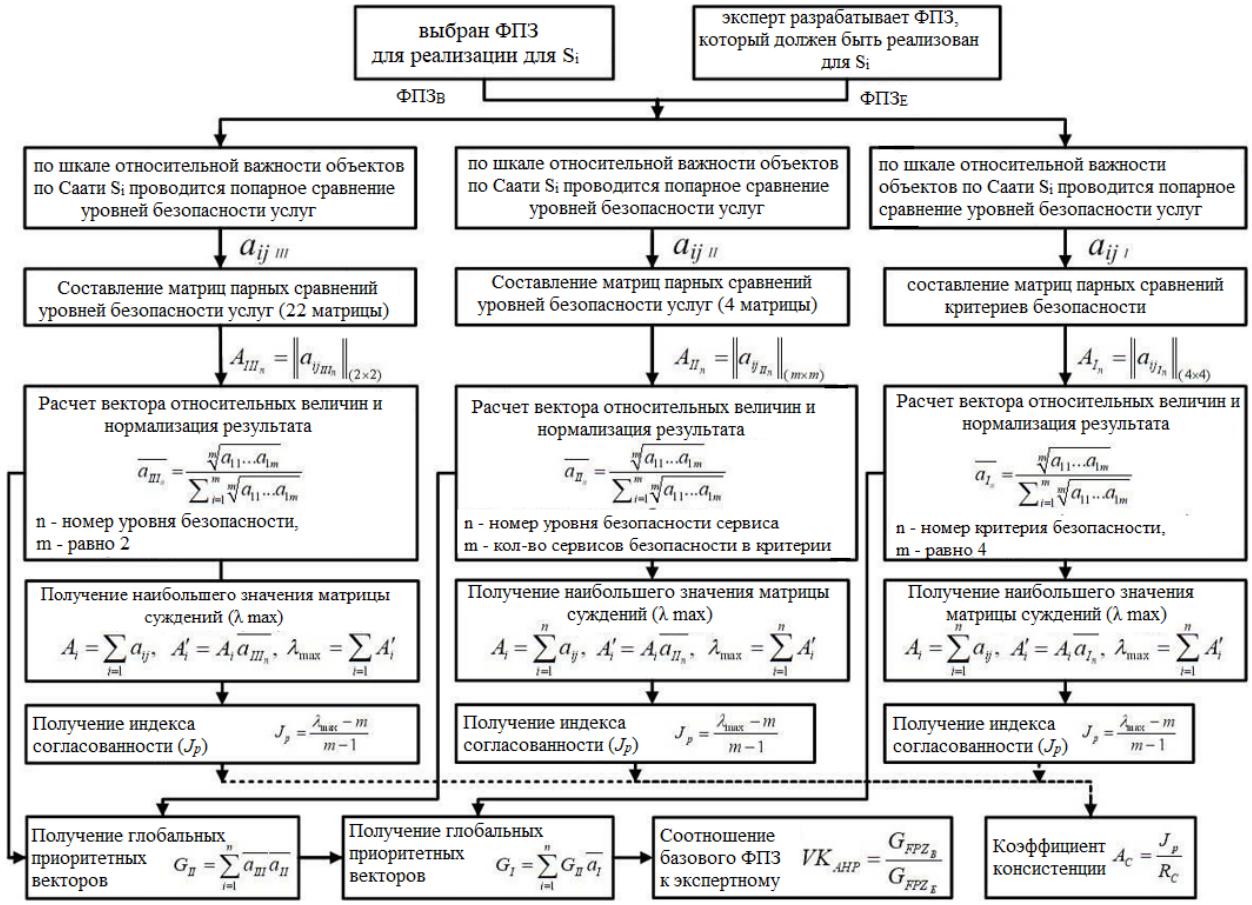

Рисунок 1. Блок-схема исследуемой модели

Для определения веса будем использовать следующие данные относительной важности (Таблица 1) [4].

