DOI 10.37882/2223-2966.2025.06.43

ОБОСНОВАНИЕ ЦЕЛЕСООБРАЗНОСТИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ НА ОСНОВЕ КОМПЛЕКСНОГО ПОКАЗАТЕЛЯ КИБЕРУСТОЙЧИВОСТИ

SUBSTANTIATION OF THE EXPEDIENCY OF ASSESSING THE SECURITY OF INFORMATION INFRASTRUCTURE BASED ON A COMPREHENSIVE CYBER RESILIENCE INDICATOR

D. Suzdalsky

Summary. The article substantiates the expediency of assessing the security of the information infrastructure based on a comprehensive cyber resilience indicator, analyzes the problem of creating a reliable enterprise information system capable of stable operation even with regular cyber-attacks. The concepts of cyber resilience and cybersecurity are discussed in detail, and key aspects of their practical application are described. The paper discusses in detail the basic principles, objectives, specific tasks, and tools necessary to ensure the sustainable functioning of information systems. Special attention is paid to the study of official documents that define the relationship between such concepts as cyber resilience, cybersecurity, business continuity and system fault tolerance. The study found that cyber resilience issues are a complex interdisciplinary field that requires an integrated approach to solving many interrelated tasks. An important conclusion of the work is that there is currently no universal methodological approach to ensuring cyber resilience, which would include a complete set of necessary methods, models, and algorithms for effective protection of information systems.

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

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

Аннотация. В статье обоснована целесообразность оценки безопасности информационной инфраструктуры на основе комплексного показателя киберустойчивости, анализируется проблема создания надежной информационной системы предприятия, способной стабильно работать даже при регулярных кибератаках. Подробно разбираются понятий киберустойчивости и кибербезопасности, а также описывают ключевые аспекты их практического применения. В работе детально рассматриваются базовые принципы, целевые установки, конкретные задачи и инструменты, необходимые для обеспечения устойчивого функционирования информационных систем.
Особое внимание уделяется изучению взаимосвязи между такими понятиями как киберустойчивость, кибербезопасность, непрерывность бизнес-процессов и отказоустойчивость систем.
В ходе исследования установлено, что вопросы киберустойчивости представляют собой комплексную междисциплинарную область, требующую комплексного подхода к решению множества взаимосвязанных задач.

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

Введение

В области информационной защиты наблюдается существенная смена терминологии: привычные термины информационной безопасности активно заменяются понятиями кибербезопасность и киберустойчивость.

Данный сдвиг в терминологии связан с возрастающей значимостью защиты цифровых систем — от малых локальных сетей до глобальной интернет-структуры. Добавление префикса «кибер-» подчеркивает непосредственную связь с цифровыми технологиями и виртуальной средой.

Кибербезопасность представляет собой многоуровневую защиту информационных систем от разнообразных угроз, которые могут исходить как от внешних, так и от внутренних источников в организации. Профессиональному сообществу необходимо решить две ключевые задачи: во-первых, упорядочить новую терминологию, во-вторых, обеспечить корректное понимание и эффективное использование этих терминов специалистами по информационной защите.

Для достижения этих целей требуется не просто обновление профессиональной терминологии, но и четкое определение места новых понятий в работе экспертов по информационной безопасности. Анализ направлен на доказательство необходимости оценки комплексного показателя киберустойчивости, включающего аспекты кибербезопасности, отказоустойчивости и непрерывности бизнес-процессов, рисунок 1.

