DOI 10.37882/2223-2966.2025.06.42

АНАЛИЗ СОВРЕМЕННЫХ ПОДХОДОВ К ОЦЕНКЕ КОМПЛЕКСНОГО ПОКАЗАТЕЛЯ КИБЕРУСТОЙЧИВОСТИ

ANALYSIS OF MODERN APPROACHES TO ASSESSING A COMPREHENSIVE INDICATOR OF CYBER-RESISTANCE

D. Suzdalsky

Summary. The article argues for the need to implement a comprehensive assessment of the security of information systems through the prism of the cyber resilience indicator. The article examines modern methods for creating cyber threat-resistant infrastructures proposed by various organizations, including NIST, the US Department of Homeland Security, MITRE, and Positive Technologies, etc. A review of existing sources revealed the lack of a universal approach to cyber resilience. At the moment, uniform criteria and metrics have not been formed to measure the effectiveness and level of cyber resilience of organizations, despite the availability of separate practical developments in this area. It is emphasized that cyber resilience issues are an interdisciplinary field that requires a comprehensive solution to interrelated tasks. In conclusion, there is a significant gap in the field of standardization — the lack of a holistic methodology combining the necessary methods, models, and algorithms to ensure the cyber stability of information systems.

Keywords: cybersecurity, functional stability, business continuity, cyber resilience.

Суздальский Дмитрий Андреевич
аспирант,
Российский Экономический Университет, г. Москва
ya.jummer@yandex.ru

Аннотация. В статье аргументируется необходимость внедрения комплексной оценки безопасности информационных систем через призму показателя киберустойчивости. Исследованы современные методики создания устойчивых к киберугрозам инфраструктур, предложенные различными организациями, включая NIST, Департамент внутренней безопасности США, MITRE и Positive Technologies и др.

Проведенный обзор существующих источников выявил отсутствие универсального подхода к обеспечению киберустойчивости. На данный момент не сформированы единые критерии и метрики для измерения эффективности и уровня киберустойчивости организаций, несмотря на наличие отдельных практических разработок в этой сфере.

Подчеркивается, что вопросы киберустойчивости представляют собой междисциплинарную область, требующую комплексного решения взаимосвязанных задач. В заключении отмечается существенный пробел в области стандартизации — отсутствие целостной методологии, объединяющей необходимые методы, модели и алгоритмы для обеспечения киберустойчивости информационных систем.

Ключевые слова: кибербезопасность, функциональная устойчивость, непрерывность бизнеса, киберустойчивость.

Введение

В настоящее время предприятия активно интегрируют корпоративные информационные системы (КИС) в свои бизнес-процессы для повышения эффективности работы. Учитывая, что успешность цифровых бизнес-операций тесно связана с использованием данных из этих систем, вопросы их защиты выходят на первый план.

В условиях усиления информационных конфликтов в киберпространстве значительно возрастает значимость защиты данных субъектов экономической деятельности (СЭД) [1–2]. Необходимо учитывать, что киберпространство является динамичной глобальной информационной средой, что делает обеспечение киберустойчивости организаций релевантным только в конкретный временной период.

Следовательно, стратегии защиты информационных систем должны обладать гибкостью и способностью к адаптации, принимая во внимание изменчивость цифровой среды и появление новых угроз. Это требует комплексного подхода к обеспечению безопасности, который охватывает защиту данных, поддержание функционирования информационных систем и непрерывность бизнес-процессов.

Для решения данной проблемы предлагается провести исследование современных инновационных методов и моделей оценки интегрального показателя киберустойчивости. Данный показатель включает в себя отдельные метрики кибербезопасности, отказоустойчивости и непрерывности бизнес-процессов [4–5].

Основной задачей анализа существующих методологий и моделей оценки интегрального показателя киберустойчивости является выявление и отбор наиболее эффективных и проверенных практик для оценки уровня киберустойчивости организаций.

Анализ существующих подходов к оценке комплексного показателя киберустойчивости

На сегодняшний день сформировалось несколько направлений в создании киберустойчивой инфраструктуры, разработанных различными организациями:

- Национальным институтом стандартов и технологий (NIST);
- Департаментом внутренней безопасности США;
- Компанией MITRE;
- Компанией Positive Technologies;
- Другими ведущими специалистами в области кибербезопасности.

Однако, несмотря на наличие множества подходов, в данной области пока не существует универсального методологического решения. Отсутствуют четко сформулированные критерии и метрики, которые позволили бы объективно оценить уровень киберустойчивости организации и эффективность применяемых мер защиты.

Тем не менее, в этой сфере накоплен определенный опыт и разработаны отдельные практические решения. Далее будут представлены результаты анализа существующих подходов и их особенностей, что позволит лучше понять текущее состояние вопроса и определить направления для дальнейшего развития методологии обеспечения киберустойчивости.

Киберустойчивость согласно NIST (Национальный институт стандартов и технологий США)

Согласно определению NIST, киберустойчивость представляет собой комплексную способность организации заблаговременно выявлять потенциальные угрозы, эффективно сопротивляться кибератакам, оперативно восстанавливать работоспособность систем после инцидентов и гибко адаптироваться к меняющимся условиям киберактивности. Данная способность охватывает защиту и реагирование на различные неблагоприятные факторы, включая информационные атаки и компрометацию систем, функционирующих с использованием цифровых ресурсов. Для реализации необходимого уровня киберустойчивости требуется проведение комплекса мероприятий, учитывающих все перечисленные выше характеристики и направленные на обеспечение надежной защиты информационных активов организации, рисунок 1. [3].

