УДК 658.5

КИБЕРБЕЗОПАСНОСТЬ СОВРЕМЕННЫХ КОМПАНИЙ

В.Я. Захаров, М.В. Кислинская, Е.Н. Лудушкина
Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского, Нижний Новгород, email: zaxarov48@yandex.ru, mvkislinskaya@yandex.ru,ludushkina@mail.ru

Аннотация. *Статья содержит обзор результатов последних зарубежных, а также российских аналитических исследований, посвященных анализу тенденций изменения кибербезопасности компаний. Системный анализ позволил определить ключевые тенденции, оказывающие сильное влияние на кибербезопасность компаний и усиливающие киберугрозы: стремительное развитие искусственного интеллекта, ускоряющее гонку кибервооружений, геополитическая волатильность, нарушения цепочек поставок. На основе контент-анализа компаний были сформулированы причины тенденций в области кибербезопасности компаний в мире и в России, проведено сравнение зарубежной и российской практик в данной области. Кроме того, в статье были даны рекомендации по усилению кибербезопасности и устойчивости отечественных предприятий. Акцент сделан на необходимости ускорения импортозамещения в области информационных технологий и, в частности, в области кибербезопасности компаний. С целью отслеживания скорости и качества процесса в рамках данной статьи был предложен индекс зрелости импортозамещения. Применение данного индекса будет полезно отечественным компаниям, отделам стратегического развития для разработки стратегий в области кибербезопасности, а также будет полезен для установления подхода к кибербезопасности не как к вынужденной статье расходов, а как к фактору устойчивости и конкурентоспособности, что, в целом, будет способствовать обеспечению технологического суверенитета и экономической безопасности российских компаний.*

Ключевые слова: *кибербезопасность, риски, устойчивость, индекс зрелости импортозамещения.*

CYBERSECURITY OF MODERN COMPANIES

V.Ya. Zakharov, M.V. Kislinskaya, E.N. Ludushkina
National Research Nizhny Novgorod State University named after N. I. Lobachevsky, Nizhny Novgorod, email: zaxarov48@yandex.ru, mvkislinskaya@yandex.ru, ludushkina@mail.ru

Abstract. *The article provides an overview of the results of recent foreign and Russian analytical studies on the trends in company cybersecurity. A systematic analysis has identified key trends that have a significant impact on company cybersecurity and increase cyber threats, such as the rapid development of artificial intelligence, accelerating the cyber arms race, geopolitical volatility, and supply chain disruptions. Based on a content analysis of companies, the article identifies the causes of trends in company cybersecurity globally and in Russia, and compares foreign and Russian practices in this area. In addition, the article provides recommendations for strengthening the cybersecurity and resilience of Russian enterprises. The article focuses on the need to accelerate import substitution in the field of information technology, particularly in the area of cybersecurity. To track the speed and quality of this process, the article proposes the index of maturity of import substitution. This index will be useful for Russian companies and their strategic development departments to develop cybersecurity strategies. It will also help them approach cybersecurity not as a necessary expense, but as a factor of sustainability and competitiveness. This will contribute to the technological sovereignty and economic security of Russian companies.*

Keywords: *cybersecurity, risks, sustainability, strategies, the index of maturity of import substitution.*

Дата поступления статьи в редакцию: 06.07.2026
Дата принятия статьи в печать: 02.09.2026

Введение

Исследования и практика подсказывают, что процессы, которые более других влияли на кибербезопасность и экономическую безопасность стран в течение последних трёх десятилетий, - глобализация и цифровая трансформация сложных систем.

Глобализация превращает мир в совокупность все более сложных, вложенных и взаимосвязанных систем, которые одновременно являются техническими, экономическими и социаль-

ными. Она принесла очевидные выгоды, но снизила устойчивость систем к потрясениям и создала условия для распространения шоков от системы к системе. Возросла вероятность каскадных шоков, способных вызывать катастрофы в мировой экономике [1]. Для поддержания национальной безопасности странам необходим системный подход к управлению их устойчивым развитием, способный повысить готовность сложных экономических систем к будущим потрясениям. Под воздействием потока стремительно развивающихся технологий сложность систем растет, как правило, быстрее, чем сложность управляющей системы.

Окружающая среда постоянно меняется, и в ответ на это меняются сложные системы и их поведение. Сложные системы неизбежно содержат радикальную неопределенность, относительно которой, согласно Дж. Кейнсу, нет научной основы для формирования какой-либо поддающейся расчету вероятности. Управление безопасностью систем, в т.ч. в киберпространстве, должно быть нацелено на обеспечение их устойчивого развития и процветания в долгосрочной перспективе благодаря наращиванию способности преодолевать непредсказуемые шоки и потрясения разных масштабов, интенсивности и сложности за счет ускоряющегося потока новых технологий.

Разнообразие сложных систем порождает столь же обширный спектр системных рисков, выявление которых затрудняется характеристиками рассматриваемых систем. Природу этих угроз можно охарактеризовать как процесс заражения, при котором отдельные сбои распространяются на систему в целом, и где нарушение в одной области может вызвать каскадное распространение по всей системе [1]. Сочетание высокой степени воздействия, низкой вероятности и труднопредсказуемого распространения угроз делает задачу топ-менеджера компании, пытающегося справиться с системными рисками, чрезвычайно сложной. Её решение требует постоянного обновления подходов и инструментов управления рисками. Современные компании сталкиваются с киберугрозами, скорость и масштаб которых превосходят возможности имеющихся средств защиты от атак; возрастает разрыв между требованиями к безопасности систем и возможностями обеспечения безопасности.