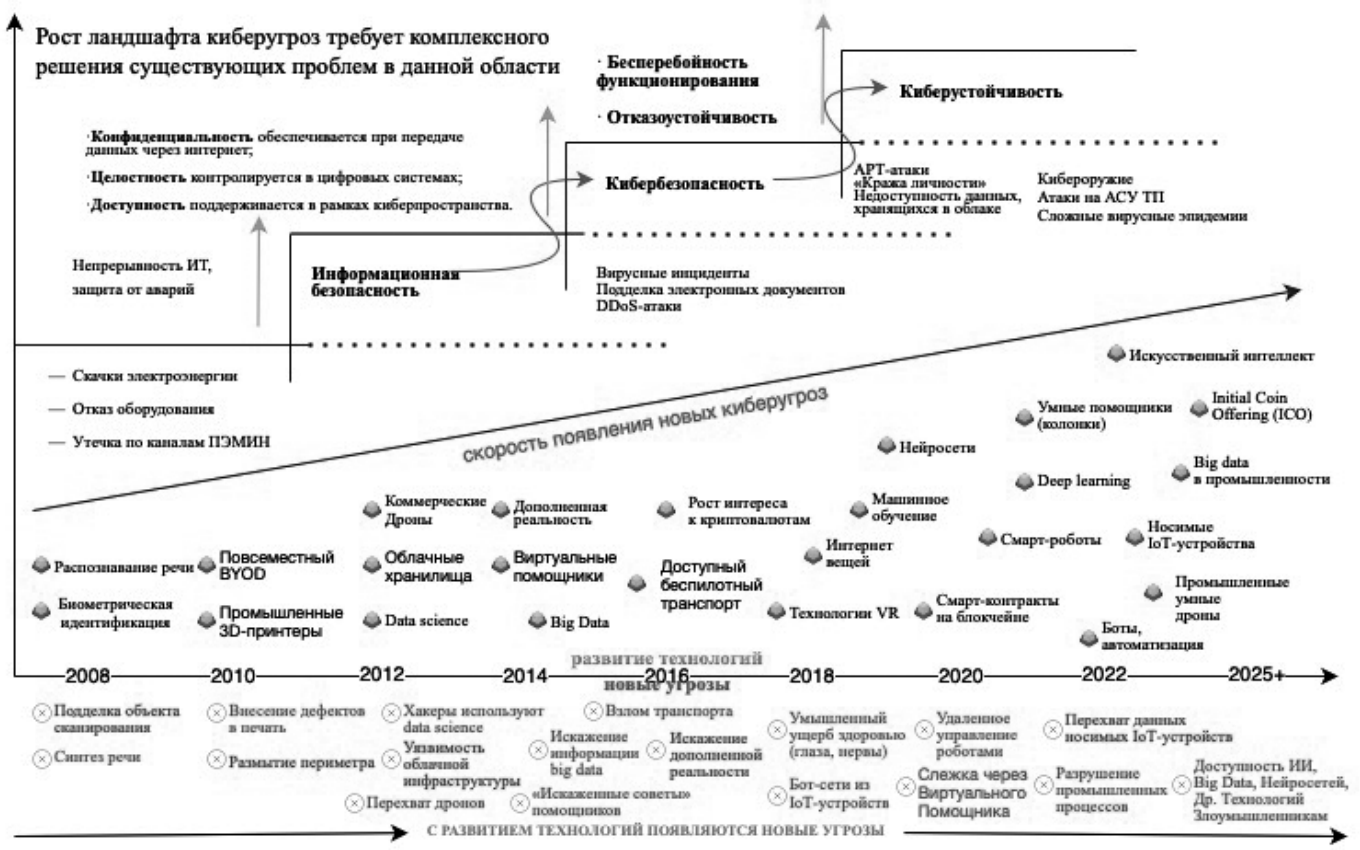

Рис. 1. Изменение ландшафта киберугроз

Киберпространство рассматривается как триединая система, объединяющая информацию, техническую инфраструктуру, программное обеспечение и процессы информационного взаимодействия между участниками. Киберустойчивость определяется как мультидисциплинарное направление, для которого разработана специальная методология, включающая конкретные цели, задачи и практические мероприятия по ее реализации.

Цель анализа обосновать целесообразность оценки комплексного показателя киберустойчивости (показатели кибербезопасности, отказоустойчивости и непрерывности бизнеса).

