Совместно с
Accenture

WORLD ECONOMIC FORUM

Обзор мировых тенденций в сфере кибербезопасности на 2025 год

АНАЛИТИЧЕСКИЙ ДОКЛАД

ЯНВАРЬ 2025 г.

Иллюстрации: Getty Images

Содержание

Предисловие

Джереми Юргенс (Jeremy Jurgens)
Управляющий директор Всемирного экономического форума

Паоло Даль Чин (Paolo Dal Cin)
Руководитель по безопасности, компания Accenture

После нескольких десятилетий относительной стабильности в мире нарастает геополитическая напряженность. Это отражается и в цифровом мире — киберпреступники становятся все искуснее, новые технологии развиваются все быстрее, а набор возможностей расширяется, поэтому киберпространство непрерывно усложняется. В этих условиях Обзор мировых тенденций в сфере кибербезопасности поможет руководителям разобраться во всех хитросплетениях и составить план создания устойчивых экосистем.

Прошлогодний отчет показал огромный разрыв между лидерами в сфере кибербезопасности и отстающими организациями с ограниченными ресурсами. Несмотря на то, что все больше руководителей сегодня осознают риски кибербезопасности, сложности ландшафта киберугроз только усугубляют это неравенство. Во взаимозависимых цепочках поставок слабые звенья становятся причиной системных сбоев, которые заметно влияют на общую устойчивость всей экосистемы.

В области кибербезопасности искусственный интеллект (ИИ) открывает не только большие возможности, но и сопряжен с серьезными угрозами. Организации внедряют ИИ, а киберпреступники стараются опередить их и использовать уязвимости, постоянно совершенствуя свои методы. В этой гонке организации стараются использовать ИИ, чтобы сместить баланс сил в свою пользу.

В будущем системы будут только усложняться. Мы ожидаем, что государство и частный сектор будут тесно сотрудничать, чтобы в безграничном киберпространстве все могли безопасно использовать цифровые технологии во благо. Это призыв к действию, и действовать нужно прямо сейчас.

Краткий обзор

В условиях геополитической нестабильности, нарастающего неравенства между организациями и все усложняющихся киберугроз руководители должны сделать безопасность своим приоритетом.

Главной темой Обзора мировых тенденций в сфере кибербезопасности (GCO) на 2024 год был разрыв между лидерами и отстающими. В отчете за этот год рассматривается возрастающая сложность киберландшафта, которая будет иметь серьезные и долгосрочные последствия не только для организаций, но и для целых стран.

На это влияет целая комбинация факторов:

– Геополитические конфликты приводят к росту неопределенности.

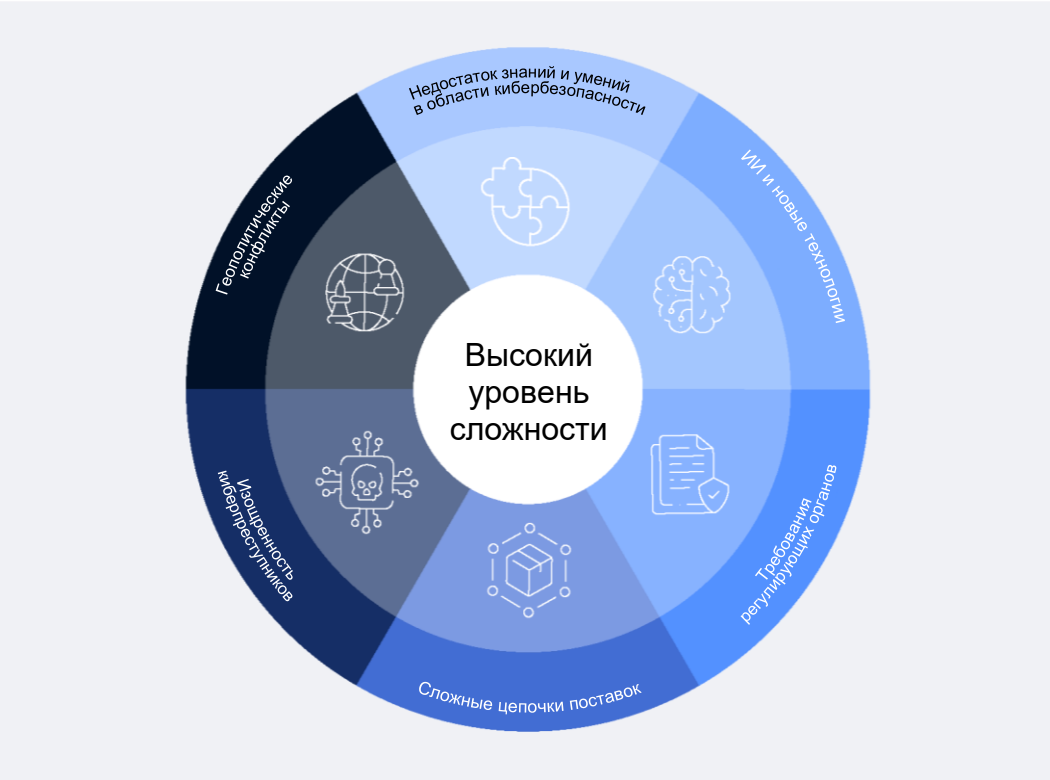
– Усложнение и более тесная интеграция цепочек поставок приводит к непредсказуемым рискам и отсутствию прозрачности.

– Быстрое внедрение новых технологий приводит к возникновению новых уязвимостей, которыми киберпреступники успешно пользуются для проведения все более изощренных и масштабных атак.

– Одновременно с этим регуляторы по всему миру вводят все больше требований, и организациям приходится принимать дополнительные меры для их выполнения.

Ситуация осложняется нехваткой квалифицированных кадров, поэтому управлять киберрисками становится еще труднее.

РИС. A **Факторы, затрудняющие обеспечение кибербезопасности**



Растущая сложность киберландшафта усугубляет неравенство в этой сфере — между крупными и малыми организациями, развитыми и развивающимися странами, государственным и частным сектором.

По данным исследований, руководители **35 %** небольших организаций испытывают трудности с обеспечением должного уровня кибербезопасности. С 2022 года этот показатель увеличился в семь раз. Напротив, количество руководителей крупных организаций, столкнувшихся с подобной проблемой, уменьшилось почти вдвое.

РИС. B **Организации с недостаточным уровнем кибербезопасности (согласно опросу)**

На Ежегодной конференции по кибербезопасности в 2024 году 71 % руководителей заявили, что малые организации уже достигли предела своих возможностей и не способны эффективно противостоять растущим киберрискам.

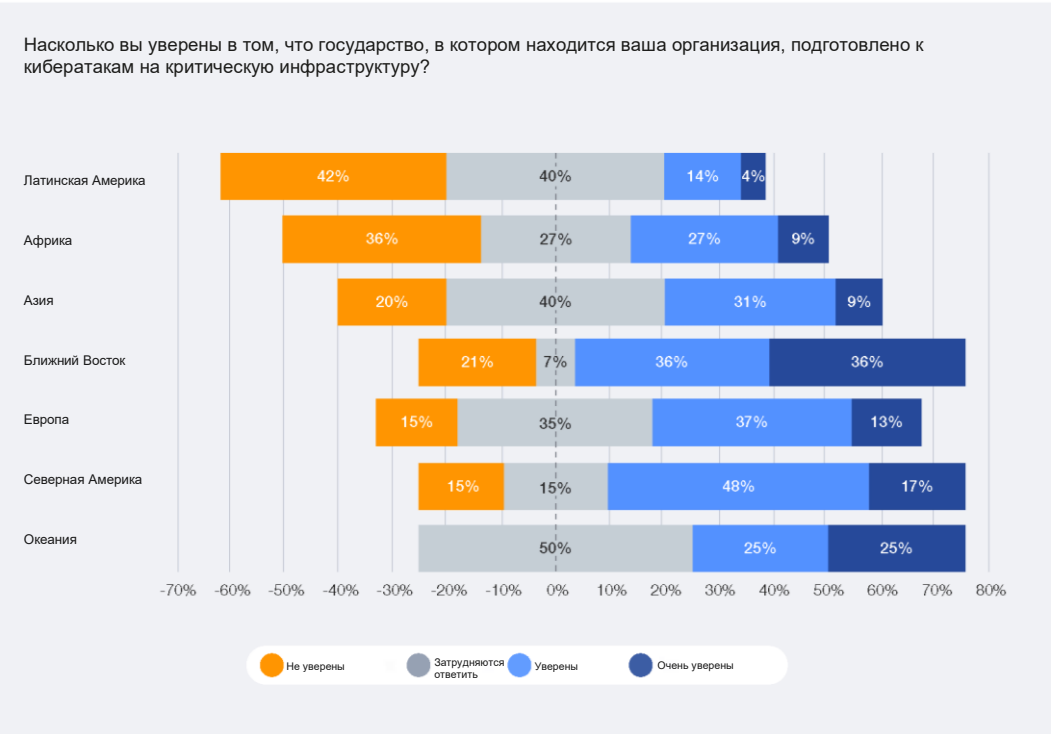
Неравенство прослеживается также и между регионами: в Европе и Северной Америке только 15 % руководителей не уверены в способности государства противостоять серьезным киберинцидентам, нацеленным на критическую инфраструктуру, тогда как в Африке так считает 36 % респондентов, а в Латинской Америке — 42 %.

Разрыв наблюдается и между секторами. Так, в государственном секторе недостаточную устойчивость к киберрискам отмечают 38 % респондентов, тогда как в частном секторе опасения выразили только 10 % руководителей средних и крупных предприятий.

Неравенство распространяется и на кадры: 49 % организаций государственного сектора заявили, что им не хватает специалистов для достижения своих целей в сфере кибербезопасности, что на 33 % больше, чем в 2024 году.

В Обзор мировых тенденций в сфере кибербезопасности на 2025 год входит более глубокий анализ самых важных факторов, влияющих на сложность ландшафта угроз, а также предоставляется ценная аналитика по критическим задачам на предстоящий год и действиям, ожидаемым от руководителей.