Цель исследования

Целью данного исследования было привлечение внимания к вопросу обеспечения кибербезопасности и устойчивости российских компаний в современных условиях системного экономико-геополитического противостояния стран.

Материал и методы исследования

В статье представлен обзор результатов последних исследований аналитических центров по вопросам обеспечения кибербезопасности компаний. Наибольшее внимание уделено анализу результатов международных опросов Global Cybersecurity Outlook как наиболее актуальных и всесторонних. Кроме того, были использованы аналитические обзоры и опросы отечественных компаний.

На основе анализа и синтеза данных обзоров, а также контент-анализа компаний, были выявлены тенденции в области кибербезопасности компаний в мире и в России, сформулированы их причины, проведено сравнение зарубежной и российской практик в данной области, а также были даны рекомендации по усилению кибербезопасности и устойчивости отечественных предприятий.

Результаты исследования

Исследования «Глобальный обзор кибербезопасности» (Global Cybersecurity Outlook) проводятся с 2022 г., они позволяют отслеживать динамику рисков в цифровом пространстве. К 2022 г. мир адаптировался к новым возможностям подключения и во время пандемии стремился перевести свою деятельность в цифровой формат. В 2022 г. усилилась волатильность геополитики и её влияние на киберриски, в том числе, связанные с взаимозависимостью цепочек поставок на фоне санкционного давления на Россию. Анализ данных, содержащихся в «глобальных обзорах кибербезопасности», позволяет констатировать тенденции, риски, проблемы и наблюдающуюся в мире поляризацию, в процессе которой растет неравенство в информационной безопасности между технологически развитыми и догоняющими странами и компаниями. В 2025 и 2026 годах возрастающая геополитическая напряженность, нефтяной и топлив-

ный кризисы, нарушение и усложнение цепочек поставок и стремительное внедрение новых технологий приводят к росту сложности и непредсказуемости развития мировой и национальных экономик.

В опросе Global Cybersecurity Outlook 2026 года приняли участие 804 руководителей, специалистов и учёных в сфере кибербезопасности из 92 стран мира [2]. Результаты опроса приводят к выводу, что в 2026 году риски, связанные с кибербезопасностью, будут нарастать из-за развития искусственного интеллекта, углубления геополитической раздробленности и усложнения цепочек поставок.

Оценка динамики киберрисков рисков киберпространства за последний год представлена в таблице 1.

Таблица 1

Оценка динамики киберрисков за последний год (в % по строке)

Киберриски	Увеличилось	Осталось на том же уровне	Снизилось
Уязвимости искусственного интеллекта	87	13	-
Мошенничество и фишинг с использованием киберпреступлений	77	21	2
Нарушение цепочек поставок	65	32	3
Эксплуатация программных уязвимостей	58	39	3
Атаки программ-вымогателей	54	39	7
Внутренняя угроза	32	61	7
Отказ в обслуживании	28	54	12

Источник: [2].

Подавляющее большинство опрошенных считают, что выросли киберриски, связанные с искусственным интеллектом, кибермошенничеством и нарушением цепочек поставок.

В 2025 году опрошенные были единодушны (87%) в том, что быстрее других растут риски, связанные с искусственным интеллектом. Доля организаций, в которых внедрены процессы оценки безопасности искусственного интеллекта, увеличилась с 37% в 2025 г. до 64% в 2026 г., т.е. практически вдвое [2, 3].

Искусственный интеллект расширяет возможности для атак (увеличивая их масштаб, скорость, сложность и точность), создавая новые уязвимости, для устранения которых не предназначены имеющиеся средства защиты. И одновременно он используется для укрепления кибербезопасности: улучшения обнаружения, ускорения реагирования, автоматизации аналитических задач. Специалисты по кибербезопасности приходят к выводу, что искусственный интеллект способен повысить уровень кибербезопасности при условии, что он внедряется в рамках надежной системы управления, в центре которой находится человеческий фактор [4].

По данным компании Heimdal, руководители американских компаний в четыре раза чаще, чем их подчиненные, считают, что риски, связанные с искусственным интеллектом, находятся под контролем (29 % против 7 %). Но только 4 из 10 опрошенных команд разработчиков утверждают, что их система безопасности готова к рискам, связанным с искусственным интеллектом; они полагают, что внедрение искусственного интеллекта опережает контроль над ним примерно в два раза [5].

На вопрос, какие проблемы кибербезопасности, связанные с генеративным искусственным интеллектом, беспокоят Вас больше всего, были получены следующие ответы (таблица 2):

Таблица 2

Риски искусственного интеллекта

Проблемы кибербезопасности, связанные с искусственным интеллектом	В процентах к числу опрошенных
Утечка данных (раскрытие персональных данных через генетически модифицированный ИИ)	30%
Развитие возможностей противодействия	28%
Техническая безопасность самих систем искусственного интеллекта	15%
Повышенная сложность управления безопасностью	13%
Правовые аспекты интеллектуальной собственности и ответственности.	9%
Риски, связанные с цепочкой поставок программного обеспечения и разработкой кода.	6%

Источник: [2].