Киберустойчивость как междисциплинарное направление

Согласно международному стандарту ISO 27032 «Кибербезопасность — Руководство по безопасности в Интернете» (2023 год), существует четкая взаимосвязь между понятиями информационной безопасности и кибербезопасности [3].

Кибербезопасность определяется как один из компонентов более широкой области информационной безопасности. Её основная задача заключается в защите различных субъектов — от отдельных людей до целых государств — от различных киберугроз. Достигается это путем эффективного управления киберрисками и поддержания их на допустимом уровне.

Таким образом, кибербезопасность можно рассматривать как специализированное направление в рамках информационной безопасности, которое фокусируется именно на защите от цифровых угроз в онлайн-пространстве, в то время как информационная безопасность охватывает более широкий спектр защитных мер в отношении информации и информационных систем, рисунок 2. Кибербезопасность и информационная безопасность имеют существенные различия в области применения своих принципов.

Если информационная безопасность обеспечивает комплексную защиту информации во всем информационном пространстве, где происходит её создание, преобразование, передача и использование, то кибербезопасность фокусируется исключительно на защите в рамках киберпространства.

Основные принципы защиты информации (конфиденциальность, целостность и доступность) в случае кибербезопасности реализуются только в цифровой среде. Это означает, что:

- Конфиденциальность обеспечивается при передаче данных через интернет;
- Целостность контролируется в цифровых системах;

- Доступность поддерживается в рамках киберпространства.

В то время как информационная безопасность охватывает более широкий спектр: защиту бумажных носителей; физическую защиту информационных систем; контроль доступа к информационным ресурсам вне цифровой среды; защиту при непосредственном обмене информацией между людьми.

Таким образом, кибербезопасность является специализированным направлением в структуре информационной безопасности, сфокусированным исключительно на защите информации в цифровой среде [1].

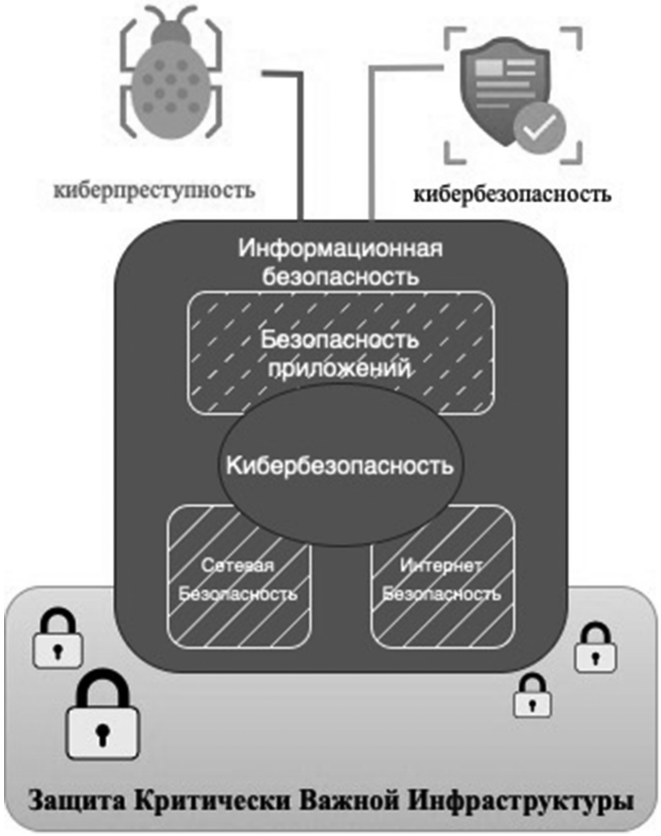

Рис. 2. Взаимосвязи между информационной безопасностью и кибербезопасностью

Киберпространство представляет собой особую сферу деятельности в рамках более широкого информационного пространства. Это комплексная система, которая включает в себя несколько ключевых компонентов:

- Коммуникационные каналы — интернет и другие телекоммуникационные сети, обеспечивающие передачу информации;
- Технологическая инфраструктура — все технические средства и системы, необходимые для функционирования коммуникационных каналов;
- Человеческая активность — любые формы деятельности пользователей, организаций и государства, осуществляемые через цифровые каналы связи.