Документ определяет следующие ключевые направления для обеспечения киберустойчивости организации:

- Проактивная защита от несанкционированного доступа и попыток взлома систем;
- Стратегическое планирование мер по выявлению потенциальных угроз и созданию эффективных механизмов противодействия;
- Устойчивость инфраструктуры к различным видам кибератак и способность сохранять работоспособность в кризисных ситуациях;
- Минимизация последствий в случае успешной реализации кибератаки;
- Восстановление систем до исходного состояния после инцидента;
- Мониторинг состояния информационных ресурсов как в штатном режиме, так и в период реагирования на атаки;
- Адаптация бизнес-процессов и технической поддержки для поддержания непрерывного функционирования организации.

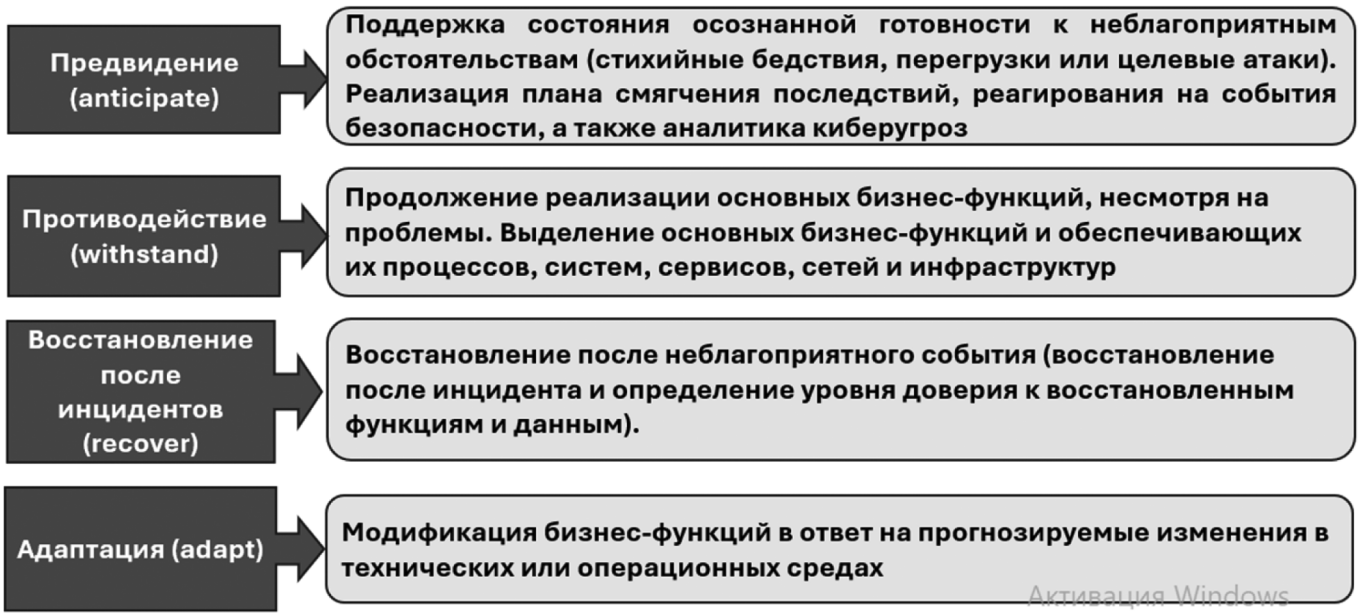

Рис. 1. Мероприятия для достижения целей обеспечения киберустойчивости согласно NIST

Для решения сформулированных задач в целях построения киберустойчивых систем реализуются техники [3], таблица 1.

Таблица 1.

Техники для решения задач обеспечения киберустойчивости

Техника	Содержание техники
Мониторинг	Непрерывное отслеживание функционирования всех систем
Адаптивное реагирование	Применение гибких инструментов реагирования на риски.
Контекстная осведомлённость	Документирование всех процессов
Скоординированная защита	Оркестрация средств безопасности
Обман/запутывание нарушителя	Введение в заблуждение нарушителя
Разнообразие	Использование различных компонентов в архитектуре системы для снижения повторяемости уязвимостей.
Динамическое позиционирование	Перемещение ресурсов (например, микросервисов) на другие аппаратно-программные платформы.
Очистка состояния	Удаление данных после окончания их использования.
Ограничение привилегий	Реализация принципа минимальных привилегий.
Реструктуризация	Текущая структуризация систем и пользователей в соответствии с целями и бизнес-функциями.
Избыточность	Дублирование данных и наиболее критичного функционала
Сегментация	Разделение инфраструктуры на изолированные компоненты с учетом их критичности и отказоустойчивости.
Подтверждение целостности	Обеспечение целостности данных в том числе с использованием технологии блокчейна.
Непредсказуемость	Обеспечение высокой степени неопределенности представлений нарушителя о системе и ее состоянии.

Перечисленные техники реализуются в рамках организационных, технических, программно-аппаратных и морально-этических мероприятий.

Методика оценки киберустойчивости Cyber Resilience Review (CRR)

Cyber Resilience Review (CRR) представляет собой методологию оценки киберустойчивости, созданную Департаментом внутренней безопасности США. Данная методика базируется на модели управления устойчивостью *CERT Resilience Management Model (CERT-RMM)* версии 1.2 и направлена на комплексную оценку способности организации противостоять киберугрозам, а также на выявление слабых мест для их последующего устранения с применением лучших отраслевых практик [6].