РИС. C **Неравенство между регионами**



Далее приводятся ключевые выводы из отчета на этот год и главные тенденции, на которые руководителям следует обратить внимание в 2025 году:

Уязвимости в цепочке поставок становятся главным источником киберрисков в экосистеме

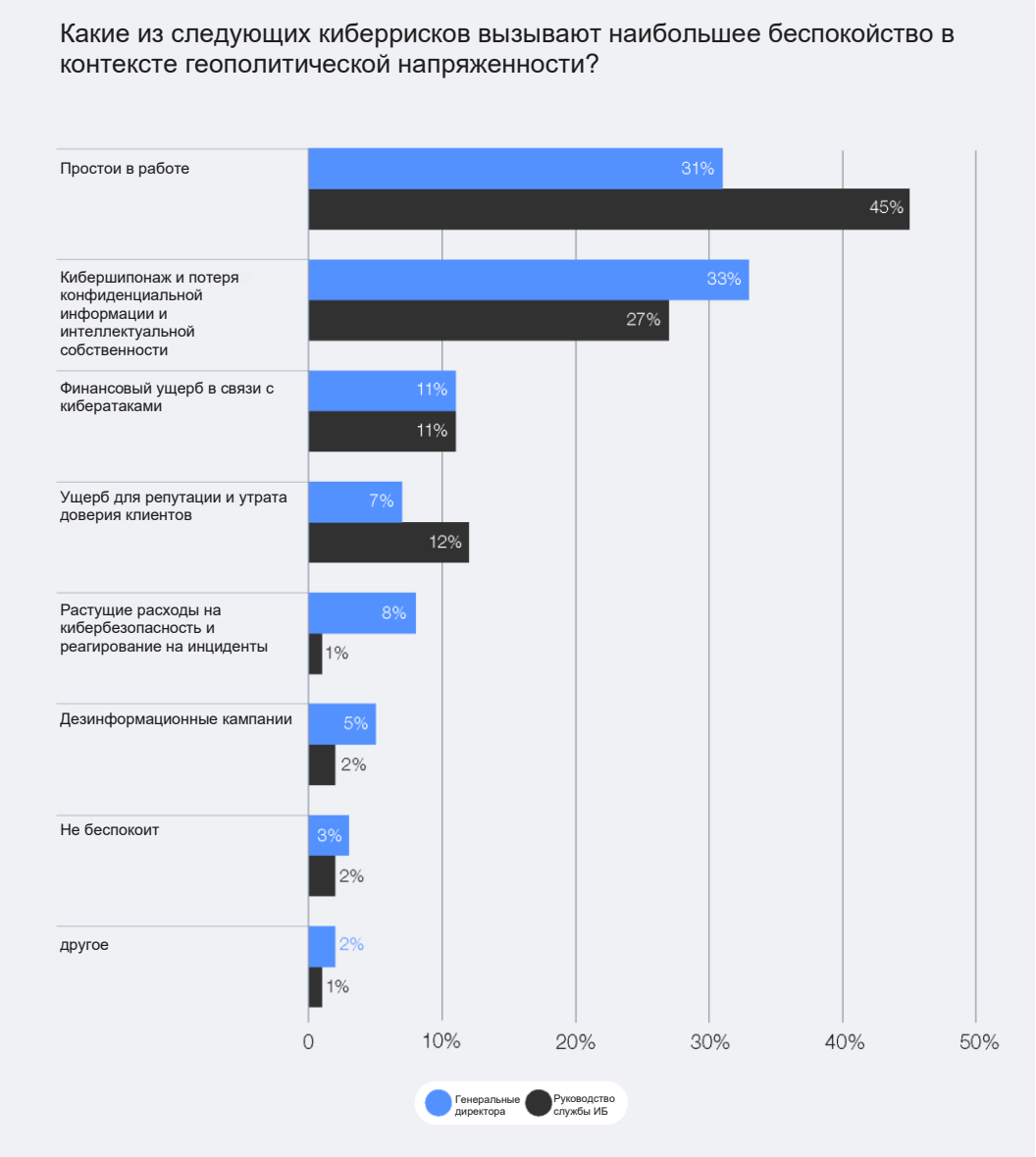
По данным опроса, проведенного среди руководителей крупных компаний, **54 %** из них считают, что одной из причин уязвимости к киберрискам являются цепочки поставок. Организации не могут контролировать уровень безопасности каждого поставщика в сложной цепочке поставок, а потому она становится главным источником киберрисков.

Главные проблемы: уязвимости в программном обеспечении, вводимые третьими сторонами, и распространение кибератак по экосистеме.

Как геополитическая напряженность влияет на стратегию кибербезопасности.

Почти **60 %** руководителей отмечают, что мировые конфликты влияют на их стратегию кибербезопасности. Геополитическая нестабильность также влияет на восприятие рисков: каждый третий генеральный директор среди основных проблем называет кибершпионаж и кражу конфиденциальной информации и интеллектуальной собственности, а 45 % руководителей по кибербезопасности беспокоятся о простоях в работе.

РИС. D **Влияние геополитической напряженности на стратегии кибербезопасности**

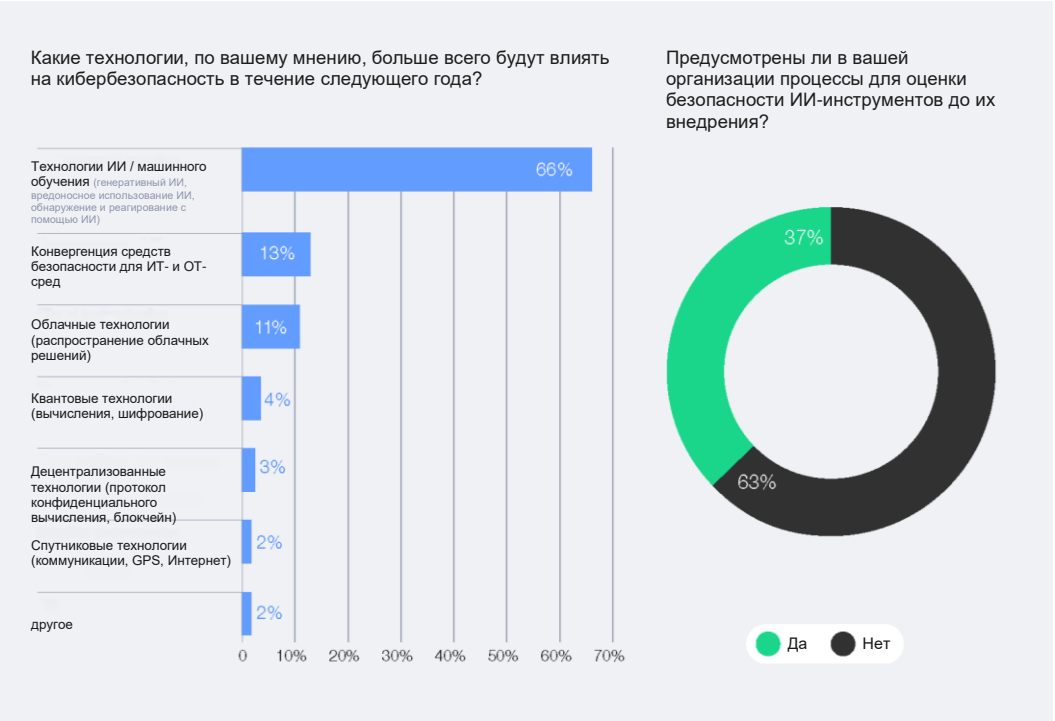


Быстрое внедрение ИИ приводит к новым уязвимостям

По мнению **66 %** опрошенных, в этом году ИИ окажет самое значительное влияние на кибербезопасность. Однако лишь **37 %** респондентов утверждают, что у них есть процессы, позволяющие оценить безопасность ИИ-инструментов до их внедрения.

Парадокс в том, что многие признают ИИ как серьезный фактор риска, но при этом внедряют эти технологии без надлежащих мер защиты.

РИС. E **Главные уязвимости в 2025 году**



Генеративный ИИ дает киберпреступникам новые возможности, например для социальной инженерии

Около **72 %** респондентов отмечают увеличение киберрисков, причем больше всего беспокойства по-прежнему вызывают вирусы-вымогатели. Почти **47 %** руководителей считают, что генеративный ИИ позволяет проводить более сложные и масштабные атаки.

В 2024 году резко возросло число атак с применением фишинга и социальной инженерии — об инцидентах сообщили **42 %** респондентов.

Регуляторы вводят новые требования, но их выполнение требует от организаций дополнительных усилий

Требования регуляторов помогают повысить уровень кибербезопасности и укрепить доверие,

однако они так многочисленны и противоречивы, что более **76 %** руководителей служб информационной безопасности (Chief Information Security Officers, CISOs) на Ежегодной конференции по кибербезопасности в рамках Всемирного экономического форума в 2024 году отметили, что организациям трудно соблюдать все требования в разных странах и регионах.

Организациям не хватает специалистов по кибербезопасности

С 2024 года нехватка кадров возросла на **8 %**, причем две трети респондентов отмечают уровень нехватки от умеренного до критического, в том числе говорят об отсутствии важных навыков для выполнения критических требований безопасности.

Более того, только **14 %** организаций уверены, что у них есть все необходимые специалисты со всеми необходимыми навыками.

1 Сложное устройство киберпространства

По мере усложнения киберпространства усугубляется неравенство между лидерами и организациями, неспособными противостоять растущим угрозам.

Нарастание геополитической напряженности, быстрое развитие новых технологий и появление все более изощренных векторов атак — все это способствует усложнению киберландшафта.

Кроме того, при обеспечении безопасности организации сталкиваются с такими трудностями, как изменение требований регуляторов, уязвимости в сложных цепочках поставок и нехватка кадров. При этом ставки очень высоки.

1.1 Усугубление неравенства

72 %

респондентов сообщают о повышении киберрисков.

Согласно Обзору мировых тенденций в сфере кибербезопасности за 2024 год существует серьезный разрыв между возможностями небольших и крупных организаций. По данным глобального отчета о рисках Всемирного экономического форума за 2024 год, киберриски затрагивают все страны и временные горизонты, причем вредоносное ПО, дипфейки и дезинформация представляют угрозу для цепочек поставок, финансовой стабильности и демократических систем. Как показал опрос директоров по управлению рисками в октябре 2024 года, киберриски вошли в тройку самых серьезных угроз для организации. Подавляющее большинство (71 %) респондентов опасаются, что киберриски и киберпреступления приведут к серьезным перебоям в работе организации.