Важно отметить, что киберпространство охватывает не только технические аспекты (сети и оборудование), но и всю совокупность действий, которые люди, организации и государственные структуры осуществляют в цифровой среде. Это делает его уникальной средой, где происходит взаимодействие между различными участниками информационного обмена.

Таким образом, киберпространство можно рассматривать как цифровую экосистему, объединяющую технические возможности и человеческую деятельность в едином информационном пространстве.[4].

Киберпространство как сложная система состоит из трех взаимосвязанных компонентов:

1) Информационный компонент включает: данные в цифровом формате; цифровые документы и файлы; электронные сообщения; мультимедийный контент; базы данных.
2) Технический компонент охватывает: физическую инфраструктуру (серверы, сети, каналы связи); информационные технологии; программное обеспечение; вычислительные системы; сетевое оборудование.
3) Социальный компонент представляет: информационное взаимодействие между пользователями; коммуникационные процессы; цифровые сервисы и платформы; электронное документооборот; виртуальные сообщества.

Все эти компоненты образуют единую экосистему, где информация циркулирует между участниками, техническая инфраструктура обеспечивает её передачу и обработку, а социальное взаимодействие определяет цели и способы использования информационных ресурсов. Важно понимать, что эти компоненты неразрывно связаны между собой. Без технической инфраструктуры невозможно существование информации в цифровом виде. Без информационного наполнения техническая инфраструктура теряет смысл. Без социального компонента отсутствует цель создания и использования киберпространства.

Таким образом, киберпространство представляет собой целостную систему, где все компоненты взаимосвязаны и взаимозависимы, образуя единую среду для цифрового взаимодействия.

Иными словами, киберпространство представляет собой триаду: информацию; техническую инфраструктуру, информационные технологии, программное обеспечение и информационное взаимодействие субъектов, рисунок 3.

Согласно международному стандарту [5] составляющими кибербезопасности являются: Интернет-безопас-

ность, включающая Веб-безопасность и Сетевая безопасность, рисунок 4.

Интернет-безопасность представляет собой комплекс мер, направленных на обеспечение безопасного и надежного предоставления услуг законным пользователям сети. Это более широкое понятие, охватывающее все аспекты защиты при работе в интернете.

Веб-безопасность является частью интернет-безопасности и фокусируется на обеспечении безопасного доступа к зарегистрированным общедоступным URL-