Таблица 1. Шкала относительной важности критериев [4]

Вербальная оценка эксперта	*Значение a_{ij}*
w_i *абсолютно лучше* w_j	9
w_i *намного лучше* w_j	8
w_i *значительно лучше* w_j	7
w_i *лучше, чем* w_j	6
w_i *существенно превосходит* w_j	5
w_i *превосходит* w_j	4
w_i *несколько превосходит* w_j	3
w_i *не существенно превосходит* w_j	2
критерии равноценны	1
w_j *не существенно преобладает* w_i	1/2
w_j *несколько преобладает* w_i	1/3
w_j *преобладает* w_i	1/4
w_j *существенно преобладает* w_i	1/5
w_j *лучше* w_i	1/6
w_j *значительно лучше* w_i	1/7
w_j *намного лучше* w_i	1/8
w_j *абсолютно лучше* w_i	1/9

Для оценки критериев безопасности, матрица сравнения будет представлена в виде, представленном в таблице 2.

Таблица 2. Матрица сравнения для критериев безопасности [5]

	Конфиденциальность	*Наблюдаемость*	*Доступность*	*Целостность*
Конфиденциальность	a_{11}	a_{12}	a_{13}	a_{14}
Наблюдаемость	a_{21}	a_{22}	a_{23}	a_{24}
Доступность	a_{31}	a_{32}	a_{33}	a_{34}
Целостность	a_{41}	a_{42}	a_{43}	a_{44}

Для критериев безопасности сервиса составляются матрицы парных сравнений. Всего матриц может быть до 4. Для критериев уровня безопасности максимальное количество матриц может быть 22.

2. Производится расчет множества собственных векторов матрицы, при этом для каждой строки матрицы вычисляется среднее геометрическое:

$$a_i = \sqrt[n]{a_{i1} \cdot a_{i2} \cdot a_{i3} \cdot a_{in}} = \sqrt[n]{\prod_{j=1}^{n} a_{ij}}, \tag{2}$$

где n - это размерность матрицы.

3. Производится нормализация полученных результатов, что приводит к формированию нормализованного вектора приоритетов:

$$\overline{a_i} = \frac{a_i}{\sum_{j=1}^{n} a_j}, \tag{3}$$

4. Необходимо проверить согласованность локальных приоритетов. Необходимо выполнить расчет наибольшего собственного значения матрицы:

$$A_i = \sum_{i=1}^{n} a_{ij}, \tag{4}$$

$$A_i' = A_i \overline{a_{ij}}, \tag{5}$$

$$\lambda_{\max} = \sum_{i=1}^{n} A_i', \tag{6}$$

Расчет индекса согласованности:

$$J_p = \frac{\lambda_{\max} - m}{m-1}, \tag{7}$$

где m - количество сравниваемых элементов (размер матрицы).

Проверка корректности индекса согласованности осуществляется путем расчета отношения согласованности АС по формуле:

$$A_c = \frac{J_p}{R_c}, \tag{8}$$

где R_c - табличное значение (Таблица 3).

Таблица 3. Случайные согласованности для матриц размерности от 2 до 9

Размер матрицы m	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
Случайная согласованность R_c	*0*	*0,58*	*0,9*	*1,1*	*1,24*	*1,32*	*1,41*	*1,45*

В случае, если $A_c \geq 0{,}10,$ то данные в матрице сравнений подлежат пересмотру и уточнению.

5. Расчет глобального приоритета для критериев высокого уровня.

Нормализованный вектор приоритета для каждого критерия более низкого уровня умножается на нормализованный вектор приоритета критериев более высокого уровня. Произведения суммируются на более высоком уровне.

$$G_i = \sum_{i=1}^{n} \overline{a_i}\,\overline{b_i}, \tag{9}$$

где n - это количество критериев уровней безопасности.

6. Определение соотношения между альтернативами ($ФПЗ_Б$ и $ФПЗ_Э$).

Для каждого ФПЗ вычисляется общий приоритет по категориям конфиденциальности, целостности, доступности и наблюдаемости. Отношение этих общих приоритетов, отражающих количественный критерий, может быть представлено в следующей форме:

$$VK_{AHP} = \frac{G_{FPZ_B}}{G_{FPZ_E}}, \tag{10}$$

где G_{FPZ_B} – табличное значение ФПЗ для отраслевой ИТС,

G_{FPZ_E} – ФПЗ, полученное экспертом с использованием структурно-логической модели и структурно-функционального метода формирования ФПЗ отраслевой ИТС.