Оценка киберустойчивости по методологии CRR охватывает следующие ключевые области:

- Asset Management — управление информационными активами;
- Control Management — контроль защитных механизмов;
- Configuration & Change Management — управление конфигурацией и изменениями;
- Vulnerability Management — работа с уязвимостями.
- Incident Management — реагирование на инциденты;
- Continuity Management — обеспечение непрерывности работы;
- Risk Management — управление рисками;
- External Dependency Management — контроль внешних зависимостей;
- Awareness & Training — обучение персонала и повышение осведомленности;
- Situational Awareness — мониторинг текущей ситуации.

Каждая из этих областей играет важную роль в формировании общей киберустойчивости организации и требует постоянного внимания и совершенствования.

Методика оценки киберустойчивости ИПУ РАН

Российские специалисты разработали критерии киберустойчивости [7] для оценки безопасности программного обеспечения. Эти критерии основаны на анализе конфигураций ПО и включают два основных положения:

- Отсутствие критических сбоёв — в инфраструктуре не должно быть таких конфигураций ПО, которые приводят к невыполнению штатных функций;
- Отсутствие скрытых угроз — в системе не должно быть конфигураций ПО, активирующих не декларированные (скрытые) функции.

Нарушение любого из этих критериев может привести к серьезным материальным потерям. Для оценки рисков была создана специальная методика, состоящая из следующих шагов:

- Составление списка штатных функций системы;
- Анализ потенциального ущерба от нарушения каждой штатной функции;
- Выявление всех скрытых функций;
- Оценка возможных последствий активации скрытых функций;
- Составление перечня уязвимостей системы;
- Определение связи между уязвимостями и функциями (как штатными, так и скрытыми);
- Комплексный анализ потенциального ущерба от всех выявленных рисков.

По результатам анализа формируются специальные таблицы, которые помогают:

- Оценить общий уровень риска;
- Выявить наиболее критические уязвимости;
- Определить приоритеты в устранении угроз;
- Сфокусироваться на проблемах с максимальным риском.

Такой подход позволяет системно подойти к оценке киберустойчивости и эффективно управлять рисками информационной безопасности.

Методика оценки защищенности организаций от кибератак, связанных с недопустимыми событиями (НС)

Positive Technologies [8] создала специальный метод для оценки того, насколько хорошо организации защищены от кибератак, которые могут привести к серьезным проблемам в их работе. Недопустимое событие в данном случае — это результат хакерской атаки, из-за которого компания не может достичь своих главных целей или серьезно нарушает свою основную деятельность.

Чтобы оценить уровень защиты, сначала выявляются потенциальные недопустимые события, а затем проводятся имитации кибератак. После этого, используя модель потенциального нарушителя и результаты тестирования по шкале в 1000 баллов, определяется уровень защиты от внешних и/или внутренних угроз.

Для проведения оценки используются три типа метрик:

- Метрики достижений — показывают результаты работы на сетевом периметре или локальной сети, не связанные с реализацией недопустимых событий;
- Метрики реализации — отражают, насколько успешно достигаются ключевые цели работы и помогают собирать данные о результатах действий, связанных с недопустимыми событиями;
- Корректирующие коэффициенты — уточняют оценку защищенности с учетом особенностей процессов информационной безопасности и сложности проводимой атаки.

За каждый обнаруженный недостаток в системе безопасности компания получает штрафные баллы. Например, за обнаружение серьезной уязвимости в веб-приложениях начисляется 2 балла, а за нахождение нескольких способов обхода сетевой защиты — 6–7 баллов. Каждая из метрик включает частные метрики, рисунок 2.

Рис. 2. Метрики оценки киберустойчивости организации

Пример метрик достижения и полученные штрафные баллы представлен в таблице 2.

Пример метрик реализации НС и полученных штрафных баллов представлен в таблице 3.

Таблица 2.
Метрики-достижения и штрафные баллы (пример)

Метрика	Результат		Количество баллов
Выявление уязвимостей на сетевом периметре	Удалось выявить уязвимости высокого или критического уровня по шкале Common Vulnerability Scoring System (CVSS) в веб-приложениях и (или) их компонентах?	Да	2
		Нет	0
	Удалось выявить уязвимости высокого или критического уровня по шкале CVSS в сервисах удаленного доступа (например, SSH, VPN, RDP)?	Да	2
		Нет	0

Таблица 3.
Метрики реализации НС и штрафные баллы

Метрика	Результат		Количество баллов
Сбор информации о целевых системах	Удалось получить доступ к любым ресурсам, на которых обрабатывается (хранится) документация с информацией о целевых системах?	Да	1
		Нет	0
	Удалось получить доступ к рабочим местам или серверам, с которых возможно подключение к целевым системам?	Да	1
		Нет	0
	Удалось ли получить учетные данные для доступа к целевым системам?	Да	1
		Нет	0
	Удалось получить доступ к рабочим местам пользователей, отвечающих за администрирование целевых систем?	Да	2
		Нет	0

Пример метрик Корректирующие коэффициенты представлен в таблице 4.