Рис. 3. Триада киберпространства

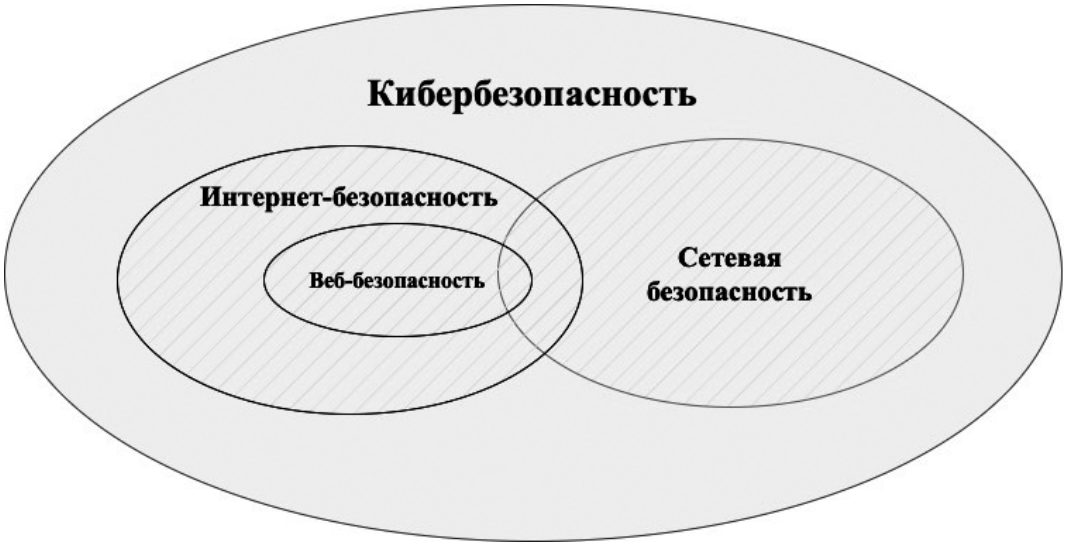

Рис. 4. Составляющие кибербезопасности

адресам через HTTP-соединение. Существует несколько основных методов передачи данных: веб-браузеры — основной инструмент для доступа к веб-сайтам через HTTP/HTTPS протоколы; электронная почта — система обмена сообщениями между пользователями; FTP (File Transfer Protocol) — протокол передачи файлов; мессенджеры — сервисы мгновенного обмена сообщениями. HTTP-соединение является основным каналом передачи данных в вебе.

Для обеспечения безопасности используются следующие механизмы: SSL/TLS-шифрование — защита передаваемых данных; аутентификация — проверка подлинности пользователей; авторизация — контроль доступа к ресурсам; защита от атак — предотвращение различных видов угроз. Целостность данных — обеспечение неизменности передаваемой информации.

Веб-безопасность играет критически важную роль в современном интернете, поскольку большинство онлайн-сервисов и приложений используют веб-технологии для взаимодействия с пользователями.

Сетевая безопасность представляет собой комплекс мер, направленных на защиту компьютерных сетей и информации от различных угроз. Она охватывает все типы сетей, существующих в организации: локальные сети (LAN); глобальные сети (WAN); персональные сети (PAN); беспроводные сети (WLAN). Основные задачи сетевой безопасности:

- Предотвращение несанкционированного доступа в сеть;
- Своевременное обнаружение угроз (вредоносные программы, аномальная активность);
- Эффективное реагирование на инциденты безопасности;
- Защита данных от утечки;
- Обеспечение целостности информации.

Ключевые принципы защиты:

- Многоуровневая защита — создание нескольких слоев обороны против злоумышленников;
- Минимальные права доступа — пользователи и программы получают доступ только к необходимым ресурсам;
- Регулярные обновления — своевременное обновление программного обеспечения для устранения уязвимостей;
- Постоянный мониторинг — контроль событий в сети.

Основные технологии защиты:

- Межсетевые экраны (firewall) для фильтрации трафика;
- VPN-технологии для создания защищенных каналов связи;
- Шифрование данных для защиты передаваемой информации;
- Системы контроля доступа для разграничения прав пользователей;
- Мониторинг уязвимостей для выявления и устранения слабых мест.

Правильная организация сетевой безопасности позволяет защитить корпоративные данные от кибератак, предотвратить финансовые потери, сохранить репутацию компании, снизить риски юридических последствий, обеспечить бесперебойную работу IT-инфраструктуры.

Организационные меры:

- Обучение персонала правилам кибербезопасности;
- Создание команды реагирования на инциденты;
- Разработка политики безопасности;
- Проведение регулярных аудитов безопасности;
- Тестирование на проникновение (пентесты).

Комплексная реализация всех перечисленных мер позволяет создать надежную систему защиты сетевой инфраструктуры организации от современных киберугроз.

Кибербезопасность обеспечивает защиту от кибератак, под которыми понимается попытка выведения компьютерной системы из строя или хищения информации за счёт уязвимостей в технических средствах или программном обеспечении. Примеры наиболее распространенных кибератак представлены в Библиотеке знаний по кибербезопасности «Кибрарий» [5]: заражение вредоносным программным обеспечением (ПО); DDoS-атаки; фишинг; атаки на цепочку поставок; атаки «человек посередине»; целевые атаки и др. внешних воздействий. Киберустойчивость представляет собой способность информационных систем осуществлять свое штатное (целевое) функционирование в условиях воздействия компьютерных атак в киберпространстве. В терминах общей теории управления кибератаки представляют собой возмущающее воздействие, система управления объектом должна компенсировать эти возмущения, а в целом (объект + система управления) должны обладать устойчивостью к этим возмущениям, т.е. быть киберустойчивыми (cyber resistant).