Как видно из таблицы 2, утечка конфиденциальных данных (30%) и развитие возможностей противодействия, т.е. растущая изощренность атак (28%) рассматриваются как наиболее сильные угрозы безопасности, связанные с генеративным искусственным интеллектом. Согласно данным опроса 2026 года, 77% организаций внедрили искусственный интеллект в сфере кибербезопасности, он способен сделать киберзащиту более надежной и эффективной, позволяя обрабатывать огромные объемы данных для раннего обнаружения угроз и выявления скрытых рисков, расставить приоритеты, обнаружить аномалии, проводить непрерывный мониторинг, выявлять уязвимости и автоматизировать их устранение в режиме реального времени, повышать уровень безопасности программного обеспечения и оптимизировать процесс принятия решений. О том, для чего компании внедряют искусственный интеллект, свидетельствуют данные таблицы 3.

Таблица 3

Направления использования искусственного интеллекта в стратегиях кибербезопасности организаций

Мотивы	В % к числу опрошенных
Для обнаружения фишинговых атак и угроз по электронной почте	52%
Для обнаружения вторжений или аномалий и реагирования на них	46%
Для автоматизации операций по обеспечению безопасности	43%
Для анализа поведения пользователей и обнаружения внутренних угроз	40%
Для анализа угроз и определения приоритетов рисков	39%
Для других целей	8%

Источник: [2].

Кроме искусственного интеллекта, руководители компаний были больше всего обеспокоены атаками программ-вымогателей, за которыми последовало кибермошенничество, увеличившееся на 77% (см. табл. 1). В подобных условиях генеральные директора в первую очередь озабочены предотвращением финансовых потерь и подготовкой к новым угрозам, а директора по информационной безопасности сосредоточены на обеспечении операционной устойчивости.

Ответы всех респондентов на вопрос, каким атакам кибермошенников за последние 12 месяцев подвергались Вы или кто-либо из вашей профессиональной сети, представлены в таблице 4.

Таблица 4

Виды и распространенность кибермошенничества

	В процентах к числу опрошенных
Фишинговые, вишинговые или смишинговые атаки	62%
Счет-фактура или мошенничество с платежами	37%
Кража личных данных	32%
Внутренняя угроза или мошенничество, инициированное сотрудником	20%
Романтика или мошенничество с использованием поддельных личных данных	17%
Инвестиции или мошенничество с криптовалютой	17 %

Источник: [2].

Из таблицы 4 видно, что три самых распространенных вида атак – это фишинг (в том числе вишинг и смишинг), мошенничество с платежами и кража персональных данных.

По данным отчета о фишинге компании SryClod за 2026 год [6], за последние 12 месяцев в 78% организаций участились случаи фишинга, в результате фишинговых атак были раскрыты данные сотрудников 86% компаний из списка Fortune 100. Организации осознают растущую угрозу фишинга, но многие из них не готовы эффективно реагировать на атаки:

- 38 % организаций полностью уверены, что смогут обнаружить факт кражи учетных данных и отреагировать на него в течение 24 часов;
- 58 % опрошенных испытывают трудности с определением того, какие учетные данные или сеансовые токены были раскрыты после фишинговой атаки;
- 68 % опрошенных требуется 4 часа или больше, чтобы выявить и устранить последствия подтвержденного фишинга.

Главная проблема – непрозрачность фишинговых атак. Если служба безопасности не может определить, какие учетные данные, сеансовые токены или другие составляющие аутентификации были раскрыты, злоумышленники получают время для закрепления в системе и проведения последующих атак. Самым эффективным способом сокращения времени признается автоматизация процессов устранения уязвимостей. Вероятность фишинговых атак, нацеленных на корпоративных пользователей, сегодня примерно в пять раз выше, чем вероятность заражения вредоносными программами [6].

Преступники с помощью генеративного искусственного интеллекта стремятся создать реалистичные письма, видеоматериалы и документы, способные обойти традиционные системы обнаружения и человеческий контроль. Эти возможности существенно изменяют ландшафт угроз, повышая киберриски в первую очередь для уязвимых групп населения, нейтрализация которых требует более сложных и гибких инструментов защиты. Киберпреступность превратилась в высокоорганизованную (с помощью платформ) и хорошо коммерциализованную деятельность, возможности которой демонстрируются открыто, вследствие чего усиливается взаимосвязь между киберпреступностью и традиционной организованной преступностью [7].

Волатильностью геополитики, усиливающей неопределенность в оперативном и стратегическом управлении компаний в мире, также необходимо учитывать. Мир фрагментируется, и борьба за перераспределение ресурсов сопровождается конфликтами, экономической напряженностью, торговыми войнами и санкциями, обострением технологической конкуренции, в результате геополитика стала критически важным фактором национальной, экономической и цифровой безопасности. Число случаев изменения стратегии кибербезопасности из-за геополитических факторов снизилось с 93% в 2023 году до 66% в 2026 году, что свидетельствует об адаптации после потрясений 2022 и 2023 годов [2, 3].

Руководители частных компаний дали следующие ответы на вопрос, насколько Вы уверены в готовности страны, в которой вы находитесь, реагировать на крупные кибер-инциденты, направленные против критической инфраструктуры, распределились следующим образом: уве-

рены – 43%; и да, и нет – 26; не уверены – 31%. Как видим, определенно сомневаются в готовности стран немногим более 40% опрошенных, и эта неуверенность растет [2].