В 2024 году произошла крупнейшая ИТ-катастрофа в истории, когда остановилась работа авиакомпаний, банков, телекомпаний, медицинских учреждений, платежных систем и банкоматов по всему миру, что привело к убыткам в размере 5 млрд долларов США. Этот инцидент подчеркнул, как рискованно зависеть от ограниченного числа поставщиков критически важных услуг. В Обзоре мировых тенденций в сфере кибербезопасности (Global Cybersecurity Outlook, GCO) (см. Приложение: методология) 72 % респондентов отметили рост киберрисков, причем растет не только частота, но и изощренность кибератак. Особенно выделяются атаки с применением вирусов-вымогателей, тактики на основе ИИ (фишинг, вишинг, дипфейки) и значительный рост числа атак на цепочку поставок.

1.2 Ожидания на предстоящий год

Отчет на 2025 год выявил ряд факторов, влияющих на усложнение киберландшафта:

- Геополитические конфликты приводят к росту неопределенности.
- Усложнение и более тесная интеграция цепочек поставок приводят к непредсказуемым рискам и отсутствию прозрачности.
- Быстрое внедрение новых технологий приводит к возникновению новых уязвимостей и угроз.

Тем временем регуляторы по всему миру вводят все больше требований, и организациям приходится принимать дополнительные меры для их выполнения. Ситуация осложняется нехваткой квалифицированных кадров, поэтому управлять киберрисками становится еще труднее.

В совокупности эти факторы повышают сложность и непредсказуемость киберландшафта и значительно влияют на бизнес.

Во-первых, они приводят к усугублению неравенства между лидерами и отстающими организациями, которым не хватает ресурсов для адаптации к новым угрозам. Этот разрыв влияет на устойчивость всей экосистемы, поскольку крупные и лучше подготовленные организации обычно зависят от обширной сети более мелких поставщиков с ограниченными возможностями, и любой инцидент у поставщика может повлиять на всю цепочку поставок. Во-вторых, в сфере кибербезопасности усиливается кадровый голод. Чтобы не отставать от развития технологий, требуются специфические навыки, которыми пока обладают немногие специалисты. При этом из-за сложности возрастает давление на уже и так перегруженные команды кибербезопасности.

Учитывая все эти трудности, для выживания в сложном ландшафте угроз требуется полностью пересмотреть стратегии кибербезопасности на уровне организации и целой экосистемы. Необходимо понимать, что киберриски влияют не только на ИТ-системы, но и на весь бизнес.

РИС. 1 | **Факторы, затрудняющие обеспечение кибербезопасности**

> **В условиях роста киберугроз и расширения поверхности атаки традиционные подходы к безопасности принесут мало пользы. Организации пытаются управлять десятками разрозненных решений и политик по всей сети, в облаке и на конечных устройствах. В результате люди — наш самый ценный ресурс — вручную сортируют оповещения, пока атаки, напротив, все больше автоматизируются. Чтобы опередить злоумышленников и лишить их технического преимущества, нам нужно пересмотреть подход к кибербезопасности и шире использовать потенциал ИИ.**
> Никеш Арора (Nikesh Arora), председатель совета директоров и генеральный директор в Palo Alto Networks

РИС. 2 | **Усложнение киберландшафта**

Геополитические конфликты

Геополитическая напряженность влияет на киберстратегию почти 60 % организаций. Каждый третий генеральный директор среди основных проблем называет кибершпионаж, а также кражу конфиденциальной информации и интеллектуальной собственности.

Изощренность киберпреступников

72 % респондентов отмечают рост киберрисков за последний год, особенно это касается мошенничества с применением кибертехнологий: фишинг, социальная инженерия и кража идентификационных данных.

Сложные цепочки поставок

54 % респондентов из крупных организаций говорят о сложности управления рисками, связанными с третьими сторонами, — цепочка поставок остается серьезным источником киберрисков.

Требования регулирующих органов

78 % руководителей частных организаций считают, что регуляторные требования в сфере кибербезопасности и защиты персональных данных эффективно сокращают риски во всей экосистеме. При этом две трети респондентов беспокоятся по поводу сложности и многообразия таких требований.

ИИ и новые технологии

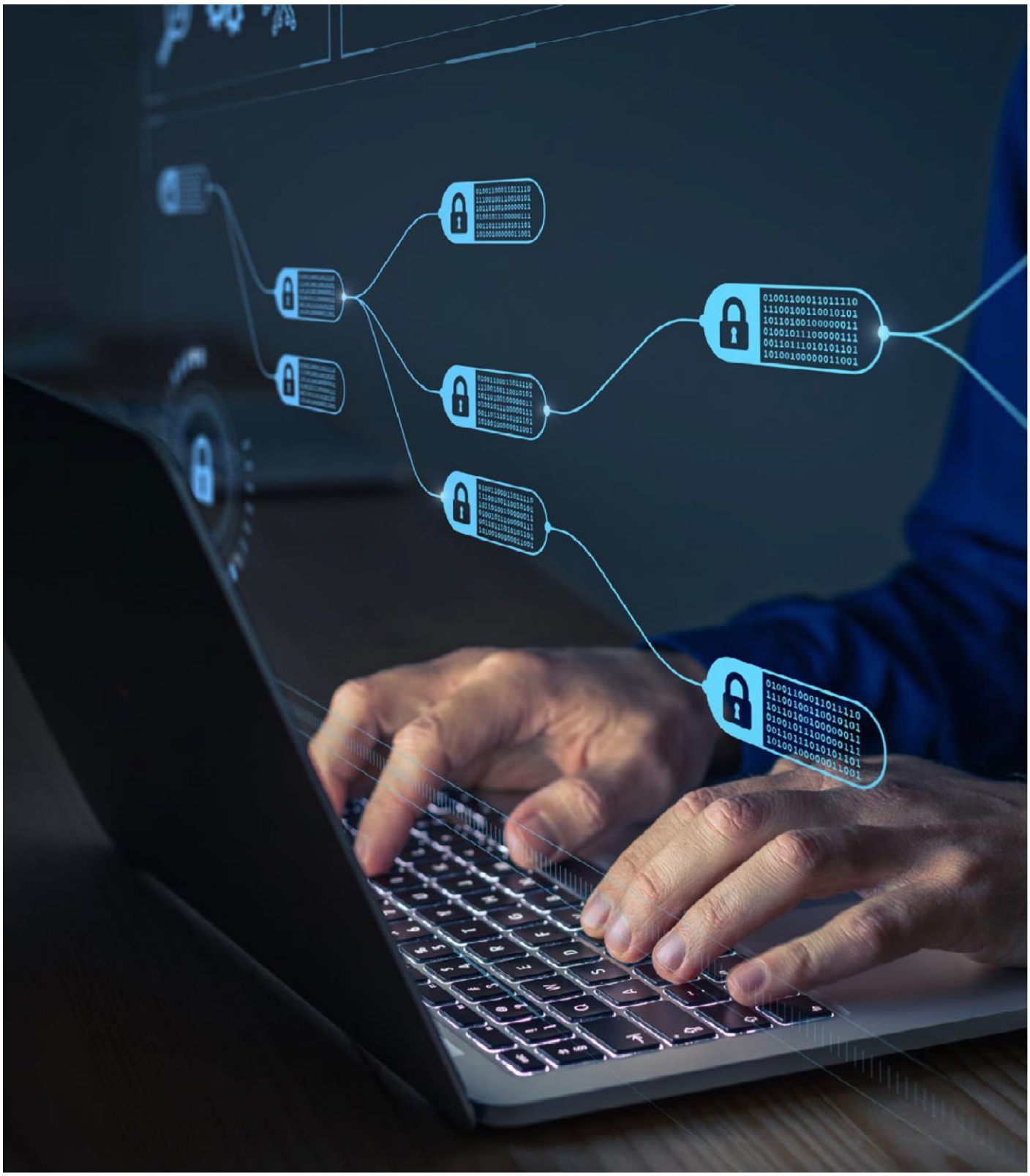
66 % респондентов полагают, что в следующем году ИИ будет влиять на кибербезопасность, но только 37 % используют процессы для безопасного внедрения ИИ.

Недостаток знаний и умений в области кибербезопасности

Нехватка специалистов усугубилась по сравнению с прошлым годом, причем две трети респондентов отмечают уровень нехватки от умеренного до критического. Только 14 % организаций уверены, что у них есть все необходимые специалисты со всеми требуемыми навыками.

2 Факторы сложности

Киберпреступники осваивают новые сложные инструменты, и развивающийся ландшафт угроз требует инновационных стратегий для борьбы со все более изощренными и масштабными атаками.



2.1 Ландшафт киберугроз

Эволюция киберпреступности

Вирусы-вымогатели по-прежнему входят в топ рисков для организаций — в опросе этого года их назвали 45 % респондентов. По мнению участников Ежегодной конференции по кибербезопасности в 2024 году, атаки с применением вирусов-вымогателей выйдут на новый уровень. Ситуация осложняется распространением вирусов-вымогателей, предоставляемых как услуга (Ransomware-as-a-Service, RaaS), поскольку для применения этой тактики не нужно быть техническим специалистом.

Мошенничество с применением кибертехнологий занимает второе место среди киберрисков для организаций на 2025 год — генеральные директора опасаются его наряду с вирусами-вымогателями и сбоями в цепочках поставок. Главным личным киберриском руководители служб ИБ и генеральные директора выбрали кражу идентификационных данных.