Результаты исследования

В большинстве стран мира информационно-телекоммуникационная отрасль занимает одну из ведущих позиций по степени критичности, уступая лишь энергетическим и транспортным системам [12].

Учитывая данную ситуацию, экспериментальная проверка разработанных в рамках исследования положений была проведена с использованием информационно-телекоммуникационной системы Национальной системы конфиденциальной связи (НСКС). С целью подтверждения модели расчета количественного критерия были построены матрицы попарных сравнений для каждого уровня критериев.

Для критериев защищенности (согласно [12]), матрица сравнений будет представлена следующим образом (Таблица 4).

Таблица 4. Матрица сравнений для критериев защищенности [5]

	Конфиденциальность	*Наблюдаемость*	*Доступность*	*Целостность*
Конфиденциальность	*1*	a_{12}	a_{13}	a_{14}
Наблюдаемость	a_{21}	*1*	a_{23}	a_{24}
Доступность	a_{31}	a_{32}	*1*	a_{34}
Целостность	a_{41}	a_{42}	a_{43}	*1*

Для критериев услуг безопасности (в соответствии с [13]) матрицы сравнений будут представлены в форме, изображенной в Таблицах 5-8.

Таблица 5 содержит матрицу критериев конфиденциальности, в которой КД представляет доверительную конфиденциальность, КА – административную конфиденциальность, КО – повторное использование объектов, КК – анализ скрытых каналов, а КВ – конфиденциальность при обмене.

Таблица 5. Матрица критериев конфиденциальности [5]

	КД	*КА*	*КО*	*КК*	*КВ*
КД	*1*	a_{12}	a_{13}	a_{14}	a_{15}
КА	a_{21}	*1*	a_{23}	a_{24}	a_{25}
КО	a_{31}	a_{32}	*1*	a_{34}	a_{35}
КК	a_{41}	a_{42}	a_{43}	*1*	a_{45}
КВ	a_{51}	a_{52}	a_{53}	a_{54}	*1*

Матрица критериев целостности представлена в таблице 6.

Таблица 6. Матрица критериев целостности [5]

	Доверительная целостность	*Административная целостность*	*Откат*	*Целостность при обмене*
Доверительная целостность	*1*	a_{12}	a_{13}	a_{14}
Административная целостность	a_{21}	*1*	a_{23}	a_{24}
Откат	a_{31}	a_{32}	*1*	a_{34}
Целостность при обмене	a_{41}	a_{42}	a_{43}	*1*

Матрица критериев доступности представлена в таблице 7.

Таблица 7. Матрица критериев доступности

	Использование ресурсов	*Устойчивость к отказам*	*Горячая замена горячей замены*	*Восстановление после сбоев*
Использование ресурсов	*1*	a_{12}	a_{13}	a_{14}
Устойчивость к отказам	a_{21}	*1*	a_{23}	a_{24}
Горячая замена горячей замены	a_{31}	a_{32}	*1*	a_{34}
Восстановление после сбоев	a_{41}	a_{42}	a_{43}	*1*

Матрица критериев наблюдаемости представлена в таблице 8, где НР - регистрация; НИ - идентификация и аутентификация; НО - распределение обязанностей, НО - аутентификация при обмене; НА - аутентификация отправителя; НП - аутентификация получателя; НК - достоверный канал; НЦ - целостность КСЗ; НТ - самотестирование.

Таблица 8. Матрица критериев наблюдаемости [5]

	НР	НИ	НО	НВ	НА	НП	НК	НЦ	НТ
НР	1	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_{18}	a_{19}
НИ	a_{21}	1	a_{23}	a_{24}	a_{25}	a_{26}	a_{27}	a_{28}	a_{29}
НО	a_{31}	a_{32}	1	a_{34}	a_{35}	a_{36}	a_{37}	a_{38}	a_{39}
НВ	a_{41}	a_{42}	a_{43}	1	a_{45}	a_{46}	a_{47}	a_{48}	a_{49}
НА	a_{51}	a_{52}	a_{53}	a_{54}	1	a_{56}	a_{57}	a_{58}	a_{59}
НП	a_{61}	a_{62}	a_{63}	a_{64}	a_{65}	1	a_{67}	a_{68}	a_{69}
НК	a_{71}	a_{72}	a_{73}	a_{74}	a_{75}	a_{76}	1	a_{78}	a_{79}
НЦ	a_{81}	a_{82}	a_{83}	a_{84}	a_{85}	a_{86}	a_{87}	1	a_{89}
НТ	a_{91}	a_{92}	a_{93}	a_{94}	a_{95}	a_{96}	a_{97}	a_{98}	1

Для критериев уровней безопасности, в нашем случае, составляются все 22 матрицы сравнений согласно таблице 9, где НР-1 - внешний анализ; НР-2 - защищенный журнал; НР-3 - сигнализация об опасности; НР-4 - детальная регистрация; НР-5 - анализ в реальном времени.