Цепочки поставок становятся все более сложными и взаимозависимыми, что усиливает непрозрачность и непредсказуемость рисков. В 2025 году каждая вторая крупная организация указали на нарушения в цепочках поставок в их экосистемах [3].

Рейтинг (значимость) основных киберрисков в цепочках поставок представлен в таблице 5.

Таблица 5

Значимость рисков, связанных с нарушением цепочек поставок

Ранг	Киберриски
1	Риск наследования - неспособность гарантировать целостность программного обеспечения, оборудования и услуг третьих лиц
2	Прозрачность: недостаточная прозрачность по всей цепочке поставок
3	Риск концентрации: слишком большая зависимость от критически важных сторонних поставщиков
4	Риск закупок: невозможно осуществлять контроль над мерами безопасности сторонних поставщиков
5	Внешние факторы: неопределенность воздействия внешних факторов

Источник: [2].

Как видим, главным риском в цепочке поставок является риск наследования, за ним следует риск непрозрачности цепочки. Атаки киберпреступников направляются на слабые звенья в экосистемах с низким уровнем кибербезопасности. Управление рисками в цепочке поставок нередко сводится к формальному соблюдению требований, тогда оно не является гибким и непрерывным процессом.

Данные о том, как организации решает проблему киберрисков в цепочке поставок, представлены в таблице 6.

Таблица 6

Действия компаний по управлению рисками цепочек поставок

Действия	Руководители высокоустойчивых организаций	Руководители неустойчивых организаций
Привлечение службы безопасности к процессу закупок	70%	31%
Оценка уровня зрелости системы безопасности наших поставщиков	59%	31%
Согласование стратегии киберустойчивости со всеми партнерами по экосистеме	48%	31%
Детальное изучение экосистемы, чтобы понять вероятные киберугрозы	48%	31%
Моделирование киберинцидентов и планирование учений по восстановлению совместно с партнерами по экосистеме	44%	6%
Обмен информацией об угрозах с партнерами в экосистеме (клиентами, поставщиками, партнерами)	30%	38%

Источник: [2].

Данные таблицы 6 показывают, что руководители устойчивых организаций активнее внедряют меры в процесс закупок и больше внимания уделяют проверке надежности поставщиков.

Идентификация приоритетов руководителей в стратегии кибербезопасности представлена в таблице 7.

Таблица 7

Стратегические приоритеты руководителей компаний

№	Факторы	(в % к числу опрошенных)
1	Геополитически мотивированные кибератаки (разрушение критически важной национальной инфраструктуры, шпионаж и т.д.)	64%
2	Дезинформация	49%
3	Конвергенцию информационных и операционных технологий, технологий интернета вещей и робототехники	42%
4	Стихийные бедствия	41%
5	Зависимость от подводных кабелей или линий связей	18%
6	Зависимость от космических средств (например, спутников, GPS, спутниковой связи)	15%
7	Ни один из вышеперечисленных	11%

Источник: [2].

На геополитический фактор указали две трети опрошенных. Из-за геополитической нестабильности изменили свои стратегии 9 из 10 крупнейших (более 100 000 работников) компаний.

Восприятие рисков руководителями компаний зависит от уровня устойчивости их компаний к внешним воздействиям. Кибермошенничество и фишинг остаются главными проблемами кибербезопасности для руководителей недостаточно устойчивых организаций. Среди руководителей высокоустойчивых организаций на первое место выходят уязвимости, связанные с искусственным интеллектом.

Организации с разным уровнем устойчивости по-разному корректируют свои стратегии кибербезопасности в условиях геополитической нестабильности (таблица 8).

Таблица 8

Влияние геополитической нестабильности на изменения в стратегиях кибербезопасности организаций

Изменения	Руководители высокоустойчивых организаций	Руководители неустойчивых организаций
Усиление внимания к анализу угроз, связанных с государственными субъектами	52%	13%
Активизация взаимодействия с государственными учреждениями и группами по обмену информацией	48%	6%
Увеличение бюджета на кибербезопасность	30%	13%
Смен поставщиков в связи с геополитическими соображениями	30%	13%
Прекращение бизнеса в некоторых странах	19%	6%
Сокращение бюджета на кибербезопасность	-	13%

Источник: [2].

Как демонстрирует таблица 8, все организации сосредоточились на анализе угроз, связанных с государственными субъектами, при этом устойчивые организации чаще усиливали взаимодействие с государственными организациями и увеличивали свои бюджеты кибербезопасности, а неустойчивые организации, напротив, снижали взаимодействие с государственными учреждениями и бюджеты кибербезопасности.

Геополитическая нестабильность и экономическая неопределенность тесно переплелись, усилив фрагментацию цифровых и технологических экосистем. Стремясь защитить критически важную инфраструктуру, многие страны снижают свою зависимость от иностранных поставщиков технологий и глобальных цепочек поставок; в основу современной политики кибербезопасности положена концепция цифровой автономии и технологического суверенитета [7]. Пересматривается доверие не только к системам и технологиям, но и к геополитической надежности экосистем, чтобы разрешить противоречие между сохранением открытости и функциональной совместимости и защитой национальной автономии.