РИС. 3 **Организационные киберриски на 2025 год (в порядке важности)**

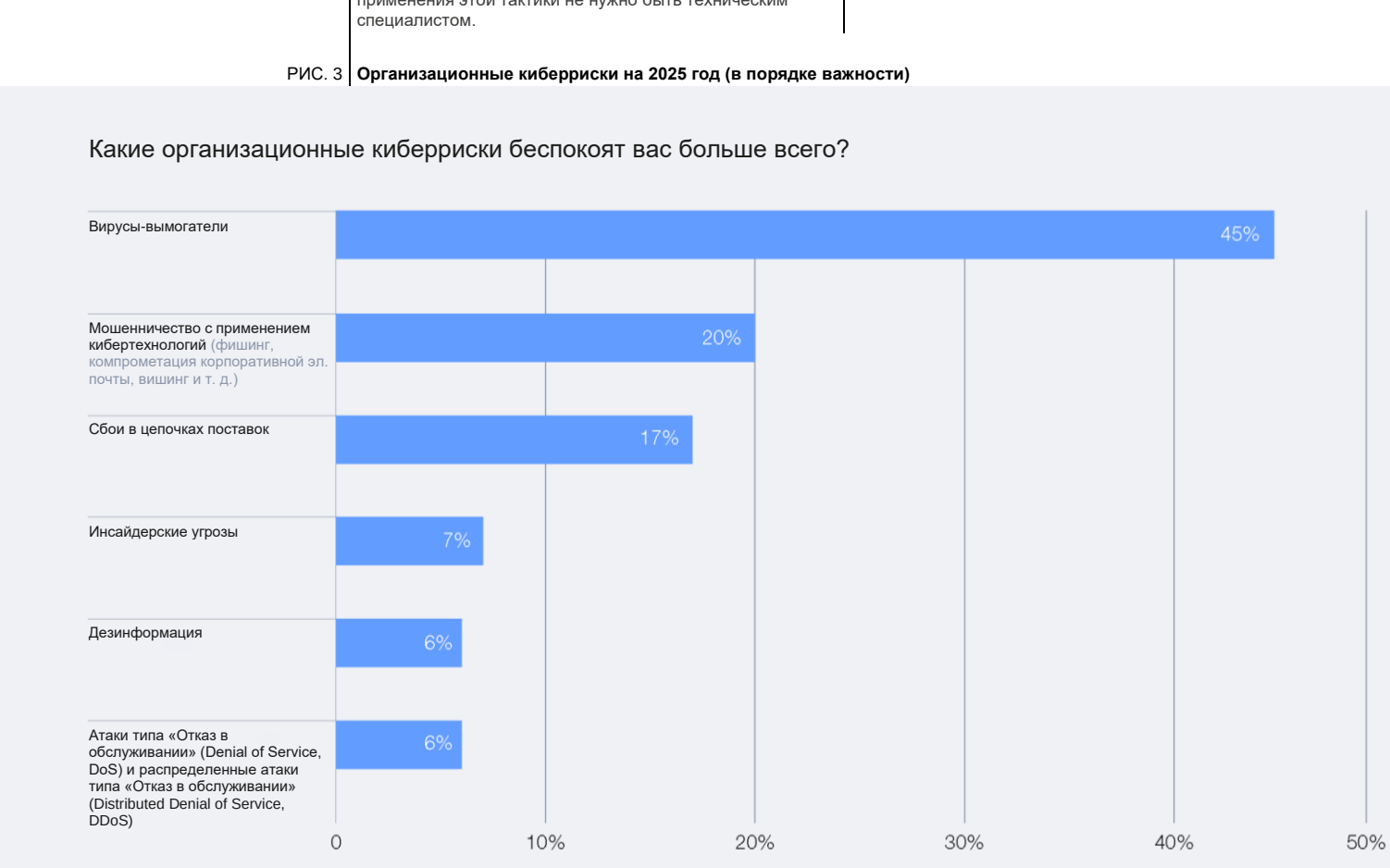


РИС. 4 | **Организационные киберриски с точки зрения гендиректоров и руководителей служб ИБ**

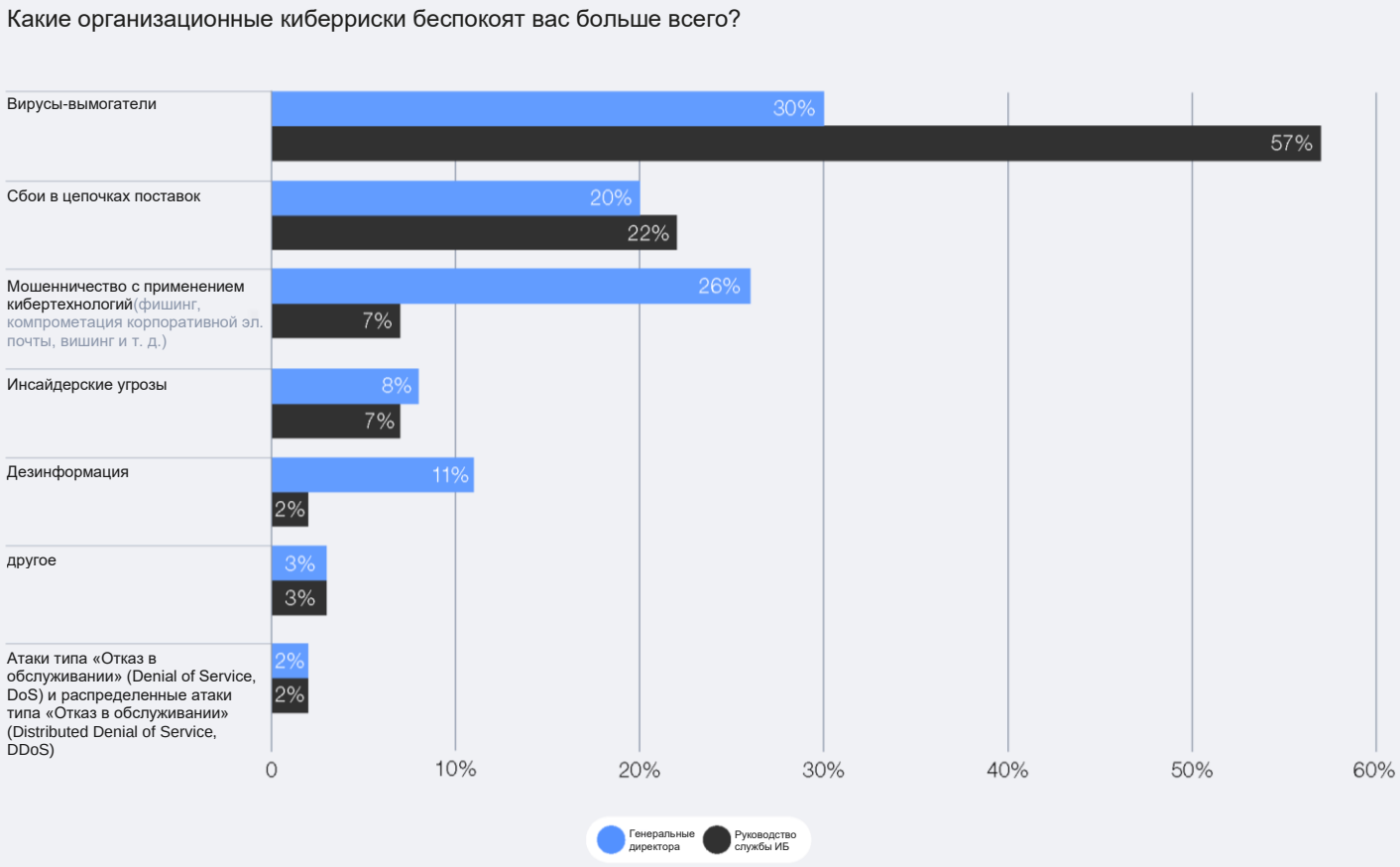
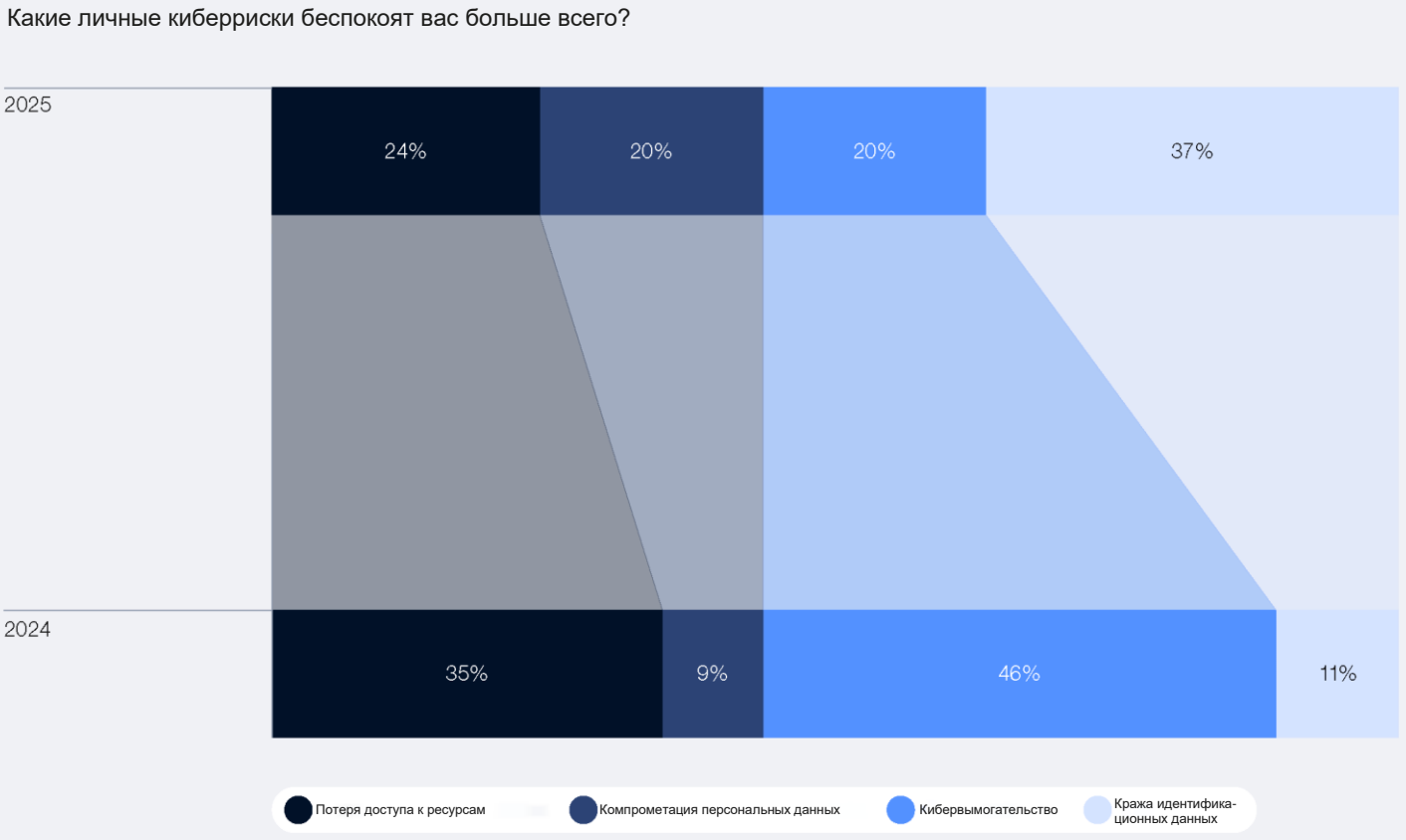


