УДК 330.3

Носков И.А.,
студент,
4 курс, направление «Экономическая безопасность»
Уфимский университет науки и технологий
Научный руководитель: Ялтонская Д.И.,
ассистент,
Институт экономики и бизнеса
Уфимский университет науки и технологий
Россия, г. Уфа

КИБЕРУСТОЙЧИВОСТЬ: КРИТИЧЕСКИЙ ЭЛЕМЕНТ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ БИЗНЕСА В ЭПОХУ ПЕРМАНЕНТНЫХ КИБЕРУГРОЗ

Аннотация: *Статья посвящена исследованию концепции киберустойчивости как фундамента экономической безопасности современного бизнеса. В статье рассматриваются недостатки традиционных защитных барьеров и доказывается необходимость перехода к стратегии быстрого восстановления после атак. Автором представлен четкий план построения системы киберустойчивости, а также проведен анализ громких кибератак в России с оценкой нанесенного ущерба. Особое место в работе занимает вопрос применения искусственного интеллекта для атоматизации реагирования и защиты от угроз.*

Ключевые слова: *Киберустойчивость, экономическая безопасность бизнеса, инвестиции, стратегический подход.*

Annotation: *The article is devoted to the study of the concept of cyber resilience as the foundation of economic security for modern businesses. The article examines the disadvantages of traditional protective barriers and proves*

the need to switch to a strategy of rapid recovery after attacks. The author presents a clear plan for building a cyber resilience system and analyzes high-profile cyberattacks in Russia, assessing the damage caused. The article also focuses on the use of artificial intelligence for automating response and protection against threats.

***Keywords**: Cyber resilience, economic security of business, investments, strategic approach.*

Сегодняшний технологичный мир характеризуется тем, что киберпреступления происходят не в отдаленном будущем, а являются неизбежностью. Устаревшие методы обеспечения информационной защищенности, основанные лишь на создании надежных барьеров, оказываются бессильными против сложных и постоянных атак. Вместо принципа безусловной защиты возникает новый, более реалистичный взгляд – киберустойчивость. Теперь это не просто часть информационных технологий, но и важнейший фактор экономической безопасности и гарантия бесперебойной работы предприятий.

Согласно исследованию компании RED Security SOC, за период с начала года до середины 2025-го количество хакерских нападений на производственные объекты достигло более 7,5 тысяч случаев, что значительно ниже показателя за тот же отрезок предыдущего года – в три раза. Наряду с этим, эксперты отмечают увеличение числа изощрённых, целенаправленных киберугроз (APT). Лидерами по количеству атак стали представители пищевой отрасли (29%), нефтяной и газовой индустрии (23%) и предприятий машиностроительной направленности (17%). [1]

Некоторые крупные кибератаки в России за последнее время:

28 июля 2025 года произошла атака на «Аэрофлот», ответственность за которую взяла на себя совместная украинско-белорусская группа Silent Crow и Belarus Cyber-Partisans. Кибератака привела к отмéне свыше ста рейсов,

серьезным неполадкам в системе бронирования, а также сделала недоступными веб-сайт, колл-центр и терминалы самообслуживания. Повреждения инфраструктуры включают в себя ликвидацию порядка семи тысяч серверов и изъятие до 22 терабайт информации, среди которой находились личные данные клиентов, внутренняя корреспонденция, а также аудио- и видеозаписи с камер наблюдения.

14 июля 2025 года на Novabev Group была совершена кибератака с целью получения выкупа. В результате действий злоумышленников функционирование компании было нарушено: торговые точки и онлайн-платформы сети WineLab, насчитывающей свыше двух тысяч магазинов в крупнейших российских городах, были заблокированы и возобновили работу лишь через несколько дней. Несмотря на требования о выплате выкупа, руководство Novabev решило отказаться от этого варианта, так как утечка персональных данных клиентов не была подтверждена. По оценкам экспертов издания Forbes, ежедневные убытки компании составили от 200 до 300 миллионов рублей (приблизительно от 2,6 до 3,8 миллионов долларов). [2]

Киберустойчивость и Кибербезопасность: в чем принципиальная разница?