В этой связи необходимо обеспечивать устойчивость и киберустойчивость компаний. Устойчивость компании понимается как её способность выживать (обеспечивать безопасность) и процветать (повышать благосостояние) в непредсказуемой, постоянно изменяющейся среде [1]. Киберустойчивость – это способность организации минимизировать влияние серьезных киберинцидентов на достижение основных бизнес-целей и выполнение задач [2]. Понятие киберустойчивости шире, чем понятие кибербезопасности.

Согласно данным опроса, уверенность в киберустойчивости организаций растет. На вопрос, как бы Вы оценили киберустойчивость вашей организации, ответы распределились следующим образом (таблица 9).

Таблица 9

Оценка киберустойчивости организаций (в процентах по столбцу)

Уровень киберустойчивости организаций	2024	2025	2026
Наша киберустойчивость недостаточна	24	22	17
Наша киберустойчивость соответствует минимальным требованиям	63	69	64
Наша киберустойчивость превосходит наши требования	13	9	19

Источник: [2].

Большинство (две трети) опрошенных оценивают киберустойчивость своих компаний как соответствующую минимальным требованиям; и только 19% заявили, что киберустойчивость их организаций превышает требуемый уровень. Данный индикатор позволяет сделать вывод об отставании систем кибербезопасности от растущей динамики угроз и необходимости сдвигов в парадигме и стратегиях кибербезопасности компаний, нацеленных на преодоление этого разрыва.

В 2025 году почти 35% малых организаций считали, что их киберустойчивость недостаточна, и с 2022 года эта доля выросла в семь раз (с 5% до 35%); доля крупных организаций, считающих, что их киберустойчивость недостаточна, сократилась почти вдвое (с 13% до 7%). Организации государственного сектора чаще сообщали о недостаточной устойчивости к кибератакам, чем организации среднего и крупного бизнеса (38% против 10%) [3]. Существует значительный разрыв в расходах на кибербезопасность между странами: развивающиеся страны тратят 1 доллар на душу населения или меньше на кибербезопасность по сравнению с 30 долларами в развитых странах [9]. В Великобритании, например, ущерб от серьезной кибератаки на бизнес в среднем составляет 250 тыс. долларов; в целом по стране общие ежегодные потери от кибератак составляют 19,4 миллиарда долларов [10]. Широкий резонанс в корпоративном мире получила успешная кибератака на компанию Jaguar Land Rover, совершенная в августе 2025 года. Прямые финансовые потери от кибератаки составили 260 миллионов долларов, выручка снизилась на 25%, экономика Великобритании потеряла 2,5 миллиарда долларов [11]. По оценкам Мирового банка в развивающихся странах за счет предотвращения крупных киберинцидентов возможно увеличить ВВП на душу населения на 1,5% [12].

Рост неравенства в кибербезопасности снижает киберустойчивость всей экосистемы, создавая для злоумышленников возможности атаковать слабые звенья.

Исследования показали, что организационная устойчивость влияет на восприятие руководителями трудностей на пути повышения киберустойчивости своих организаций. На вопрос, в чём заключается главная проблема, с которой сталкивается ваша организация на пути к обеспечению киберустойчивости, были даны следующие ответы (таблица 10).

Таблица 10

Основные проблемы на пути повышения киберустойчивости

Проблемы	Руководители высокоустойчивых организаций	Руководители неустойчивых организаций
Уязвимости третьих сторон и цепочки поставок	78%	31%
Быстро меняющаяся картина угроз и новые технологии	56%	13%
Сложности, связанные с соблюдением нормативных требований и корпоративным управлением	41%	25%
Отсутствие прозрачности в средах ИТ, ОТ и Интернета вещей	19%	56%
Нехватка специалистов и экспертов в области кибербезопасности	19%	56%
Недостаточное планирование реагирования на инциденты и восстановления после них	15%	19%
Устаревшие системы	15%	25%
Нехватка средств	15%	63%

Источник: [2].

По мере повышения устойчивости организаций руководители чаще переключают внимание с внутренних ресурсных ограничений на более широкие риски, связанные с экосистемой. Если руководители неустойчивых организаций главные проблемы повышения киберустойчивости своих организаций видят в нехватке специалистов по кибербезопасности (56%) и финансовых ресурсов (63%), то руководители организаций с высоким уровнем устойчивости наиболее серьезной проблемой для повышения киберустойчивости назвали зависимость от цепочек поставок и сторонних организаций (78%).

Отличия организаций с высоким уровнем устойчивости, обеспечивающих высокий уровень кибербезопасности, от недостаточно устойчивых компаний с низким уровнем кибербезопасности заключаются в следующем [2]:

- вовлекают совет директоров в вопросы кибербезопасности (99%);
- более высоко оценивают эффективность нормативных актов по кибербезопасности;
- реже сообщают о нехватке сотрудников, необходимых для достижения целей в области кибербезопасности (22% против 85%);
- активнее вовлекают службу безопасности в процесс закупок (75% против 53%);
- проверяют безопасность своих ИИ-инструментов (71% и 20%);
- имеют антикризисные планы и сценарии действий, а также регулярно проводят учения с участием всех участников экосистемы (44% и 16%);
- организации более активно взаимодействуют со всей своей экосистемой: делятся информацией о кибербезопасности с партнерами (53% против 31%), оценивают безопасность своих поставщиков (74% против 48%), оценивают подверженность партнеров рискам (44% против 23%).