РИС. 5 | **Изменение приоритетов по личным киберрискам: 2024 и 2025 гг.**



Быстрое развитие и внедрение цифровых платформ по всему миру закономерно приводит к развитию ландшафта киберугроз, причем атаки становятся не только масштабнее, но и изощреннее. С расширением цифрового следа расширяется и поверхность атаки. Мы должны совместными усилиями бороться с растущей угрозой. В Интернете нет границ, поэтому организации и правительства должны сотрудничать, чтобы не оставить злоумышленникам ни одного шанса.
Иван Джон Е. Уй (Ivan John E. Uy), Секретарь Департамента информационных и коммуникационных технологий Филиппин

Злоумышленники используют новые инструменты для повышения эффективности и масштаба традиционных видов атак, таких как вымогательство с помощью вирусов и компрометация корпоративной электронной почты (Business Email Compromise, BEC). Генеративный ИИ сокращает расходы на кампании с применением фишинга и социальной инженерии, упрощая преступникам доступ к ресурсам организации. Организациям следует приложить дополнительные усилия для защиты от таких привычных форм атаки, как фишинг и кибермошенничество, потому что сейчас они гораздо лучше подготовлены.

Бизнес-модель «кибератаки как услуга» (Cybercrime-as-a-Service, CaaS) продолжает набирать популярность, поскольку даже преступники без технических навыков могут заниматься незаконной деятельностью с помощью купленных инструментов и инструкций. Эта успешная модель внедряется и в других областях киберпреступлений, например используется для фишинговых атак с применением ИИ. Подобные платформы представляют собой серьезную проблему, так как устраняют барьеры для киберпреступников. Правоохранительные органы борются с CaaS-платформами, но пока их успехи незначительны.

Организованная киберпреступность

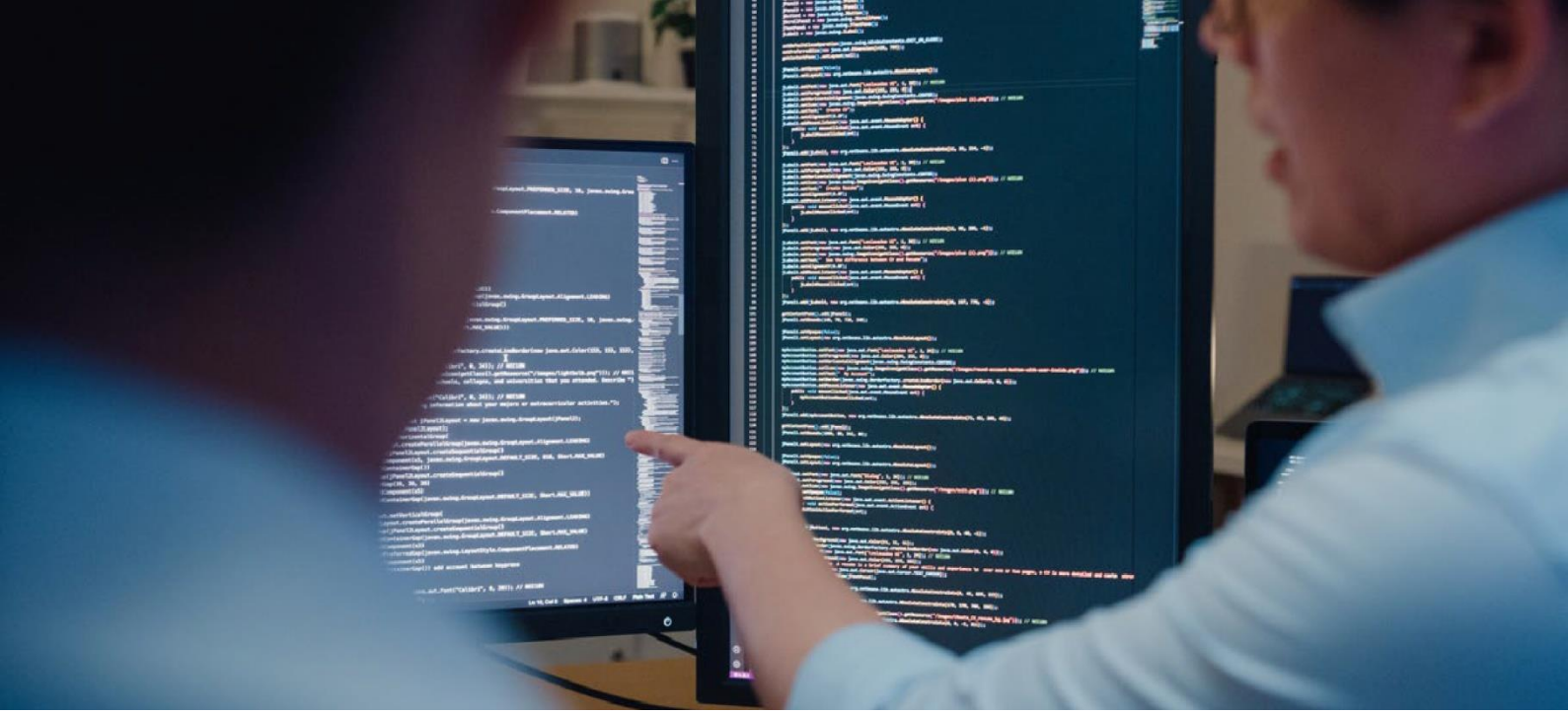
Кибермошенничество так распространилось и стало настолько выгодным, что привлекло внимание обычных организованных преступных групп. Их вмешательство влияет на характер киберпреступлений и повышает их воздействие на общество.

Один из ужасных примеров таких преступлений — принудительный труд более 220 тысяч человек на скам-фермах в Юго-Восточной Азии. Эти фермы, используемые для сбора данных, дезинформации, социальной инженерии и совершения других преступлений, по сути, предоставляют «преступные услуги».

По данным Global Anti-Scam Alliance, в прошлом году мошенники по всему миру выманили более 1 трлн долларов США, а некоторые страны потеряли более 3 % ВВП.

Выход традиционных преступных групп на киберарену меняет саму природу киберпреступлений. Организованные преступные группы не боятся причинить физический вред и не беспокоятся о перебоях в работе критических социальных служб, например медицинских учреждений. Этот «культурный» сдвиг в сочетании с распространенностью CaaS-платформ приводит к тому, что мишенью для атаки, например с целью вымогательства, может стать почти любая организация.

Киберпреступления и ландшафт угроз постоянно развиваются, и мы рискуем не только деньгами — эта разрушительная сила затрагивает общество. Мы обязаны проявлять бдительность и сотрудничать с представителями разных отраслей, чтобы защитить будущее цифрового мира. Киберпреступления мешают работе, подрывают уверенность и нарушают работу бизнеса и критической инфраструктуры. В этом году мы должны не просто реагировать на атаки, но действовать на упреждение, применять систематические подходы и объединять усилия, чтобы обеспечить устойчивость к киберугрозам и защитить наше общее будущее.
Кен Си (Ken Xie), основатель, председатель совета директоров и генеральный директор Fortinet



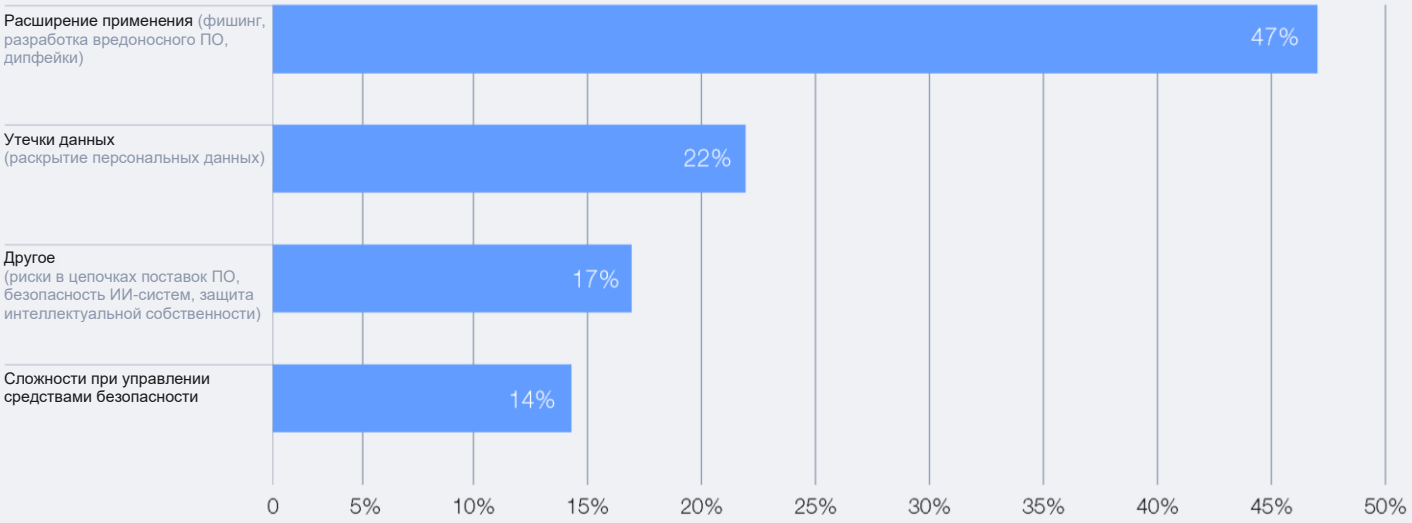
Использование ИИ в киберпреступности

Генеративный ИИ меняет киберландшафт, поскольку с его помощью преступники совершенствуют свои методы, автоматизируют атаки и персонализируют подход к жертвам. 47 % респондентов выражают беспокойство по поводу применения генеративного ИИ в преступных целях, и преступники действительно широко используют его в своих схемах.

Около 42 % респондентов признались, что в прошлом году их организация стала жертвой социальной инженерии, — этот показатель только вырастет с развитием ИИ, поскольку его будет осваивать все больше преступников.