Кибербезопасность представляет собой комплекс мер, направленных на предотвращение несанкционированного доступа к информационным системам и данным. Это своего рода защитная стена, которая препятствует проникновению злоумышленников.

Киберустойчивость — более широкое понятие, охватывающее способность организации не только противостоять атакам, но и эффективно восстанавливаться после них. Это стратегический подход к защите информационных активов.

Важно понимать, что кибербезопасность является неотъемлемой частью киберустойчивости, но не исчерпывает её полностью. Эффективная защита информационных систем требует комплексного подхода, где превентивные меры сочетаются с возможностями восстановления и адаптации к новым угрозам. Сравнение двух понятий проводится в таблице 1 (Сравнительный анализ).

Таблица 1.

Сравнительный анализ

Критерий	Кибербезопасность	Киберустойчивость
Цель	Предотвращение атак	Обеспечение непрерывности
Уровень	Тактический	Стратегический
Фокус	Защита от угроз	Восстановление после угроз
Методы	Технические средства	Комплексный подход
Результат	Блокировка атак	Сохранение работоспособности

Практические шаги по построению киберустойчивости в компании

Шаг 1: Оценка рисков и зрелости — Основа для построения

Прежде чем инвестировать в какие-либо решения, необходимо понять две ключевые вещи: что мы защищаем и от кого. Этот этап является диагностикой, без которой все дальнейшие действия будут слепыми.

- ·Определение самых ценных активов
- ·Выявление самых вероятных угроз
- ·Аудит текущего состояния безопасности

Результатом этого шага должна стать Карта рисков, которая расставляет приоритеты: какие активы требуют максимального внимания и инвестиций исходя из вероятности угроз.

Шаг 2: Разработка стратегии и политик

Полученные на первом этапе данные ложатся в основу документов, которые регламентируют действия до, во время, и после киберинцидента. Стратегия превращает разрозненные меры в единый план.

План реагирования на инциденты (IRP): Это «красная кнопка». IRP детально описывает, что делать, когда атака обнаружена: кто принимает решения, кто входит в группу реагирования (CIRT), как изолировать угрозу, как уведомлять клиентов и регуляторов. Его цель — минимизировать ущерб и время простоя.

План обеспечения непрерывности бизнеса (BCP) и План аварийного восстановления (DRP): Если IRP — это про «тушение пожара», то BCP/DRP — про то, как продолжать работать, пока пожар тушат, и как быстро восстановить все после этого. BCP фокусируется на критических бизнес-процессах (например, как вести продажи без доступа к основной CRM), а DRP — на восстановлении ИТ-систем и данных из резервных копий.

Шаг 3: Инвестиции в технологии — Выбор правильных инструментов

Несмотря на то, что технологии сами по себе не решают всех проблем, продуманный выбор и интеграция инструментов значительно повышают эффективность работы вашей команды.

- Надёжное аварийное восстановление начинается с резервного копирования данных. Придерживайтесь принципа 3-2-1: создавайте три копии информации, храните их на двух различных типах носителей, а одну из них разместите за пределами основной инфраструктуры (например, в облачном хранилище). Важно также регулярно проверять работоспособность резервных копий и возможность восстановления из них данных.
- Решения для обеспечения отказоустойчивости: Проектируйте инфраструктуру с учетом сбоев. Используйте кластеризацию, балансировку нагрузки, дата-центры или облачные решения.
- Инструменты для мониторинга и анализа (SIEM-системы): Чтобы обнаружить сложную атаку, необходимо собирать данные с сетевых

устройств, серверов и рабочих станций. SIEM-системы (Security Information and Event Management) собирают и анализируют данные в режиме реального времени, выявляя аномалии и подозрительную активность.