Сегодня Россия входит в ТОП-10 стран по уровню расходов на информационную безопасность, уступая США, Китаю, Великобритании, Японии, Франции, Австралии, Канаде, Германии. Обгоняет такие крупные страны, как Индия, Бразилия, Италия, Аргентина и др. С учетом экспертных оценок, при сохранении текущих параметров российский рынок ИБ к 2031 году может превысить 1 трлн рублей. Среднегодовой темп роста в текущем прогнозе оценивается на уровне 19,4% (рис. 1) [13].

На протяжении многих лет Россия входит в число наиболее приоритетных целей киберпреступников. В период с июля 2024-го по сентябрь 2025 года на Россию пришлось от 14% до 16% всех успешных кибератак в мире и 72% атак, зафиксированных в СНГ [14].

За период в четыре года по показателю подтверждённых инцидентов информационной безопасности можно заметить отчетливые всплески, связанные с политической обстановкой.

Например, значительный рост атак в 3 квартале 2022 г. был связан с вхождением новых территорий в состав РФ (рис. 1).

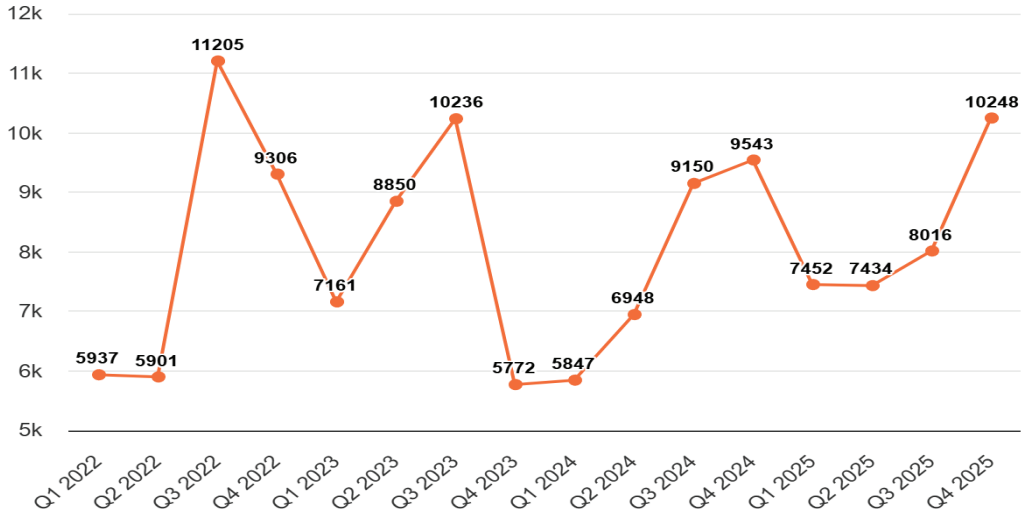

Рис. 1. *Подтверждённые инциденты информационной безопасности в 2022-2025 гг. [15]*

Основными методами кибератак в России, как и во всем мире, по-прежнему остаются использование вредоносного программного обеспечения и социальная инженерия (рис. 2).

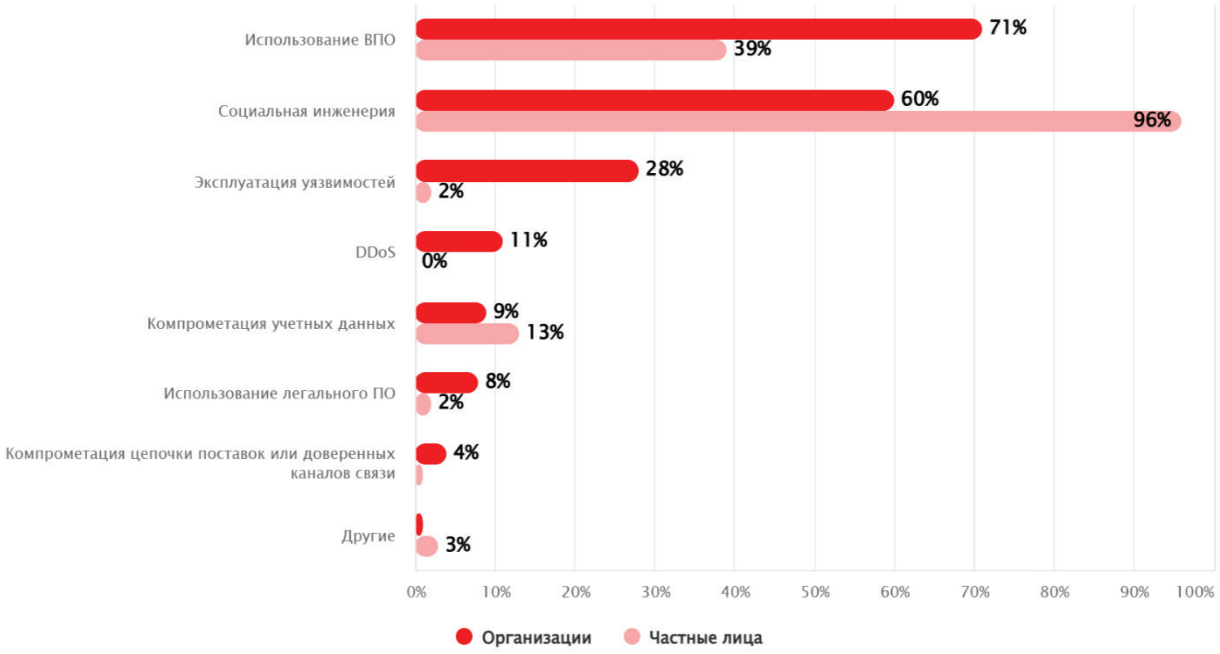

Рис. 2. *Методы атак на российские организации и частных лиц (доля успешных атак) [14].*

Наиболее распространенные последствия кибератак на организации в России – это утечка конфиденциальной информации и нарушение основной деятельности компаний. Эти два последствия часто взаимосвязаны.