РИС. 6 **Применение генеративного ИИ для киберпреступлений**

Какие киберриски, связанные с генеративным ИИ, беспокоят вас больше всего?



С помощью генеративного ИИ киберпреступники убедительно имитируют стиль письма высшего руководства организации. ИИ опирается на контекстные данные из социальных сетей, публичных заявлений, похищенных документов и других источников, и такие атаки с применением социальной инженерии гораздо сложнее распознать.

Генеративный ИИ помогает преступникам применять техники социальной инженерии на разных языках, а значит без лишних затрат расширять охват, обманывая людей из разных стран.

Используя технологии генеративного ИИ, злоумышленники могут создавать убедительные подделки голоса, видео, изображений и стиля письма высших должностных лиц. Если специальный персонал долго не распознает эти дипфейки, злоумышленники могут использовать их для обмана организаций или получения доступа к информационным системам. Исследование Accenture показало, что продажа инструментов, связанных с созданием дипфейков, на форумах в даркнете выросла на 223 % с первого квартала 2023 года по первый квартал 2024 года.

Также на Ежегодной конференции по кибербезопасности 2024 года 55 % руководителей служб информационной безопасности заявили, что для их организации дипфейки представляют собой киберугрозу среднего или даже значительного уровня. Поскольку персонал остается основной мишенью дипфейковых атак и фишинговых кампаний в целом, организациям необходимо пересмотреть подход к обучению и защите от новых методов киберпреступности всех своих работников — от рядовых сотрудников до топ-менеджеров.

Будучи мировыми лидерами, мы рассматриваем киберпространство не только как источник опасности, но и как инструмент для реальных преобразований в сфере обеспечения безопасности людей и организаций. Вредоносная киберактивность причиняет значительный вред наиболее уязвимым группам населения. Поэтому нам необходимо как можно скорее внедрять решения на уровне экосистем, которые объединят всех — от небольших местных компаний до крупных глобальных корпораций. Совместными усилиями мы сможем коренным образом изменить ситуацию в 2025 году, осуществив масштабные изменения и разработав систему цифровой безопасности, которая будет доступна для всех.
Филип Райнер (Philip Reiner), генеральный директор и основатель Института безопасности и технологий

В конечном счете генеративный ИИ упрощает вход на арену киберпреступности, снижая как финансовые расходы, так и требования к уровню подготовки специалистов. Предполагается, что генеративный ИИ упростит процесс обнаружения уязвимостей в системе и распространения вредоносных программ. Это позволит проводить операции в более крупном масштабе, чем было возможно ранее, когда все зависело только от человеческих возможностей.

Осознавая опасность киберугроз и мотивы, которые побуждают киберпреступников к действиям, компании могут более точно определить риски, с которыми они сталкиваются. Это поможет им скорректировать свои стратегии безопасности и расставить приоритеты, чтобы стать более защищенными от подобных угроз.

В условиях постоянно меняющихся методов работы злоумышленников и растущего числа киберугроз необходимо применять комплексный подход к обеспечению безопасности. Ответные меры требуют взаимодействия не только между органами правопорядка различных государств, но и с экспертами в области кибербезопасности, обладающими специальными навыками, опытом и знаниями. В 2024 году Управление ИНТЕРПОЛА по борьбе с киберпреступностью поддержало несколько региональных и глобальных операций по предотвращению киберпреступлений, которые оказались очень успешными во многом благодаря этому сотрудничеству. В преддверии 2025 года наша команда будет активно развивать новые и укреплять уже существующие партнерские связи, чтобы оказывать еще большее влияние на борьбу с киберпреступностью.
Нил Джеттон (Neal Jetton), директор Управления по борьбе с киберпреступностью Международной организации уголовной полиции (ИНТЕРПОЛ)

ТИПИЧНЫЙ ПРИМЕР 1
Старые способы мошенничества и новые технологии – Arup

Компания Arup оказалась в центре внимания прессы, но не по тем причинам, которые можно было бы ожидать. Она стала мишенью преступников, совершивших крупное мошенничество. Один из заголовков гласил: «Мошенники используют технологию deepfake, чтобы обмануть работника на миллионы». Однако история оказалась гораздо сложнее, чем можно было предположить.

Этот случай привлек внимание СМИ очевидно потому, что злоумышленники использовали поддельные видео и голосовые сообщения, чтобы создать иллюзию общения с реальными коллегами. Однако, как отметил Роб Грейг (Rob Greig), директор по информационным технологиям Arup, самое удивительное заключается в том, что злоумышленники не получили доступа к ИТ-сетям компании и не нарушили ее бизнес-процессы. Вероятно, они применяли «передовые методы социальной инженерии», чтобы убедить сотрудников перевести им деньги.

Это была сложная и хорошо продуманная атака, осуществленная с помощью различных методов, таких как фишинг, вишинг и смишинг. Для придания убедительности использовались поддельные документы и создавалось ложное чувство срочности. Но по сути это было обычное платежное мошенничество в современном исполнении.

После произошедшего компания тщательно проанализировала все аспекты своих систем и процессов. Одним из самых важных извлеченных уроков стало осознание того, что недостаточно полагаться только на меры кибербезопасности. Чтобы добиться настоящей устойчивости к киберугрозам, необходима культура критического мышления и умение распознавать тревожные сигналы во всех аспектах деятельности организации.

Однако самым важным уроком является то, что компания, полиция и государственные органы должны найти более эффективные способы обмена информацией и борьбы с мошенниками.

За рамками киберпреступлений: новые угрозы критически важной инфраструктуре и безопасности персонала

С появлением новых технологий кибербезопасность уже не ограничивается только защитой конфиденциальности, целостности и доступности информации. Она включает в себя обеспечение безопасности персонала и должна учитывать реальный риск для жизни людей в случае кибератаки или взлома системы.
Бушра Алблуши (Bushra AlBlooshi), директор Департамента управления рисками в области кибербезопасности Дубайского центра электронной безопасности

Растущая геополитическая напряженность и постоянно совершенствующиеся киберугрозы представляют серьезную опасность для критически важной инфраструктуры, которая работает на основе сетей взаимосвязанных устройств и устаревших систем. Ярким примером таких уязвимостей служит продолжающийся украинский конфликт. Критически важные сектора, такие как энергетика, телекоммуникации, водоснабжение и теплоснабжение, неоднократно подвергались как кибератакам, так и физическим нападениям. Эти атаки нередко нацелены на то, чтобы вывести из строя системы управления и похитить данные, что представляет серьезную угрозу для операционных технологий. С развитием киберугроз они становятся все более серьезными и представляют опасность не только для функционирования систем, но и для безопасности людей, увеличивая серьезность и последствия сбоев в работе жизненно важных объектов инфраструктуры. Ниже перечислены некоторые ключевые области, которые требуют особого внимания из-за высокого уровня риска.

Водные объекты

Кибератаки на водные объекты представляют собой серьезную угрозу для общественной и национальной безопасности, а также для инфраструктуры. Агентство кибербезопасности и безопасности инфраструктуры США (Cybersecurity and Infrastructure Security Agency, CISA) определило эти риски в наборе инструментов, подчеркнув наличие уязвимостей в системах операционных технологий, используемых на водоочистных сооружениях, таких как пункты удаленного доступа и устаревшее программное обеспечение. Киберпреступники могут воспользоваться этими уязвимостями, чтобы нарушить процессы очистки воды, а это может привести к загрязнению, перебоям в обслуживании или другим серьезным проблемам. В октябре 2024 года произошел серьезный инцидент, который вызвал тревогу за безопасность критически важной инфраструктуры. Крупнейший водоканал в Соединенных Штатах подвергся кибератаке, что привело к перебоям в его работе и вызвало опасения за состояние инфраструктуры.

Биотехнологическая безопасность

Стремительный технологический прогресс изменил ландшафт биологических угроз, и на первый план вышла задача обеспечения биотехнологической безопасности. Всемирная организация здравоохранения (ВОЗ) предупреждает, что достижения в области искусственного интеллекта, кибератак и генной инженерии могут представлять собой серьезные угрозы для обеспечения биотехнологической безопасности в мире. В отчете ВОЗ за 2024 год обозначено несколько способов, с помощью которых киберугрозы могут поставить под удар биотехнологическую безопасность. К ним относятся: доступ к конфиденциальным данным или исследованиям; нарушение работы систем защиты в лабораториях; кража или повреждение информации, связанной с обеспечением биотехнологической безопасности; шпионаж с целью получения конкурентных преимуществ или причинения вреда. Кроме того, кибератаки могут вывести из строя ключевые лабораторные системы, что приведет к сбоям в работе и потере данных. Это чревато задержками в проведении важных исследований или нарушениями в протоколах обеспечения безопасности. В течение 2024 года нападениям подверглись две лаборатории в Южной Африке и Великобритании. Эти уязвимости подчеркивают необходимость применения современных методов защиты от киберугроз в рамках стратегий обеспечения биотехнологической безопасности, цель которых — свести к минимуму возрастающие риски.

Однако конфиденциальный характер геномных данных создает новые риски, поскольку уникальные свойства этих данных позволяют установить личность человека и определить его родственные связи. Эти особенности делают геномные данные уязвимыми перед различными угрозами. К ним относятся возможность деанонимизации, даже если используются якобы анонимные наборы данных, и несанкционированный доступ, который может привести к нарушению конфиденциальности и использованию данных в не предназначенных для этого целях. В конце 2023 года произошел взлом компании, занимающейся генетическими тестами, в результате которого были раскрыты данные почти 7 миллионов человек. Этот инцидент уже привлек внимание к возможным рискам, связанным с хранением и использованием генетической информации.

С развитием геномики как ключевой области исследований становится все более важным обеспечить защиту конфиденциальных биологических данных, а также систем и пользователей, которые с ними связаны. Крайне важно гарантировать безопасность биоинформационных платформ и предотвратить их несоответствующее использование в биотехнологических целях. Необходимо предусмотреть защиту аналитических данных и обеспечение безопасности более широкой экосистемы взаимосвязанных систем для снижения рисков в различных секторах. С развитием новых технологий, таких как биоинформатика, аналитика и киберфизические системы, потребность в надежной защите данных будет только увеличиваться. Это ставит перед специалистами по кибербезопасности новые задачи, к которым они должны быть готовы.
Хода Аль-Хазими (Hoda Al Khazimi), директор Центра кибербезопасности Нью-Йоркского университета в Абу-Даби

Инфраструктура систем связи

Геополитическая напряженность, проявляющаяся в растущем числе атак на критически важную телекоммуникационную инфраструктуру, находит свое отражение в различных формах: от крупномасштабного кибершпионажа, спонсируемого государством, до атак на спутники и подводные кабели.