В одной из первых отечественных фундаментальных работ, посвященной киберустойчивости цифровой экономики [6] дается следующее определение киберустойчивости с учетом целеполагания защищаемой кибернетической системы — Киберустойчивость (Cyber Resilience) —«способность киберсистемы, функционирующей по определенному алгоритму, достигать цели функционирования в условиях информационно-технических воздействий злоумышленников». В документе

«Разработка киберустойчивых систем: подход к инженерии системной безопасности» Национального института по стандартизации и технологиям США [7] представлено схожее определение. Под киберустойчивостью понимается «способность предвидеть, противостоять, восстанавливаться и адаптироваться к нагрузкам, атакам или компрометациям систем, которые используют или активируются киберресурсами». Необходимо учитывать, что киберустойчивость — это не разовое достижение определенного состояния, а непрерывный процесс совершенствования защитных механизмов и адаптации к постоянно меняющемуся ландшафту киберугроз.

В англоязычной литературе употребляются термины Cyber Resilience или Cyber Sustainability. Киберустойчивости посвящено значительное количество работ. В настоящее время в условиях высокого уровня киберугроз требуется обеспечение не только безопасного, но непрерывного и устойчивого функционирования информационной инфраструктуры. В современных условиях проблема киберустойчивости информационных систем становится все более значимой областью исследований. Это обусловлено необходимостью не просто обеспечить безопасность информационных систем, но гарантировать их непрерывное и устойчивое функционирование даже при высоком уровне киберугроз.

Особую актуальность данному направлению придает поддержка на государственном уровне. Это подтверждается включением задач по обеспечению киберустойчивости в:

- Национальный проект «Цифровая экономика»;
- Новый Национальный проект «Экономика данных и цифровая трансформация государства»;

Федеральный проект «Инфраструктура кибербезопасности» направлен на решение критически важных задач по обеспечению киберустойчивости цифровых платформ и экосистем, что особенно важно в условиях массированных и разнородных кибератак со стороны злоумышленников.

Существует ряд фундаментальных причин, обуславливающих необходимость развития данного направления:

- Структурная сложность современных информационных систем;
- Функциональная сложность интегрированных решений;
- Наличие потенциальных уязвимостей и «спящих» аппаратно-программных закладок;
- Недостаточная эффективность существующих моделей и методов обеспечения кибербезопасности;
- Ограниченность применяемых средств защиты информации.

Все эти факторы создают необходимость в разработке новых подходов к обеспечению киберустойчивости информационных систем и требуют комплексного решения существующих проблем в данной области. В работе [6] показано, что киберустойчивость представляет собой мультидисциплинарное направление, которое охватывает самые разные предметные области, рисунок 5.

В рамках решения задач управления информационными рисками выделяют три ключевых задачи управления киберустойчивостью:

- Кибербезопасность — защита информационных активов от цифровых угроз и несанкционированного доступа;
- Отказоустойчивость — способность информационной инфраструктуры сохранять работоспособность при сбоях и отказах;
- Непрерывность бизнеса — обеспечение бесперебойной работы организации при различных инцидентах.

Отказоустойчивость является технической основой киберустойчивости и включает резервирование критически важных систем, дублирование каналов связи, автоматическое переключение на резервные мощности, мониторинг состояния инфраструктуры. Проблематика отказоустойчивости имеет прямое отношение к реализации бизнес-процессов компании. Конечные сервисы должны быть гарантированно доступны пользователю вне зависимости от того, что произошло с оборудованием. Т.е. отказоустойчивость — способность информационной системы сохранять работоспособность при выходе из строя отдельных компонентов или подсистем. Основной принцип заключается в том, что конечные сервисы должны оставаться доступными для пользователей независимо от проблем с оборудованием. Основные метрики оценки отказоустойчивости системы: вероятность безотказной работы — вероятность того, что система проработает заданное время без сбоев; коэффициент готовности — отношение времени бесперебойной работы к общему времени эксплуатации; среднее время между отказами — период между сбоями системы; среднее время восстановления — время, необходимое для устранения сбоя.