Шаг 4: Обучение и формирование культуры безопасности — Человеческий фактор

Самый совершенный фаерволл можно обойти одним фишинговым письмом. Сотрудники — это первый рубец обороны, и их необходимо готовить.

Регулярное обучение персонала основам кибербезопасности (распознавание фишинга, надежные пароли) и практические учения (фишинговые тесты) формируют культуру безопасности, делая защиту общим делом.

Внедрение этих четырех шагов создает не статичную «крепость», а гибкую, обучающуюся и готовую к ударам организацию, способную выстоять в современном киберпространстве.

Почему инвестиции в киберустойчивость — это выгодно?

1. Прямая экономия: количественная оценка предотвращенных убытков.

- Прямые финансовые потери: выплаты по искам, штрафы регуляторов
- Юридические и регуляторные издержки: расходы на судебные разбирательства, обязательные аудиты и корректирующие действия, предписанные контролирующими органами.
- Операционные издержки: стоимость простоя критических систем. Сюда же относятся затраты на ликвидацию инцидента, восстановление систем и данных. [3]

2. Стратегические и репутационные выгоды: создание долгосрочной стоимости

- Укрепление доверия и деловой репутации: для клиентов, партнеров и инвесторов способность компании защищать свои и их данные становится ключевым фактором доверия.
- Повышение инвестиционной привлекательности: Инвесторы все чаще включают киберриски в число ключевых нефинансовых рисков. Прозрачная и эффективная программа киберустойчивости снижает инвестиционные риски и может положительно влиять на стоимость акций компании.

3. Выполнение регуляторных требований и управление рисками

- Снижение правовых рисков: соответствие нормам снижает вероятность судебных исков и репутационного ущерба.
- Структурирование управления рисками: Инвестиции в киберустойчивость позволяют интегрировать управление киберрисками в общую систему риск-менеджмента компании, делая ее более предсказуемой и управляемой. [4]

Роль ИИ в современной киберустойчивости

Быстрое совершенствование технологий искусственного интеллекта (ИИ) существенно трансформирует сферу киберугроз и способы противодействия им. В то время как ранее стратегия киберустойчивости базировалась на ответных действиях, сейчас благодаря ИИ возможно переходить к более активной и гибкой модели. ИИ выступает важнейшим элементом не просто отражения нападений, но и их предвидения, автоматизированного реагирования и снижения последствий, что непосредственно повышает финансовую защищенность организации.

- Защита от AI-powered атак (дипфейки, автоматизированный фишинг, генерация вредоносного кода)

Для чего это нужно: злоумышленники активно используют ИИ для создания высококачественных и массовых атак. Генеративные модели

позволяют им в автоматическом режиме писать убедительные фишинговые письма без грамматических ошибок, генерировать полиморфный вредоносный код, который меняет сигнатуру для обхода традиционных антивирусов, и создавать реалистичные дипфейк-аудио и видео для социальной инженерии и мошенничества.

Для противодействия применяются аналогичные технологии на основе ИИ. Например, системы анализа электронной почты используют NLP (обработку естественного языка) для выявления фишинговых паттернов и подозрительных формулировок, даже если письмо идеально с точки зрения грамматики. Алгоритмы компьютерного зрения анализируют видео- и аудиоконтент на предмет артефактов, характерных для дипфейков.

Влияние на киберустойчивость: позволяет бороться с угрозами "нового поколения" на опережение, снижая риск успешной атаки через самый уязвимый вектор — человека. Это напрямую защищает от финансовых потерь (как в случае с мошенничеством с дипфейк-голосом директора) и репутационного ущерба.