После атаки на систему спутниковой связи ViaSat в 2022 году, которая продемонстрировала серьезные последствия кибердаров по военным и мирным системам связи в Европе, были зафиксированы еще 124 кибератаки, направленные против космического сектора в связи с украинским конфликтом. В эпоху растущей зависимости от космических технологий этот сектор становится главной целью шпионажа, дезорганизации работы и использования в качестве оружия.

Подводные кабели играют ключевую роль в обеспечении глобального потока передачи данных и экономического обмена. Стратегическая значимость этих объектов делает их уязвимыми для отслеживания и возможных повреждений, особенно в условиях ограниченных мер безопасности и роста геополитической напряженности.

С момента начала украинского конфликта в Балтийском море произошло несколько инцидентов, которые наглядно демонстрируют, насколько важно защитить эти стратегически значимые объекты инфраструктуры.

Климат и энергетика

По мере обострения глобального климатического кризиса его влияние на кибербезопасность становится все более значительным. Современные технологии в значительной степени зависят от потребляемой электроэнергии, что делает электросети особенно привлекательными для киберпреступников. В то же время энергетические системы претерпевают глубокие преобразования по мере того, как общество переходит на возобновляемые источники энергии. Крайне важно, чтобы эти новые энергосистемы проектировались с учетом обеспечения безопасности как основополагающего приоритета. В противном случае, при попытке быстрого решения проблемы глобального кризиса, есть вероятность появления уязвимостей, которые могут поставить под угрозу стабильность новой энергетической инфраструктуры. Это, в свою очередь, может иметь серьезные последствия для экономики и общества.

2.2 Безопасность в эпоху ИИ

Последствия, к которым может привести отсутствие или наличие уязвимостей в системах обеспечения безопасности ИИ, могут быть весьма значительными, особенно учитывая растущую популярность этой технологии. Я убежден, что ИИ должен разрабатываться и внедряться безопасным, надежным и заслуживающим доверия образом на благо общества. Для достижения этой цели потребуется всеобъемлющий, многосторонний подход с участием многих заинтересованных сторон. Цифровые технологии, такие как ИИ, не имеют границ и распространяются по всему миру. Необходимо объединить усилия и действовать сообща, чтобы гарантировать защищенность ИИ, несмотря на сохраняющуюся геополитическую напряженность и стратегическое соперничество в сфере ключевых и инновационных технологий.
Дэвид Кох (David Koh), комиссар по кибербезопасности и главный исполнительный директор Сингапурского агентства кибербезопасности (Cyber Security Agency of Singapore, CSA)

«Эпоха ИИ, движимая стремительными достижениями в области искусственного интеллекта, квантовых вычислений и блокчейна, меняет все в режиме реального времени». С наступлением эры ИИ открываются новые горизонты, но вместе с тем возникают и новые риски. Безопасность становится ключевым фактором, способствующим успешному развитию этих революционных технологий.

Парадокс киберрисков, связанных с ИИ

Новые технологии открывают перед организациями огромные перспективы для повышения эффективности и оптимизации бизнес-процессов. В результате многие компании активно разрабатывают стратегии по внедрению этих технологий в свою инфраструктуру. Однако, несмотря на все преимущества, внедрение новых технологий в компании также сопряжено с определенными киберрисками. Эти риски часто остаются незамеченными или недостаточно учитываются, что может привести к серьезным последствиям для бизнеса.

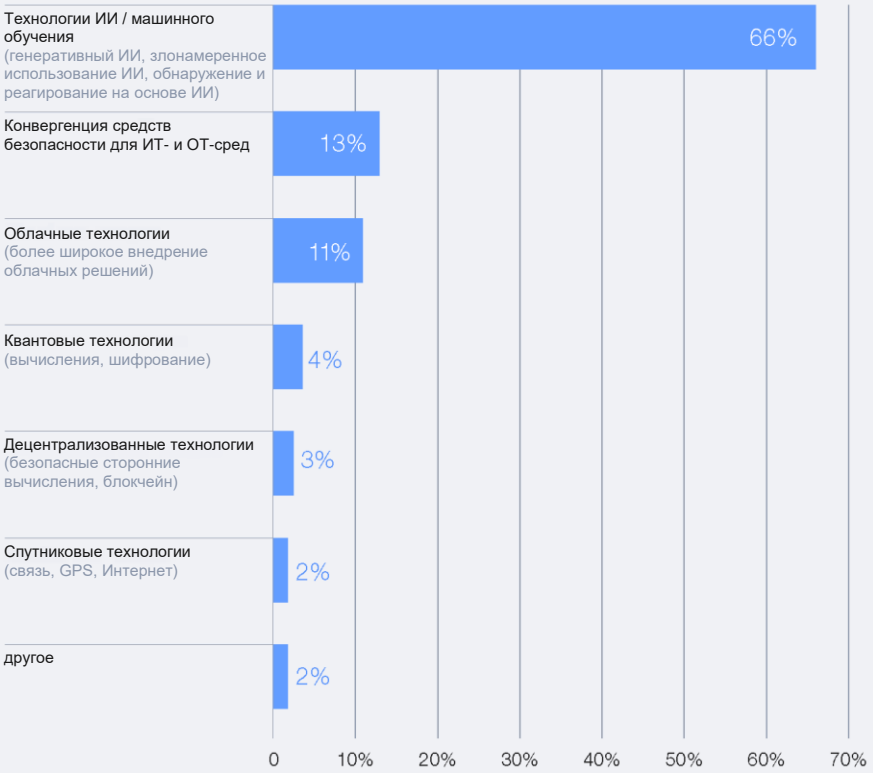
Хотя ИИ не является чем-то новым, появление так называемого «генеративного ИИ» (GenAI) значительно ускорило его внедрение в различных организациях по всему миру. Организации тестируют или внедряют ИИ-технологии для повышения эффективности и получения конкурентных преимуществ. Однако не всегда они уделяют должное внимание разработке стратегий и процессов, необходимых для безопасной реализации этих технологий.

При внедрении ИИ организациям крайне важно оценить киберриски и установить соответствующие меры контроля кибербезопасности. Это поможет обеспечить как операционную, так и более широкую киберустойчивость бизнеса.

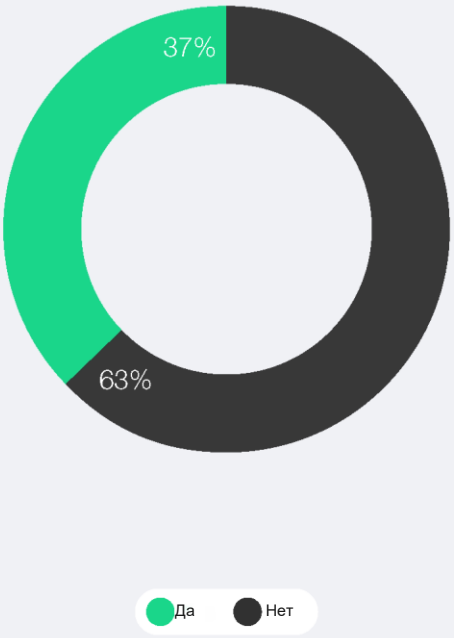
Согласно исследованию, проведенному GCO, 66 % компаний ожидают, что в следующем году ИИ станет одним из самых значительных факторов, влияющих на кибербезопасность. Однако только 37 % опрошенных компаний сообщили о том, что они проводят оценку безопасности инструментов ИИ перед их внедрением. Существует риск того, что компании будут внедрять или использовать системы ИИ (созданные самостоятельно или полученные от внешних поставщиков) без должного анализа возможных рисков для кибербезопасности и без принятия необходимых мер по их минимизации. Это может привести к появлению уязвимостей в их ИТ-инфраструктуре.

РИС. 7 **Уязвимости кибербезопасности, которые, по мнению экспертов, могут возникнуть в 2025 году**

Какие технологии, по вашему мнению, больше всего будут влиять на кибербезопасность в течение следующего года?



Предусмотрены ли в вашей организации процессы для оценки безопасности ИИ-инструментов до их внедрения?



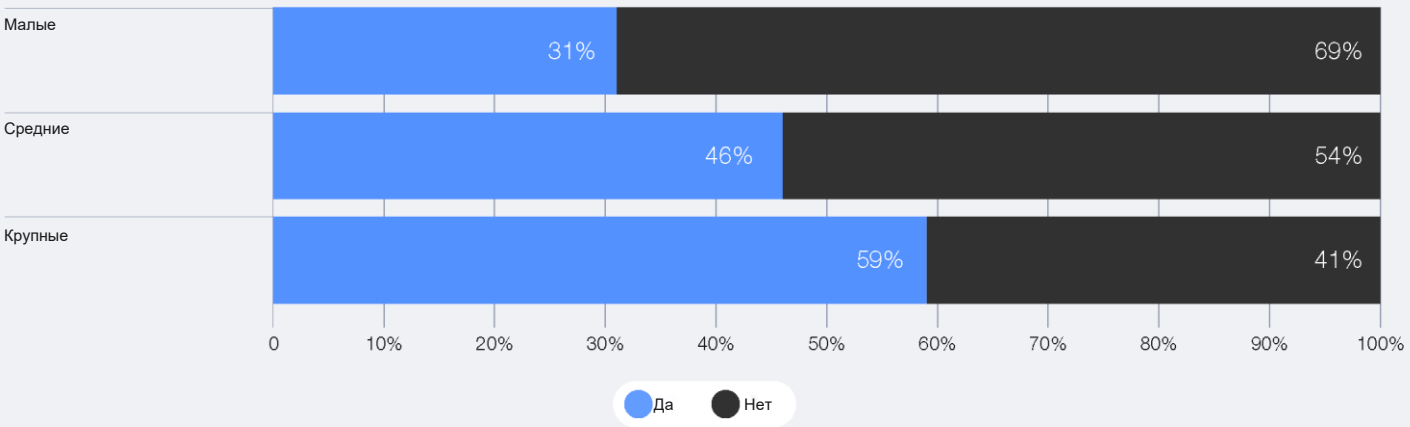
Этот вопрос вызывает особую тревогу у небольших компаний, поскольку 69 % из них не имеют надежных механизмов для обеспечения безопасного использования технологий ИИ. Эти механизмы могут включать в себя проведение инвентаризации всех новых ресурсов (аппаратных средств и программного обеспечения), связанных с инфраструктурой ИИ, обеспечение защиты обучающих данных, отслеживание поведения систем ИИ для оперативного выявления подозрительной активности.