Ключевыми причинами усиления интенсивности и количества киберугроз в мире, очевидно, является цифровизация и развитие генеративного искусственного интеллекта. Кроме того, все причины возможно объединить в группы:

- технологические (искусственный интеллект как инструмент автоматизации атак, ускорения поиска технологических уязвимостей, распространение вредоносного программного обеспечения как услуги);
- экономические (финансовая мотивация, развитие теневых рынков данных и доступов, высокая ключевая ставка в течение длительного периода);

– социальные (человеческий фактор: невнимательность, доверчивость, ошибки, социальная инженерия);
– организационные (недостаток специалистов и инвестиций в кибербезопасность, особенно у малого и среднего бизнеса, рост числа подключенных устройств, рост зависимости от информационных систем, уязвимость цепочек поставок и подрядчиков);
– геополитические (санкции, конфликты, кризисы приводят к волнам кибератак).

При анализе кибербезопасности в мире и в России были сформулированы черты сходства и отличия.

К основным чертам сходства можно отнести:
– рост расходов на кибербезопасность;
– переход к системным подходам;
– кадровый дефицит;
– ужесточение регуляторных требований;
– развитие облачных технологий;
– гибридная работа;
– автоматизация реагирования на инциденты;
– усиление влияния роли государства и её регуляторов.

К основным чертам, отличающим кибербезопасность компаний в России от мировой практики, относятся:
– импортозамещение (после 2022 г. произошёл и продолжает происходить массовый переход на российские решения);
– темп внедрения инноваций (российский рынок пока догоняет в освоении новых классов решений);
– развитость системных и стратегических решений (характерна в основном крупному бизнесу в области критически важной инфраструктуры);
– темпы роста рынка кибербезопасности в России высокие, но по абсолютным значениям ниже мировых;
– санкции (российские компании вынуждены быстро адаптироваться к ограничениям доступа к зарубежным технологиям, что требует дополнительных временных, людских, организационных и финансовых ресурсов);
– образовательная подготовка (в мире шире развита система подготовки кадров через университеты и профессиональные сертификации);
– экосистема стартапов (в России доминируют госкорпорации и крупные компании, а не независимые стратапы).

Таким образом, российский рынок кибербезопасности активно развивается, следуя мировым трендам, но отличается ускоренным импортозамещением, вынужденным развитием в качестве объекта постоянных усиленных атак в условиях санкционных ограничений.

В подобных условиях перспективы развития российской практики в области кибербезопасности видятся в следующем:
– дальнейшее активное импортозамещение;
– дальнейшее усиление регуляторного давления как стимула к росту зрелости процессов обеспечения кибербезопасности компаний;
– рост инвестиций в киберустойчивость компаний;
– усиление контроля за безопасностью внешних партнёров и поставщиков информационных услуг;
– развитие сервисных и гибридных моделей, облачных платформ для малого и среднего бизнеса;
– усиление практики тестирования;
– повышение уровня образованности населения в области кибербезопасности;
– подготовка специалистов в области киберустойчивости компаний;
– развитие отечественного генеративного искусственного интеллекта;
– внедрение отечественного искусственного интеллекта в анализ аномалий и противодействие кибератакам и фроду;
– совершенствование управленческого учёта компаний для выстраивания прозрачных профилей рисков, выявления внутренних сигналов в противодействии фроду;

- создание государственных инициатив и платформ для обмена опытом между бизнесом и государством, особенно в рамках защиты критически важной инфраструктуры и промышленности;
- переход от концепции защиты от атак к способности быстрому восстановлению и минимизации ущерба, т.е. к киберустойчивости.

Первостепенным движением является ускорение импортозамещения в области информационных технологий и, в частности, в области кибербезопасности компаний. Это позволит обеспечить технологический суверенитет и экономическую безопасность российских компаний. А кибербезопасность будет рассматриваться не как вынужденная статья расходов, а как фактор устойчивости и конкурентоспособности.

С целью отслеживания скорости и качества процесса в рамках данной статьи предлагается проводить мониторинг индекса зрелости импортозамещения.

Данный индекс позволит не просто фиксировать факт перехода на отечественные средства защиты информации, но и количественно оценивать его влияние на устойчивость предприятий. Оценку предлагается проводить по четырём направлениям: техническая функциональность, соответствие регуляторным требованиям, влияние на внутренние бизнес-процессы, экономическая эффективность. Каждому направлению конкретное предприятие присваивает весовой коэффициент в зависимости от специфики своей отрасли. Итоговый индекс рассчитывается как взвешенная сумма оценок. Для получения более полного представления о процессе импортозамещения предлагается проводить мониторинг по типам угроз (внешние угрозы, риски цепочек поставок, мобильные рабочие места, инсайдерские угрозы) и уровням инфраструктуры (физический, канальный, сетевой, транспортный, сеансовый, прикладной).