Пример: В 2024 году произошел резкий всплеск атак с использованием ИИ-генераторов, таких как WormGPT и FraudGPT, которые позволяют злоумышленникам создавать сложные фишинговые кампании и вредоносные программы. Киберзащитные компании, в ответ, внедрили в свои продукты аналогичные ИИ-модели, способные детектировать контент, созданный этими инструментами, анализируя стилистические и семантические паттерны. [5]

- Применение машинного обучения в системах обнаружения угроз

Для чего это нужно: традиционные сигнатурные методы обнаружения бессильны против атак нулевого дня и целевых сложных кампаний. Машинное обучение позволяет анализировать огромные объемы данных (сетевой трафик, файлы систем, активность процессов) для выявления аномалий и скрытых паттернов, указывающих на злонамеренную активность.

Модели ML обучаются на исторических данных о нормальном поведении системы и известных атаках. В реальном времени они непрерывно сравнивают текущую активность с базовым профилем "нормы". Например, могут обнаружить нехарактерный исходящий трафик с сервера (признак утечки данных) или аномальную активность учетной записи в нерабочее время.

Влияние на киберустойчивость: Сокращает "время жизни" угрозы в системе. Если классические методы могли обнаружить атаку через дни или недели, ML-системы делают это за минуты или часы, что критически уменьшает потенциальный ущерб.

Пример: платформа Darktrace применяет машинное обучение без участия человека для создания «цифровой защиты» сетевой инфраструктуры. Как показал один случай. Злоумышленники получили доступ к современному аквариуму, который был оснащен подключением к интернету и использовали его как плацдарм для проникновения во внутреннюю сеть казино. система выявила необычную работу в сети и нейтрализовала угрозу. [6]

- Автоматизация анализа поведения через UEBA (User and Entity Behavior Analytics)

Для чего это нужно: зачастую успешные кибератаки реализуются посредством законных логинов и паролей, заполученных путем фишинга или из-за утечек данных. Традиционные средства защиты оказываются бессильными против таких атак. UEBA же сосредоточен на изучении активности не только отдельных пользователей, но и различных элементов инфраструктуры – серверов, принтеров, учетных записей программного обеспечения.

Система формирует поведенческий портрет каждого пользователя и каждого устройства: фиксируются обычные IP-адреса подключения, время входа, запрашиваемые системы и объем скачиваемых данных. Любое

отклонение от установленного шаблона (например, массовая загрузка файлов ночью с неизвестного девайса) вызывает сигнал тревоги.

Влияние на киберустойчивость: Позволяет обнаруживать инсайдерские угрозы, взломанные аккаунты и перемещение злоумышленника внутри сети. Это критически важно для предотвращения дальнейшего развития атаки и масштабной утечки информации.

Пример: В 2022 году компания Exabeam сообщила о случае, когда их UEBA-система помогла клиенту из банковской сферы выявить скомпрометированную учётную запись сотрудника. Система заметила, что аккаунт, обычно используемый для доступа к внутренней базе знаний, неожиданно начал делать множество запросов к базам с данными клиентов, что существенно отличалось от его привычной активности. Проблема была решена до того, как информация покинула пределы компании. [7]

- Проактивные системы реагирования на основе ИИ

Для чего это нужно:

Чтобы максимально сократить время между выявлением угрозы и её устранением – фактор, определяющий масштаб ущерба. Аналитик, или эксперт не способен реагировать так же быстро, как машина.

Объединение систем выявления угроз (основанных на машинном обучении и UEBA) с платформами безопасности и автоматизации реагирования (SOAR). При фиксации аномалии ИИ-алгоритм не только формирует уведомление, но и автоматически запускает сценарий действий: отключает зараженный компьютер от сети, блокирует подозрительный IP-адрес на межсетевом экране, принудительно меняет пароль пользователя.

Влияние на киберустойчивость: переводит киберустойчивость из состояния "обнаружить и проанализировать" в режим "обнаружить и нейтрализовать". Автоматизация типовых задач по реагированию освобождает специалистов для решения более сложных стратегических вопросов и снижает затраты на ликвидацию инцидентов.