Таблица 9. Матрица критериев уровней безопасности [5]

	НР-1	НР-2	НР-3	НР-4	НР-5
НР-1	1	a_{12}	a_{13}	a_{14}	a_{15}
НР-2	a_{21}	1	a_{23}	a_{24}	a_{25}
НР-3	a_{31}	a_{32}	1	a_{34}	a_{35}
НР-4	a_{41}	a_{42}	a_{43}	1	a_{45}
НР-5	a_{51}	a_{52}	a_{53}	a_{54}	1

При заполнении матрицы применяется шкала, представленная в таблице 1. Расчет собственного множества векторов матрицы осуществляется по формуле (2), представляя собой среднее геометрическое для каждой матрицы. Нормализация результатов, приводящая к получению нормализованного вектора приоритетов, выполняется согласно формуле (3) с использованием того же программного обеспечения. Проверка согласованности локальных приоритетов также осуществляется с применением методов, описанных в источниках (4-7).

Дискуссия

Результаты исследования, включающие матрицу сравнений для критериев защищенности информационно-технических систем (ИТС), таких как конфиденциальность, наблюдаемость, доступность и целостность, позволяют более детально оценить устойчивость систем к различным угрозам. Применение метода анализа иерархий в данном контексте дало возможность формализовать экспертные оценки и перейти от качественных характеристик к количественным, что значительно повышает точность и воспроизводимость оценок.

Полученные данные показывают, что критерии, такие как конфиденциальность и доступность, играют ключевую роль в общей оценке защищенности ИТС. Это согласуется с выводами других исследователей, которые также отмечают важность этих параметров для устойчивости систем в условиях внешних и внутренних угроз.

В частности, согласно [4-5], конфиденциальность считается одним из основополагающих элементов кибербезопасности, так как утечка данных может иметь критические последствия для безопасности инфраструктуры.

Интересным результатом является значимость наблюдаемости, которая часто недооценивается в традиционных подходах к оценке защищенности. В данном исследовании она оказалась важным фактором, влияющим на способность системы адекватно реагировать на угрозы. Это открывает новые перспективы для будущих исследований, которые могли бы углубленно изучить взаимосвязь между наблюдаемостью и другими критериями.

Кроме того, разработанная матрица сравнений демонстрирует, что целостность данных также является критическим компонентом в обеспечении защищенности, что подтверждается многочисленными исследованиями в области информационной безопасности. Нарушение целостности может привести к серьёзным сбоям в работе ИТС, что делает этот параметр неотъемлемой частью общей модели устойчивости. Перспективы дальнейших исследований связаны с углубленным анализом взаимосвязей между критериями защищенности и адаптацией предложенной модели к различным типам ИТС. Также интересным направлением будет разработка гибридных моделей, сочетающих количественные и качественные методы оценки для улучшения точности и надежности выводов.

Выводы

В результате проведенного исследования была разработана модель расчета количественного критерия оценки устойчивости информационно-телекоммуникационных систем (ИТС), ориентированная на применение метода анализа иерархий. Основное внимание уделялось критериям защищенности, таким как конфиденциальность, наблюдаемость, доступность и целостность. Составленная матрица сравнений, использующая эти критерии, позволила формализовать процесс оценки и повысить его объективность.

Полученные результаты подтвердили значимость каждого из критериев в общей оценке защищенности систем, что согласуется с мнением других исследователей в области информационной безопасности. В частности, наблюдаемость и целостность данных оказались ключевыми факторами, влияющими на устойчивость ИТС к различным угрозам.