В процессе оценки безопасности организации по различным показателям производится начисление баллов. Для определения общего уровня киберустойчивости (защищенности) организации применяется следующая формула расчета ОПР:

$$ОПР=(NMAX–NФАКТ)\times K1\times K2\times...\times KX\times NMAX1000+D$$

$$ОИТОГ=min(1000; ОПР)$$

где: NMAX — предельное количество штрафных баллов, которое может быть начислено организации во время проведения аудита;

Таблица 4.
Корректирующие коэффициенты и их значения

Метрика	Результат	Значение
Обход средств защиты	Средства защиты не обнаружены или их наличие не оказало какого-либо существенного влияния на проведение атак	0,9
	Наличие средств защиты замедлило или осложнило развитие векторов атаки, потребовалось использовать техники их обхода	0,95
	Наличие средств защиты заблокировало развитие векторов атаки, пришлось искать альтернативные системы для взлома	1
Обход правил фильтрации сетевого трафика между сегментами сети	Правила фильтрации сетевого трафика между сегментами сети не препятствовали развитию векторов атаки	0,8
	Обход правил фильтрации сетевого трафика между сегментами сети усложнил ход работ, но в итоге удалось реализовать НС	0,9
	Реализовать НС не удалось из-за ограничений фильтрации сетевого трафика между сегментами сети	1

NФАКТ — реальное количество набранных штрафных баллов;

K1×K2×...×KX=KKOPP — комплекс корректировочных коэффициентов;

D — временной промежуток до наступления первого инцидента в хронологическом порядке.

Показатель NMAX определяется исходя из специфики инфраструктуры организации (наличие доменной структуры) и результатов тестирования (успешность преодоления сетевого периметра и получения доступа к локальной вычислительной сети).

По итогам оценки используется шестиуровневая система градаций, установленная на основе экспертного мнения:

- Высокий уровень — 851–1000 баллов;
- Выше среднего — 651–850 баллов;
- Средний уровень — 501–650 баллов;
- Ниже среднего — 301–500 баллов;
- Низкий уровень — 51–300 баллов;
- Крайне низкий — 0–50 баллов.

Каждый диапазон баллов отражает определенный уровень киберустойчивости организации, что позволяет объективно оценить состояние информационной безопасности.

Анализ инструментов, используемых для оценки уровня киберустойчивости на примере навигатора киберустойчивости MaxPatrol Carbon

Решение задач по обеспечению кибербезопасности возложено на инструмент MaxPatrol Carbon от Positive Technologies [9]. Данное решение позволяет не только устанавливать необходимые требования к инфраструктуре, но и контролировать их выполнение для эффективного выявления и пресечения действий злоумышленников. Ключевая особенность продукта заключается в обеспечении киберустойчивости организации — её способности сохранять работоспособность бизнес-процессов и ИТ-инфраструктуры под воздействием кибератак.

По утверждению разработчиков, оценка уровня киберустойчивости является ключевым фактором успешной реализации комплексной защиты. Это достигается за счет поддержания постоянного состояния готовности организации к отражению кибератак и обеспечения бесперебойного функционирования всех систем.

Эффективность защиты определяется способностью системы быстро обнаруживать и нейтрализовать угрозы. Для количественной оценки киберустойчивости применяются две основные метрики: TTR (time to response, t_1) — время обнаружения и пресечения атаки, и TTA (time to attack, t_2) — время, за которое злоумышленник достигает своей цели. При условии, что t_1 меньше t_2, организация существенно снижает риски потенциальных потерь и ущерба от кибератак, рисунок 3.

Этот метод, разработанный компанией Хардкор-ИТ, направлен на существенное замедление действий атакующих (параметр TTA — время атаки) для того, чтобы специалисты по кибербезопасности получили достаточно времени на обнаружение и устранение угрозы (параметр TTR — время реагирования).

Успешность применения данного подхода определяется соотношением этих временных показателей: если время атаки (TTA) меньше времени реагирования (TTR), то атака считается успешной для злоумышленников. Таким образом, основная задача заключается в том, чтобы добиться ситуации, когда TTR становится меньше TTA, что обеспечивает эффективную защиту от APT-угроз (целенаправленных длительных атак).

Методика оценки защищенности организаций от кибератак, связанных с использованием фреймворка

Российская компания Innostage представила исследование [10], в котором аргументирует потребность в создании универсального подхода к оценке киберустойчивости организации. Разработанный методологический фреймворк, по замыслу авторов, должен состоять из пяти последовательных этапов.

Фреймворк представляет собой комплексный инструментарий, включающий набор правил, шаблонов и методических материалов для создания решений в сфере кибербезопасности и смежных областях.

Структура компании в рамках данной методологии разделена на два ключевых модуля:

Модуль обработки — объединяет компоненты, связанные с управлением, обнаружением угроз и операционной деятельностью.