Пример: В компании, специализирующейся на продаже стройматериалов, одно из устройств было заражено трояном Emotet, который стремительно распространял вредоносные файлы и осуществлял кражу финансовой информации. Уже через несколько минут Технология Darktrace Antigena заблокировала вредоносную коммуникацию между зараженным устройством и незнакомым сервером. [8]

Таким образом, внедрение искусственного интеллекта в стратегию киберустойчивости трансформирует её из фиксированного набора регламентов в гибкую, самообучающуюся и обладающую возможностью самостоятельной защиты систему. В современных условиях это не просто желательное дополнение, а жизненно важная необходимость для поддержания экономической безопасности бизнеса в эпоху всё более изощренных и автоматизированных атак.

Заключение

Проведенный анализ однозначно свидетельствует, что в современной цифровой экосистеме, характеризующейся перманентными и эволюционирующими киберугрозами, киберустойчивость перестала быть сугубо технической задачей или опциональным элементом ИТ-инфраструктуры. Она трансформировалась в критический, неотъемлемый компонент экономической устойчивости бизнеса. Экономическая безопасность, понимаемая как защищенность жизненно важных интересов компании от внутренних и внешних угроз, сегодня напрямую зависит от ее способности противостоять цифровым вызовам.

Таким образом, тезис о том, что инвестиции в киберустойчивость являются затратами, окончательно утратил свою актуальность. Как показано в работе, это — стратегические инвестиции в устойчивость, конкурентоспособность и долгосрочное выживание.

Подводя итог, можно утверждать, что построение эффективной системы киберустойчивости — это уже не вопрос технического соответствия, а ключевая управленческая компетенция и моральная ответственность руководства. Компании, которые осознали эту парадигму и интегрировали киберустойчивость в свою бизнес-стратегию, не просто защищаются от угроз. Они формируют прочный фундамент для роста и лидерства в условиях неопределенности.

Использованные источники:

1. Сайт «Коммерсантъ» лидер российской деловой журналистики. [Электронный ресурс]. URL: https://www.kommersant.ru/doc/7924676 (дата обращения: 01.02.2026)
2. Сайт «Техчат» [Электронный ресурс]. URL: https://tenchat.ru/media/3623119-kiberataki-na-rossiyskiye-kompanii-itogi-iyulya-2025-goda (дата обращения: 02.02.2026)
3. Научная статья «Экономика инвестиций в информационную безопасность» Гордон Л.А., Лоеб М.П. (2002), сайт «Researchgate» [Электронный ресурс]. URL: https://www.researchgate.net/publication/288351571_The_Economics_of_Information_Security_Investment (дата обращения: 07.02.2026)
4. Доклад всемирного экономического форума (2023). «Прогноз развития глобальной кибербезопасности» // World Economic Forum. (2023). The Global Cybersecurity Outlook Report. сайт «Researchgate» [Электронный ресурс]. URL: https://gem.university/wp-content/uploads/documents/pdf/news/wef_global_security_outlook_report_2023.pdf (дата обращения: 07.02.2026)
5. Информационный портал по безопасности SecurityLab [Электронный ресурс]. URL: https://www.securitylab.ru/news/554877.php (дата обращения: 12.02.2026)

6. Статья от «Технический центр Интернет» [Электронный ресурс]. URL: https://www.tcinet.ru/press-centre/technology-news/5348/ (дата обращения: 12.02.2026)

7. Организация в области киберзащиты, предоставляющая интеллектуальные системы автоматизации безопасных операций, основанные на искусственном интеллекте «Exabeam». [Электронный ресурс]. URL: https://www.exabeam.com/ (дата обращения: 12.02.2026)

8. Британская фирма, занимающаяся созданием программных решений для защиты информации «Darktrace». [Электронный ресурс]. URL: https://www.darktrace.com/es/news/darktrace-ai-stops-emotet-trojan-cyber-attack-at-saudi-arabian-construction-supply-giant (дата обращения: 14.02.2026)