Исследование также выявило необходимость дальнейшего углубленного анализа взаимосвязей между критериями защищенности и их влияния на устойчивость систем. Будущие исследования могут сосредоточиться на разработке гибридных моделей, которые объединяют количественные и качественные подходы к оценке защищенности. Это откроет новые возможности для повышения надежности и эффективности информационно-телекоммуникационных систем, критически важных для функционирования инфраструктуры и обеспечения национальной безопасности.

В заключение, результаты данной работы могут быть полезными для практиков и исследователей в области информационной безопасности, обеспечивая основу для дальнейших исследований и разработки более эффективных стратегий защиты информационно-технических систем.

Список использованных источников

[1] Закон Республики Казахстан «Об информатизации» от 24 ноября 2016 года (с изменениями и дополнениями от 10 сентября 2023 года). https://adilet.zan.kz/rus/docs/Z1500000418

[2] Постановление Правительства Казахстана «Об утверждении Правил и критериев отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры» №529 от 8 сентября 2016 года (с изменениями и дополнениями от 13 июля 2023 года). https://adilet.zan.kz/rus/docs/V2300032996

[3] Концепция кибербезопасности («Киберщит Казахстана») Постановление Правительства Республики Казахстан от 30 июня 2017 года №407 (с изменениями и дополнениями от 17 марта 2023 года). https://adilet.zan.kz/rus/docs/P1700000407

[4] Юдин А.Ю., Сидоренко В.М., Гнатюк С.А., Верховец А.С. Модель расчета количественного критерия оценки защищенности информационно-телекоммуникационных систем критической

инфраструктуры государства // Современные информационные системы. – 2021. - Т. 5, № 4. - С. 109-115. https://doi.org/10.20998/2522-9052.2021.4.15

[5] Gnatyuk S. et al. The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems // IntelITSIS. – 2022. – С. 390-399.

[6] Гнатюк С.А., Юдин А.Ю., Сидоренко В.М., Евченко Я.П. Метод формирования функционального профиля защищенности отраслевых информационно-телекоммуникационных систем // Кибербезопасность: образование, наука, техника. – 2021. - Т. 3, № 11. - С. 166-182.

[7] Sarkar T.K., Salazar-Palma M., Zhu M.D., Chen H. Mathematical Principles Related to Modern System Analysis // Modern Characterization of Electromagnetic Systems and its Associated Metrology. – 2021. - P. 1-20. DOI: 10.1002/9781119076230.ch1.

[8] Guo X., Gao M., Zhang M., Chen Y., Tseng S.-P. Design and Implementation of Teaching Quality Assessment System based on Analytic Hierarchy Process Fuzzy Comprehensive Evaluation method // 2020 8th International Conference on Orange Technology (ICOT). – 2020. - P. 1-3. DOI: 10.1109/ICOT51877.2020.9468778.

[9] Sandoval-Alfaro O.E., Quintero-Meza R.R. Application of Data Analytics Techniques for Decision Making in the Retrospective Stage of the Agile Scrum Methodology // 2021 Mexican International Conference on Computer Science (ENC). – 2021. - P. 1-8. DOI: 10.1109/ENC53357.2021.9534800.

[10] Коробов В. Б., Тутыгин А. Г. Преимущества и недостатки метода анализа иерархий // Известия Российского государственного педагогического университета им. АИ Герцена. – 2010. – №. 122.

[11] Ma Z., Wang S., Deng X., Jiang W. An improved approach for adversarial decision making under uncertainty based on simultaneous game // 2018 Chinese Control and Decision Conference (CCDC). – 2018. - P. 2499-2503. DOI: 10.1109/CCDC.2018.8407545.

[12] Гнатюк С., Сидоренко В., Положенцев А., Сотниченко Ю. Экспериментальное определение уровня кибербезопасности в критической инфраструктуре гражданской авиации // Материалы Международной научно- практической конференции IEEE 2020: Problems of Infocommunications Science and Technology, PIC S and T. – Kyiv, Ukraine, 2020. - P. 757-764.