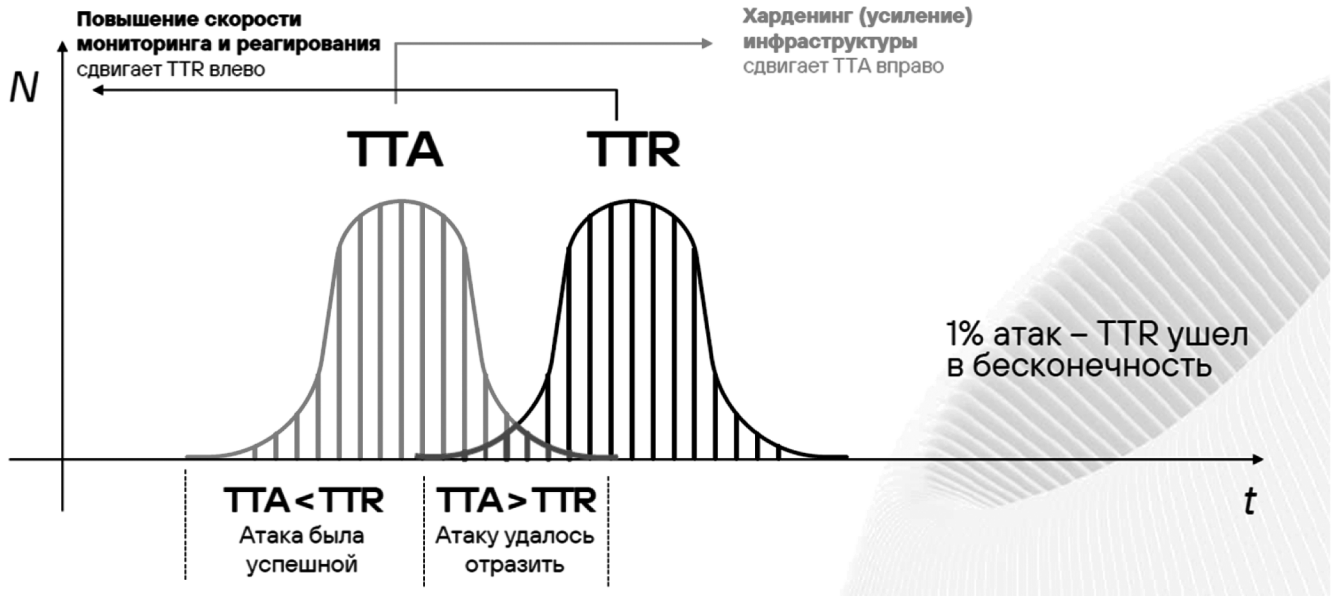

Рис. 3. Соотношение времени реализации атаки TTA и времени обнаружения и остановки атаки TTR

Системный модуль — включает программное обеспечение, аппаратные компоненты, сетевое оборудование и инфраструктуру

Каждый элемент системы характеризуется определенным набором атрибутов, которые оцениваются по четырехбалльной шкале. Показатели киберустойчивости классифицируются по четырем уровням, рисунок 4:

- Первоначальный;
- Определенный;
- Основной;
- Стандартный.

Используемые инструменты позволяют проводить количественную оценку текущих показателей кибербезопасности и сравнивать их с базовыми или эталонными значениями, что дает возможность объективно оценивать уровень защищенности организации.

Достигнутый уровень киберустойчивости визуализируется с помощью лепестковых диаграмм. Этот способ является эффективным инструментом визуализации уровня киберустойчивости организации. Данный метод позволяет наглядно сравнить текущие показатели с тремя ключевыми уровнями, рисунок 5:

- Базовый уровень — минимальный набор требований к киберустойчивости, необходимый для функционирования организации;
- Стандартный уровень — общепринятые отраслевые нормы и требования по киберустойчивости;
- Показатели бенчмарков (эталонный) — результаты эталонных тестов, демонстрирующие лучшие практики в области киберустойчивости.

Визуализация на лепестковой диаграмме представляет собой:

- Каждый параметр киберустойчивости отображается как отдельный луч;
- Значения параметров соединяются линиями, образуя «лепестки»;
- Различные уровни (базовый, стандартный, бенчмарк) отображаются разными цветами;
- Текущие показатели организации наносятся на диаграмму для сравнения.

Преимущества такого подхода:

- Наглядное представление многомерных данных;