Заключение

Растущая частота и стоимость киберинцидентов, свидетельствующие о росте сложности и непредсказуемости киберпространства, создают реальные угрозы для макроэкономической устойчивости стран. Нарастание киберрисков, вызванное усилением взаимосвязанности сложных систем, стремительным развитием искусственного интеллекта, геополитической неопределенностью и нарушениями в цепочках поставок стало стратегическим системным вызовом (технологическим, экономическим и социальным) для благополучия многих стран. Очевидна необходимость переоценки киберстратегий, которую можно назвать сдвигом в парадигме кибербезопасности компаний, их экосистем, национальных и мировой экономики.

Кибербезопасность призвана не только снижать риски и предотвращать (минимизировать) потери, но главное – обеспечить устойчивое развитие экономическим системам в долгосрочной перспективе, стимулируя инновации, создание рабочих мест и повышение конкурентоспособности. Инвестиции в надежное управление киберрисками и стратегии обеспечения устойчивого развития поддерживают национальную безопасность России и способны укрепить основы киберустойчивой экономики.

Литература

1. Захаров В.Я. и др. Безопасность сложных экономических систем: управление рисками их цифровой трансформации // Экономический анализ: теория и практика. 2021. Т. 20. Вып. 4. С. 592-623. DOI: 10.24891/ea.20.4.592 EDN: DXTAYS.

2. World Economic Forum (2026). Global Cybersecurity Outlook 2026. [Электронный ресурс]. URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2026/ (дата обращения 22.06.2026).

3. World Economic Forum (2025). Global Cybersecurity Outlook 2025. [Электронный ресурс]. URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/ (дата обращения 22.06.2026).

4. World Economic Forum. (2025). Artificial intelligence and cybersecurity: Balancing risks and rewards. [Электронный ресурс]. URL: https://reports.weforum.org/docs/WEF_Artificial_Intelligence_ and_Cybersecurity_ Balancing_Risks_and_Rewards_2025.pdf (дата обращения 22.06.2026).

5. The State of AI Risk Management in 2026. URL: https://heimdalsecurity.com/blog/state-ai-risk-management/?utm_source=cybernewswire&utm_medium=pr&utm_campaign=ai-risk-report-2026&utm_content=report (дата обращения 22.06.2026).

6. SpyCloud 2026 Phishing Pulse Report. [Электронный ресурс]. URL: https://spycloud.com/resource/report/phishing-pulse-report-2026/?utm_medium= pr&utm_source=cybernewswire&utm_campaign=phishing-pulse-report-2026 (дата обращения 22.06.2026).

7. World Economic Forum. (2025) Fighting cyber-enabled fraud: A systemic defense approach. [Электронный ресурс]. URL: https://www.weforum.org/publications/fighting-cyber-enabled-fraud-a-systemic-defence-approach / (дата обращения 22.06.2026).

8. Распоряжение Правительства РФ от 20 мая 2023 г. № 1315-р «Об утверждении Концепции технологического развития на период до 2030 г.». [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/406831204/?ysclid= mqm44dzrq3985273065 (дата обращения 22.06.2026).

9. World Economic Forum. (2025). The Cyber Resilience Compass: Journeys towards resilience. [Электронный ресурс]. URL: https://www.weforum.org/publications/the-cyber-resilience-compass-journeys-towards-resilience (дата обращения 22.06.2026).

10. Calculating the real cost of cyber insecurity: Addressing the data deficit, 2025. [Электронный ресурс]. URL: https://www.cybereconomics.org/post-details/calculating-the-real-cost-of-cyber-insecurity (дата обращения 22.06.2026).

11. United Kingdom Department for Science, Innovation & Technology. (2025). Summary of research on the economic impact of cyber-attacks. [Электронный ресурс]. URL: https://www.gov.uk/government/publications/independent-research-on-the-economicimpact-of-cyber-attacks-on-the-uk/summary-of-research-on-the-economic-impact-of-cyber-attacks (дата обращения 22.06.2026).

12. World Bank (2024). Cybersecurity Economics for Emerging Markets. [Электронный ресурс]. URL: https://openknowledge.worldbank.org/server/api/core/bitstreams/719698c9-b21b-4dd4-a875-bfc34b2961ce/content (дата обращения 22.06.2026).

13. Рынок информационной безопасности России: текущее состояние и перспективы развития до 2031 года / Центр стратегических исследований. Москва. 2026. [Электронный ресурс]. URL: https://www.csr.ru/ru/research/ezhegodnoe-issledovanie-rynka-informatsionnoy-bezopasnosti-ib/ (дата обращения 22.06.2026).

14. Авезова Я., Резников Р., Беседина В. PT Cyber Analytics. CODE RED 2026: Актуальные киберугрозы для российских организаций. [Электронный ресурс]. URL: https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/#id43 (дата обращения 22.06.2026).

15. Кибератаки на российские компании в 2025 году. ГК «Солар». [Электронный ресурс]. URL: https://rt-solar.ru/analytics/reports/6432/ (дата обращения 22.06.2026).