[13] СТ РК ИСО/МЭК 27002-2009, Свод правил по управлению защитой информации, СТ РК ИСО/МЭК РК, 2009. https://online.zakon.kz/Document/?doc_id=31458716

References

[1] Zakon Respubliki Kazakhstan «Ob informatizatsii» ot 24 noyabrya 2016 goda (s izmeneniyami i dopolneniyami ot 10 sentyabrya 2023 goda). https://adilet.zan.kz/rus/docs/Z1500000418

[2] Postanovleniye Pravitel'stva Kazakhstana «Ob utverzhdenii Pravil i kriteriyev otneseniya ob''yektov informatsionno-kommunikatsionnoy infrastruktury k kriticheski vazhnym ob''yektam informatsionno-kommunikatsionnoy infrastruktury» №529 ot 8 sentyabrya 2016 goda (s izmeneniyami i dopolneniyami ot 13 iyulya 2023 goda). https://adilet.zan.kz/rus/docs/V2300032996

[3] Kontseptsiya kiberbezopasnosti («Kibershchit Kazakhstana») Postanovleniye Pravitel'stva Respubliki Kazakhstan ot 30 iyunya 2017 goda №407 (s izmeneniyami i dopolneniyami ot 17 marta 2023 goda). https://adilet.zan.kz/rus/docs/P1700000407

[4] Yudin A.YU., Sidorenko V.M., Gnatyuk S.A., Verkhovets A.S. Model' rascheta kolichestvennogo kriteriya otsenki zashchishchennosti informatsionno-telekommunikatsionnykh sistem kriticheskoy infrastruktury gosudarstva // Sovremennyye informatsionnyye sistemy. – 2021. - T. 5, № 4. - C. 109-115. https://doi.org/10.20998/2522-9052.2021.4.15

[5] Gnatyuk S. et al. The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems // IntelITSIS. – 2022. – S. 390-399.

[6] Gnatyuk S.A., Yudin A.YU., Sidorenko V.M., Yevchenko YA.P. Metod formirovaniya funktsional'nogo profilya zashchishchennosti otraslevykh informatsionno-telekommunikatsionnykh sistem // Kiberbezopasnost': obrazovaniye, nauka, tekhnika. – 2021. - T. 3, № 11. - C. 166-182.

[7] Sarkar T.K., Salazar-Palma M., Zhu M.D., Chen H. Mathematical Principles Related to Modern System Analysis // Modern Characterization of Electromagnetic Systems and its Associated Metrology. – 2021. - P. 1-20. DOI: 10.1002/9781119076230.ch1.

[8] Guo X., Gao M., Zhang M., Chen Y., Tseng S.-P. Design and Implementation of Teaching Quality Assessment System based on Analytic Hierarchy Process Fuzzy Comprehensive Evaluation method // 2020 8th International Conference on Orange Technology (ICOT). – 2020. - P. 1-3. DOI: 10.1109/ICOT51877.2020.9468778.

[9] Sandoval-Alfaro O.E., Quintero-Meza R.R. Application of Data Analytics Techniques for Decision Making in the Retrospective Stage of the Agile Scrum Methodology // 2021 Mexican International Conference on Computer Science (ENC). – 2021. - P. 1-8. DOI: 10.1109/ENC53357.2021.9534800.

[10] Korobov V. B., Tutygin A. G. Preimushchestva i nedostatki metoda analiza iyerarkhiy // Izvestiya Rossiyskogo gosudarstvennogo pedagogicheskogo universiteta im. AI Gertsena. – 2010. – №. 122.

[11] Ma Z., Wang S., Deng X., Jiang W. An improved approach for adversarial decision making under uncertainty based on simultaneous game // 2018 Chinese Control and Decision Conference (CCDC). – 2018. - P. 2499-2503. DOI: 10.1109/CCDC.2018.8407545.

[12] Gnatyuk S., Sidorenko V., Polozhentsev A., Sotnichenko YU. Eksperimental'noye opredeleniye urovnya kiberbezopasnosti v kriticheskoy infrastrukture grazhdanskoy aviatsii // Materialy Mezhdunarodnoy nauchno-prakticheskoy konferentsii IEEE 2020: Problems of Infocommunications Science and Technology, PIC S and T. – Kyiv, Ukraine, 2020. - R. 757-764.

[13] ST RK ISO/MEK 27002-2009, Svod pravil po upravleniyu zashchitoy informatsii, ST RK ISO/MEK RK, 2009. https://online.zakon.kz/Document/?doc_id=31458716