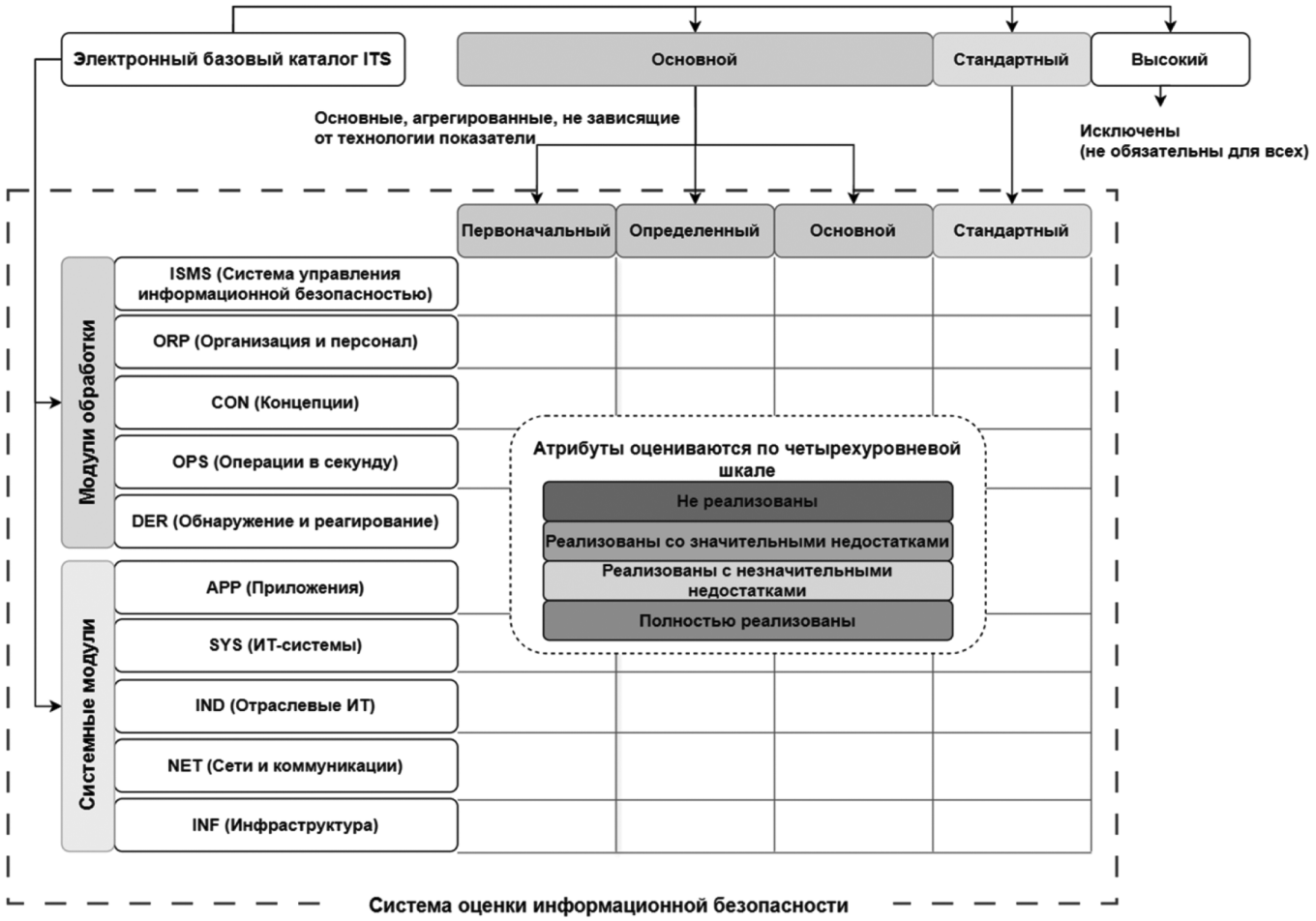

Рис. 4. Фреймворк оценки киберустойчивости компаний

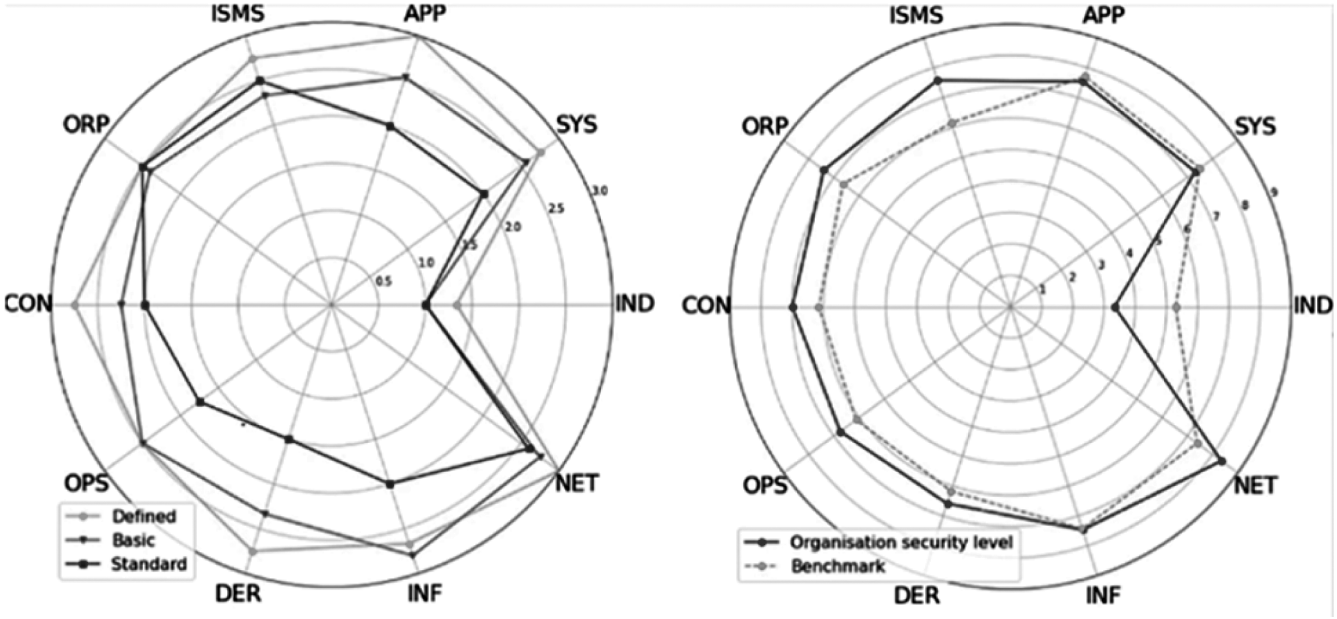

Рис. 5. Результаты сравнения достигнутого уровня киберустойчивости с базовым и стандартным уровнями (слева), а также с показателями эталонных тестов (бенчмарков) справа

- Возможность быстрого сравнения различных показателей;
- Визуализация пробелов между текущими и целевыми значениями;
- Простота интерпретации результатов для всех заинтересованных сторон.

Такой метод визуализации позволяет не только оценить текущий уровень киберустойчивости, но и определить приоритетные направления для улучшения, а также отслеживать динамику изменений в процессе совершенствования системы киберзащиты.

Подход обеспечения необходимого уровня киберустойчивости на основе построения Центра киберустойчивости

В работе [11] показано, что в банковской сфере проблема киберустойчивости является достаточно актуальной, что подтверждается множеством исследований. Ключевым документом, на который опираются специалисты, является руководство IOSCO по устойчивости финансового рынка к угрозам кибербезопасности, разработанное в 2016 году.