Система отказоустойчивости охватывает: отдельные компоненты — серверы, сетевые устройства, системы хранения данных; подсистемы — базы данных, приложения, сетевые сервисы; инфраструктура в целом — все элементы IT-системы предприятия. Основные механизмы обеспечения отказоустойчивости [7]:

- Резервирование компонентов — дублирование критически важных элементов системы;
- Кластеризация — объединение нескольких серверов для обеспечения непрерывной работы;
- Репликация данных — создание копий информации на разных носителях;

Рис. 5. Киберустойчивость как мультидисциплинарное направление

- Мониторинг состояния — постоянный контроль работоспособности всех элементов;
- Автоматическое переключение — мгновенный переход на резервные системы при сбоях.

Эффективная система отказоустойчивости обеспечивает: непрерывность бизнес-процессов; защиту критически важной информации; поддержание репутации компании; снижение финансовых потерь от простоев; соответствие требованиям регуляторов.

Под непрерывностью бизнеса согласно стандарту [8] понимают стратегическую и тактическую способность организации планировать свою работу в случае возникновения инцидентов и нарушений деятельности. Основная цель — обеспечение непрерывности деловых операций на установленном приемлемом уровне. Непрерывность бизнеса фокусируется на разработке планов восстановления деятельности, создании резервных площадок, подготовке персонала к действиям в кризисных ситуациях, тестировании планов восстановления. Ресурсы же, выделяемые на обеспечение непрерывности бизнеса, распределяются следующим образом:

- 60–80 % — организационные меры и разработка программы управления непрерывностью бизнеса
- 20–40 % — выбор и внедрение технических решений.

Менеджмент непрерывности бизнеса включает в себя идентификацию потенциальных угроз, разработку эффективных ответных мер, защиту интересов ключевых заинтересованных сторон, поддержание репутации организации, обеспечение восстановления деятельности. План обеспечения непрерывности бизнеса должен содержать документированные процедуры реагирования на инциденты, механизмы поддержания критически важных видов деятельности, сроки восстановления основных бизнес-процессов, учет потребностей вовлеченного персонала.

Таким образом для обеспечения надежной защиты современных организаций необходимо рассматривать киберустойчивость как многогранную проблему, требующую системного подхода. Три столпа киберустойчивости формируют основу комплексной защиты:

1) Защита информационных активов направлена на противодействие цифровым угрозам и включает:
- Создание многоуровневой системы защиты данных;
- Контроль доступа к информационным ресурсам;
- Защиту от вредоносного программного обеспечения;
- Обеспечение конфиденциальности передаваемой информации.

2) Надежность инфраструктуры обеспечивает бесперебойную работу систем через:
- Создание резервных мощностей;
- Разработку процедур восстановления после сбоев;
- Проведение регулярных стресс-тестов;
- Автоматизацию процессов реагирования на инциденты;
- Подготовку персонала к действиям в нештатных ситуациях.

3) Стабильность бизнес-функционирования гарантирует непрерывность работы организации посредством:
- Формирования стратегий управления рисками;
- Создания планов восстановления деятельности;
- Обеспечения постоянного информационного обмена;
- Защиты и регулярного резервирования данных;
- Поддержания высокого качества услуг.

Критерии оценки эффективности системы киберустойчивости должны учитывать:

- Скорость восстановления после нарушений;
- Процент предотвращенных кибератак;
- Количество устраненных уязвимостей;
- Эффективность работы систем резервирования;
- Уровень компетентности сотрудников в вопросах безопасности;
- Реализацию планов по обеспечению непрерывности работы.