В настоящее время в организациях наблюдается фрагментация систем управления:

- Система управления качеством;
- Система управления кибербезопасностью;
- Система управления непрерывностью бизнеса.

Основной недостаток текущей системы заключается в отсутствии интеграции между этими процессами, что приводит к разрыву в передаче данных между различными подразделениями.

Для устранения существующих противоречий предлагается разработать единую методологию на основе следующих документов:

- Руководство IOSCO по киберустойчивости финансовых рынков (2016);
- Специальная публикация NIST 800–160 Volume 2 (2018);
- Международный стандарт ISO/IEC 27001:2016.

Соответственно Центр киберустойчивости должен обеспечивать выполнение следующих ключевых функций, рисунок 6:

- Интеграция процессов непрерывности бизнеса, отказоустойчивости ИТ-инфраструктуры и кибербезопасности в единый процесс;
- Разработка сценариев реагирования на инциденты и оценка рисков снижения киберустойчивости;
- Проведение учений и тренировок персонала;
- Внедрение единой системы управления инцидентами;
- Разработка и мониторинг планов развития методов и средств обеспечения киберустойчивости.

Такой комплексный подход позволит создать эффективную систему защиты, где все компоненты будут работать согласованно, обеспечивая высокий уровень киберустойчивости организации.

Полученные результаты

В процессе проведенного исследования была осуществлена детальная оценка современных методик и моделей, применяемых для измерения интегрального индекса киберустойчивости, включающего параметры

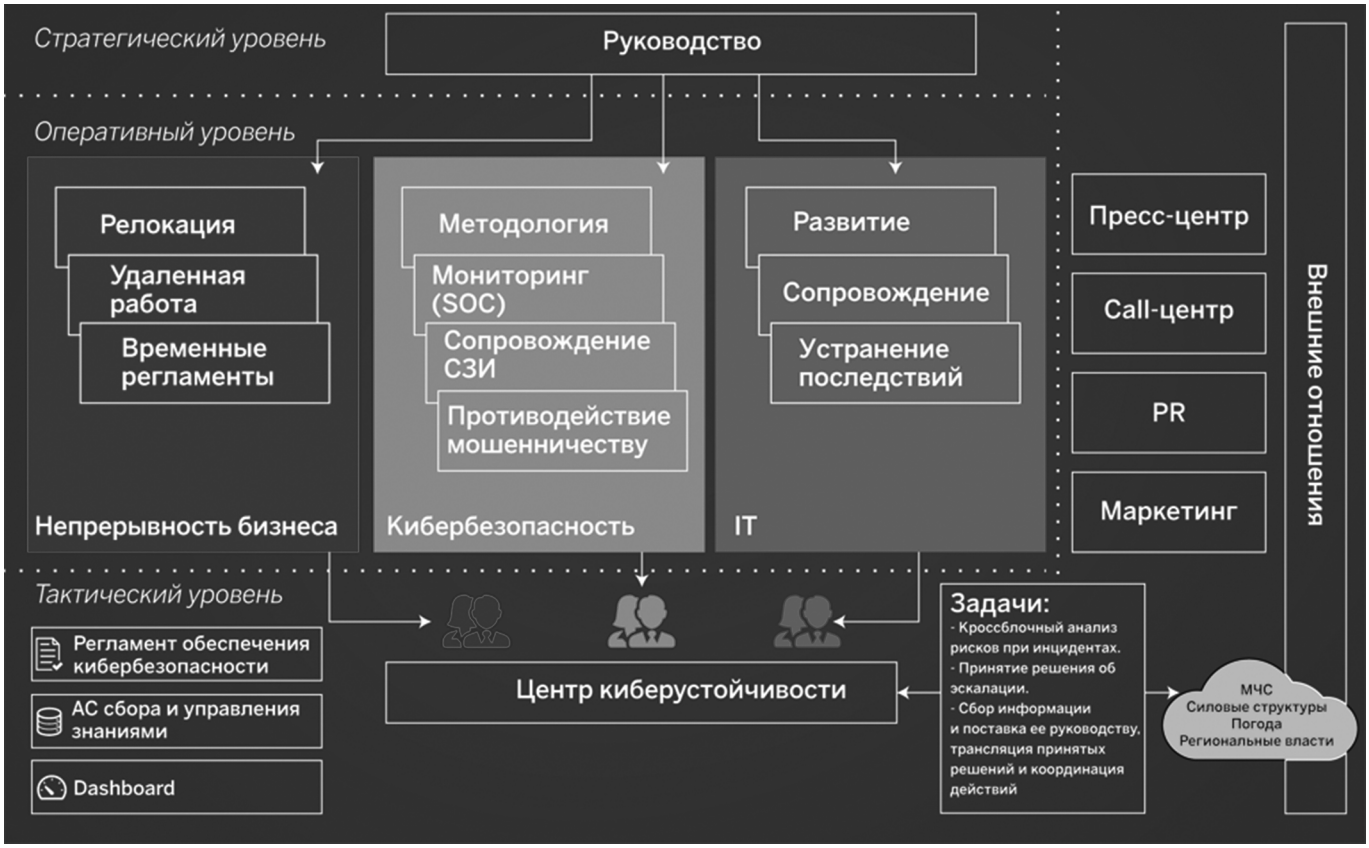

Рис. 6. Структурная схема центра киберустойчивости

кибербезопасности, отказоустойчивости и бизнес-непрерывности.