Такой интегрированный подход позволяет не только своевременно выявлять и устранять угрозы, но и обеспечивать долгосрочную стабильность функционирования организации в условиях динамично развивающегося цифрового пространства. Регулярный мониторинг показателей и их корректировка в соответствии с изменяющейся обстановкой является ключевым фактором успешной реализации стратегии киберустойчивости.

Полученные результаты

В ходе исследования выявлена ключевая проблема современной кибербезопасности — отсутствие четких количественных показателей и метрик для оценки уровня киберустойчивости. Специалисты сталкиваются с необходимостью перехода от общих требований к конкретным измеримым параметрам, что становится все более актуальным в современных условиях. Отсутствие количественных оценок создает серьезные препятствия для сравнения различных систем безопасности, оптимизации существующих процессов, планирования перехода от текущего состояния к целевому.

Заключение

Киберустойчивость представляет собой комплексное понятие, включающее три основные составляющие: кибербезопасность, непрерывность бизнеса, отказоустойчивость

Обеспечение непрерывности бизнеса требует:

- Организационных мер — 60–80 %;
- Технических мер — 20–40 %.

Технические меры направлены на обеспечение функциональной устойчивости и отказоустойчивости информационной инфраструктуры. Проблематика киберустойчивости является междисциплинарным направлением, требующим решения взаимосвязанных задач. При этом на текущий момент отсутствует единая методология, включающая совокупность методов, математические модели, алгоритмы обеспечения киберустойчивости. Это создает значительные сложности для практической реализации мер по обеспечению необходимого уровня кибербезопасности и устойчивости бизнес-процессов.

ЛИТЕРАТУРА

1. Кибербезопасность 2022–2023. Тренды и прогнозы [Электронный ресурс]. — 2023. — URL: https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/?utm_source=yandex&utm_medium=cpc&utm_campaign=83387165-search-cyber-keywords&utm_content=5134114004-13515166514&calltouch_tm=yd_c:83387165_gb:5134114004_ad:13515166514_ph:43371020357_st:search_pt:premium_p:1_s:none_dt:desktop_reg:213_ret:43371020357_apt:none&_openstat=ZGlyZWN0LnlhbmRleC5ydTs4MzM4NzE2NTsxMzUxNTE2NjUxNDt5YW5kZXgucnU6cHJlbWl1bQ&yclid=11017443921774510079#id1 (дата обращения 18.05.2024).
2. Российский рынок кибербезопасности может вырасти в 2,5 раза к 2026 году. [Электронный ресурс]. — 2022. — URL: https://www.vedomosti.ru/business/news/2022/08/02/934195-rossiiskii-rinok-kiberbezopasnosti-mozhet-virasti (дата обращения 18.05.2024).
3. Международный стандарт ISO-IEC-27032–2023 Кибербезопасность — Руководство по безопасности в Интернете [Электронный ресурс] Режим доступа https://cdn.standards.iteh.ai/samples/76070/be57667fdd0b432490c253ca538c9938/IS O-IEC-27032-2023.pdf (Дата обращения 4.03.2025).
4. Проект концепции стратегии кибербезопасности РФ [Электронный ресурс] http://council.gov.ru/media/files /41d4b3dfbdb25cea8a73.pd (Дата обращения 4.03.2025).
5. Библиотека знаний по кибербезопасности «Кибрарий» [Электронный ресурс] Режим доступа: http://www.sberbank.ru/ru/person/kibrary/vocabulary/kiberataka (Дата обращения 4.03.2025).
6. Петренко С.А. Киберустойчивость цифровой экономики. Как обеспечить безопасность и непрерывность бизнеса. — СПб.: Питер, 2021. — 384 с.
7. 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).
8. ГОСТ Р 53647.2–2009 Менеджмент непрерывности бизнеса. Часть 2. Требования.

Журнал «Современная наука: актуальные проблемы теории и практики»