Результаты анализа продемонстрировали отсутствие единой признанной методологии для оценки киберустойчивости. На сегодняшний день исследования в данной области носят разрозненный характер и охватывают лишь отдельные аспекты проблемы.

В ходе работы были определены фундаментальные принципы обеспечения киберустойчивости и составлен подробный план необходимых мероприятий. Предложен комплекс технических и организационных решений, охватывающих административные, технические, программно-аппаратные и этические аспекты. Разработаны конкретные подходы к реализации мер безопасности как до, так и после кибератак на инфраструктуру [13–14].

Отдельные разработчики предлагают систему метрик, основанную на штрафных баллах для вычисления общего уровня защищенности. При этом более высокая киберустойчивость коррелирует с меньшим количеством штрафных очков.

Доказана необходимость создания специализированного центра киберустойчивости, который будет координировать все функции по обеспечению безопасности организации. Особое внимание заслуживает работа российской компании Innostage, где ведется разработка уникального фреймворка для оценки киберустойчивости. Данный инструмент предусматривает структурированное описание процессов и стандартизацию процедур оценки уровня киберустойчивости с последующим сравнением полученных результатов с базовыми, стандартными показателями и эталонными тестами.

Заключение

В настоящее время активно ведется работа по созданию и обоснованию систем количественных показателей. Без наличия четких числовых критериев становится невозможным проводить сравнительный анализ, оптимизировать рабочие процессы и принимать эффективные меры для достижения желаемого состояния организации.

Проведенный анализ показал существенные пробелы в существующих методиках: отсутствуют четко проработанные метрики, критерии и показатели для полноценного анализа и оценки уровня киберустойчивости компании. Для решения этой актуальной задачи необходима разработка специального математического инструментария, который позволит создать эффективные модели оценки киберустойчивости и выработать оптимальные управленческие решения в данной области.

ЛИТЕРАТУРА

1. Кибербезопасность 2022–2023. Тренды и прогнозы [Электронный ресурс]. -Российский рынок кибербезопасности может вырасти в 2,5 раза к 2026 году. [Электронный ресурс]. -NIST Releases SP 800-160 Vol. 2: Developing Cyber Resilient Systems — A Systems Security Engineering Approach [Электронный ресурс]. Режим доступа https://csrc.nist.gov/News/2019/sp-800-160-vol2-developing cyber-resilient-systems (дата обращения: 25.12.2024).
2. ГОСТ Р 53647.2–2009 Менеджмент непрерывности бизнеса. Часть 2. Требования.
3. Богомаз М. Отказоустойчивая IT инфраструктура: принципы и способы организации [Электронный ресурс] https://timeweb.cloud/tutorials/servers/otkazoustojchivaya-it-infrastruktura?ysclid=m60vpzcbz672207437 (дата обращения: 04.03.2025).
4. Модель управления устойчивостью CERT Resilience Management Model [Электронный ресурс]. Режим доступа: ttps://insights.sei.cmu.edu/library/cert-resilience-managementmodel-cert-rmm-version-12/ (дата обращения: 12.04.2025).
5. Методика оценки киберустойчивости / Труды 7-й международной конференции «Управление развитием крупномасштабных систем» (MLSD-2013, Москва). М.: ИПУ РАН, 2013. Т. II. С. 193–200
6. Методика оценки защищенности организаций от кибератак [Электронный ресурс]. Режим доступа: https://pt-rezbez.storage.yandexcloud.net/Metodika_oczenki_zashhishhennosti_organizaczij_ot_kiberatak_666990ec6a.pdf (дата обращения: 12.04.2025).
7. Обзор MaxPatrol Carbon, российского навигатора по киберустойчивости [Электронный ресурс]. Режим доступа: https://www.anti-malware.ru/reviews/MaxPatrol-Carbon (дата обращения: 12.04.2025).
8. Новиков И. Innostage разрабатывает методику оценки киберустойчивости компаний [Электронный ресурс]. Режим доступа: https://www.anti-malware.ru/analytics/ Technology_Analysis/Innostage-Cyber-Resilience (дата обращения: 12.04.2025).
9. Маркин Д. Киберустойчивость — что это такое и как ее достичь? Банковское обозрение. №10 (237)/2018 [Электронный ресурс]. Режим доступа https://bosfera.ru/bo/kiberustoychivost-chto-eto-takoe-i-kak-ee-dostich (дата обращения: 12.04.2025).
10. Петров Л.Ф. Нелинейные модели в экономических и социальных исследованиях. Вестник Российского экономического университета имени Г.В. Плеханова. 2022;(4):23-31. https://doi.org/10.21686/2413-2829-2022-4-23-31
11. Суздальский Д.А. Применение нечетких когнитивных карт в условиях принятия решений для обеспечения информационной безопасности / Д.А. Суздальский // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. — 2024. — № 3. — С. 113–117. — DOI 10.37882/2223–2966.2024.03.33. — EDN GZXDKL.
12. Суздальский Д.А. Оптимизация оценки риска для поддержки принятия решений с использованием интеллектуальной модели, основанной на нечетких логических выводах возобновляемых правил / Д.А. Суздальский // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. — 2024. — № 6. — С. 121–127. — DOI 10.37882/2223–2966.2024.06.36. — EDN DEIZSW.

Журнал «Современная наука: актуальные проблемы теории и практики»