Это помогает преодолеть цифровое неравенство, поскольку организации с ограниченными ресурсами становятся более подверженными рискам, связанным с небезопасными моделями ИИ. Кроме того, это повышает общую уязвимость экосистемы, в которой работают эти организации.

Для обеспечения безопасного внедрения технологий ИИ необходимо применять комплексный подход. Согласно исследованию KPMG, 74 % руководителей компаний по всему миру считают, что формирование эффективной киберкультуры является ключевым условием успешной интеграции ИИ в их организации.

РИС. 8 **Крупные компании чаще применяют процедуры обеспечения безопасности с помощью ИИ**

Предусмотрены ли в вашей организации процессы для оценки безопасности ИИ-инструментов до их внедрения?



Современные большие языковые модели (Large Language Models, LLM) недостаточно защищены, а возможные угрозы в виде враждебных атак и саботажа в цепочке поставок не всегда эффективно нейтрализуются. Поэтому внедрение этих моделей в критически важную инфраструктуру до устранения векторов таких атак может оказаться опасным и требует тщательного переосмысления.
Мередит Уиттакер (Meredith Whittaker), президент Signal

В июне 2023 года Всемирный экономический форум основал Альянс по управлению искусственным интеллектом. Цель этого альянса — сформулировать и реализовать практические рекомендации по ответственному проектированию, разработке и внедрению систем ИИ. В своем отчете *«Искусственный интеллект и кибербезопасность: баланс рисков и преимуществ»* руководство задает несколько вопросов, которые помогут определить и рассмотреть ключевые параметры для принятия решения о внедрении ИИ и соответствующих мер по обеспечению кибербезопасности.

1. Существует ли определенная граница допустимого риска для технологий ИИ, и все ли ответственные за риски понимают это?
2. Следует ли учитывать все возможные риски и преимущества при оценке новых проектов в области ИИ?
3. Существует ли в организации эффективный процесс управления и контроля за внедрением проектов, связанных с ИИ?
4. Есть ли у организации четкое представление о рисках и уязвимостях, связанных с использованием или внедрением технологий ИИ?
5. Существует ли ясное представление о том, какие внутренние заинтересованные стороны должны быть вовлечены в процесс оценки и снижения киберрисков, связанных с использованием ИИ?
6. Существуют ли процессы, которые гарантируют, что внедрение ИИ не будет противоречить общей политике организации и ее юридическим и нормативным обязательствам? Например, это касается вопросов защиты данных, охраны труда и техники безопасности.

ИИ для киберзащиты

ИИ способен существенно повысить эффективность методов защиты от киберугроз. Это дает специалистам по кибербезопасности значительное преимущество, позволяя использовать современные инструменты для быстрого выявления и реагирования на угрозы. Однако для этого им необходимо постоянно следить за стремительным развитием ИИ. Проще говоря, ИИ может значительно расширить возможности человека, что сделает защиту от киберугроз более надежной и эффективной.

ИИ меняет мир кибербезопасности, экономя ресурсы и высвобождая человеческие силы. Благодаря ему системы могут обрабатывать огромные объемы данных, что позволяет выявлять угрозы на ранних стадиях и обнаруживать скрытые риски. ИИ способен улучшить процессы сортировки и расстановки приоритетов в предупреждениях об угрозах, обнаружения аномалий и распознавания шаблонов. С его помощью также можно классифицировать уязвимости, автоматизировать их исправление, ускорять обработку данных и управлять конфигурациями. Кроме того, ИИ может выступать в роли консультанта по безопасности типа «ИИ-руководителя службы информационной безопасности» или «Виртуального руководителя службы информационной безопасности». Его задача — повысить безопасность программного обеспечения и оптимизировать процесс принятия решений, чтобы максимально использовать ограниченные ресурсы. В свете последних разработок в области ИИ, вероятно, в ближайшем будущем появятся инструменты, которые помогут специалистам по кибербезопасности оптимизировать ресурсы и использовать автономных помощников для достижения этой цели.

Большие языковые модели (LLM) помогают собирать больше данных для анализа, что позволяет запустить цикл «угроза-интеллектуальная система». Модели ИИ могут анализировать и классифицировать типы вопросов, задаваемых злоумышленниками, модели их взаимодействия и даже лингвистические маркеры, способные определять конкретные группы или отдельных лиц.

После этого данные можно отправить обратно в системы анализа рисков. Это позволит улучшить механизмы обнаружения и предоставит специалистам по кибербезопасности более точные данные за счет оптимизации процессов анализа информации и ее сортировки. Благодаря использованию ИИ и машинного обучения, специалисты по кибербезопасности могут проводить непрерывный мониторинг и анализ в режиме реального времени. Это позволяет оперативно выявлять и устранять уязвимости в программном обеспечении, включая угрозы и эксплойты нулевого дня. Современные системы обнаружения угроз, основанные на поведенческом анализе, сетевой сегментации и машинном обучении, способны предотвращать потенциальные взломы и ограничивать активность злоумышленников в уже инфицированных средах.

Использование LLM в системах-ловушках для злоумышленников открывает новые перспективы в области кибербезопасности, основанной на принципах дезинформации. Применение LLM в таких системах-ловушках позволяет специалистам по кибербезопасности создавать сложные и гибкие сценарии, которые могут адаптироваться к поведению злоумышленников в режиме реального времени. Эта инновация основана на способности больших языковых моделей имитировать поведение человека, что делает ловушки более реалистичными и привлекательными для злоумышленников.

В отличие от статичных систем или заранее подготовленных ответов, LLM способны создавать нюансированные диалоги, соответствующие контексту. Эти диалоги эффективно реагируют на запросы злоумышленников, удерживая их внимание и создавая иллюзию, будто они общаются с легитимными системами. При этом создаются условия, в которых злоумышленники, сами того не замечая, раскрывают свои намерения, методы и даже детали операций, думая, что достигают целей своих атак.

Одним из ключевых проектов, реализованных в 2020 году при поддержке Европейского союза (ЕС), стал проект «Сфинкс». Это инициатива, направленная на научные исследования и разработку инновационных решений в области кибербезопасности. Ее задача — привлекать злоумышленников, изучать их методы и разрабатывать эффективные меры противодействия. Системы-ловушки для злоумышленников на основе ИИ используют продвинутые алгоритмы обработки данных об атаках для обнаружения ИИ и управления им.

LLM способны создавать реалистичные ресурсы, которые могут привлечь внимание злоумышленников. Эти ресурсы могут представлять собой поддельные учетные данные, правдоподобные конфигурации систем или сгенерированные материалы, содержащие конфиденциальную информацию, которая может вызвать интерес у хакеров. Эти ресурсы, созданные на базе LLM, помогают создавать иллюзию подлинности. При этом увеличивается вероятность того, что злоумышленники задержатся в ловушке, и у специалистов по кибербезопасности будет больше времени для реагирования.

Подготовка к квантовой угрозе

40 %

организаций активно занимаются изучением квантовых угроз, чтобы заранее подготовиться к ним.

Квантовые вычисления открывают огромные перспективы в экономике и науке, позволяя достичь невиданной ранее вычислительной мощности. Однако достижения в области квантовых вычислений также ускоряют появление новых угроз безопасности. В частности, существует риск взлома шифрования с открытым ключом, что имеет жизненно важное значение для защиты цифровых систем, таких как онлайн-банкинг и системы правительственной связи. В то время как сроки реализации всего потенциала квантовых вычислений остаются неопределенными, связанные с ними риски квантовых угроз уже существуют.

В специальной рабочей группе, организованной на Ежегодной конференции по кибербезопасности в 2024 году, 40 % организаций сообщили, что начали принимать превентивные меры, включая оценку рисков, чтобы лучше понять потенциальные угрозы, связанные с квантовыми вычислениями. Многие организации уделяют все больше внимания угрозе «Собери данные сейчас, расшифруй позже». Эта угроза предполагает сбор зашифрованных данных в настоящее время с целью их расшифровки в будущем, когда квантовые вычисления станут способны преодолевать существующие методы шифрования. Это создает серьезные вызовы как для текущей, так и для будущей защиты данных. Тем не менее, некоторые организации все еще рассчитывают на поддержку в виде отраслевых стандартов, методических указаний и правительственных постановлений.

Было предпринято множество усилий, чтобы подстегнуть принятие необходимых мер. Группа экспертов G7 по кибербезопасности определила основные риски для безопасности финансовой системы. В своем отчете они дали рекомендации правительствам и центральным банкам, а также призвали их к действиям. Всемирный экономический форум совместно с Управлением по финансовому поведению также подготовил рекомендации для формирования глобальных нормативных процедур. Эти рекомендации направлены на выработку согласованного подхода к обеспечению безопасности квантовых вычислений на международном уровне.

Недавно Национальный институт стандартов и криптографии (National Institute of Standards and Cryptography, NIST) представил три долгожданных стандарта алгоритмов постквантовой криптографии (Post-Quantum Cryptography, PQC). Эти алгоритмы были разработаны для защиты от кибератак, исходящих от квантовых компьютеров. Помимо стандартов PQC, существуют и другие технологии, которые привлекают внимание специалистов. Среди них — квантовое распределение ключей (Quantum Key Distribution, QKD) и квантовая генерация случайных чисел (Quantum Random Number Generation, QRNG). Эти технологии, как по отдельности, так и в сочетании, помогут снизить риски, связанные с квантовой криптографией с открытым ключом.

Переход к квантовому миру начинается с создания прочного фундамента в сфере кибербезопасности и разработки четкого плана подготовки к внедрению квантовых технологий. Такой подход подчеркивает необходимость активного движения организаций в направлении квантовой трансформации уже сейчас.

2.3 Растущая взаимозависимость экосистем и связанные риски

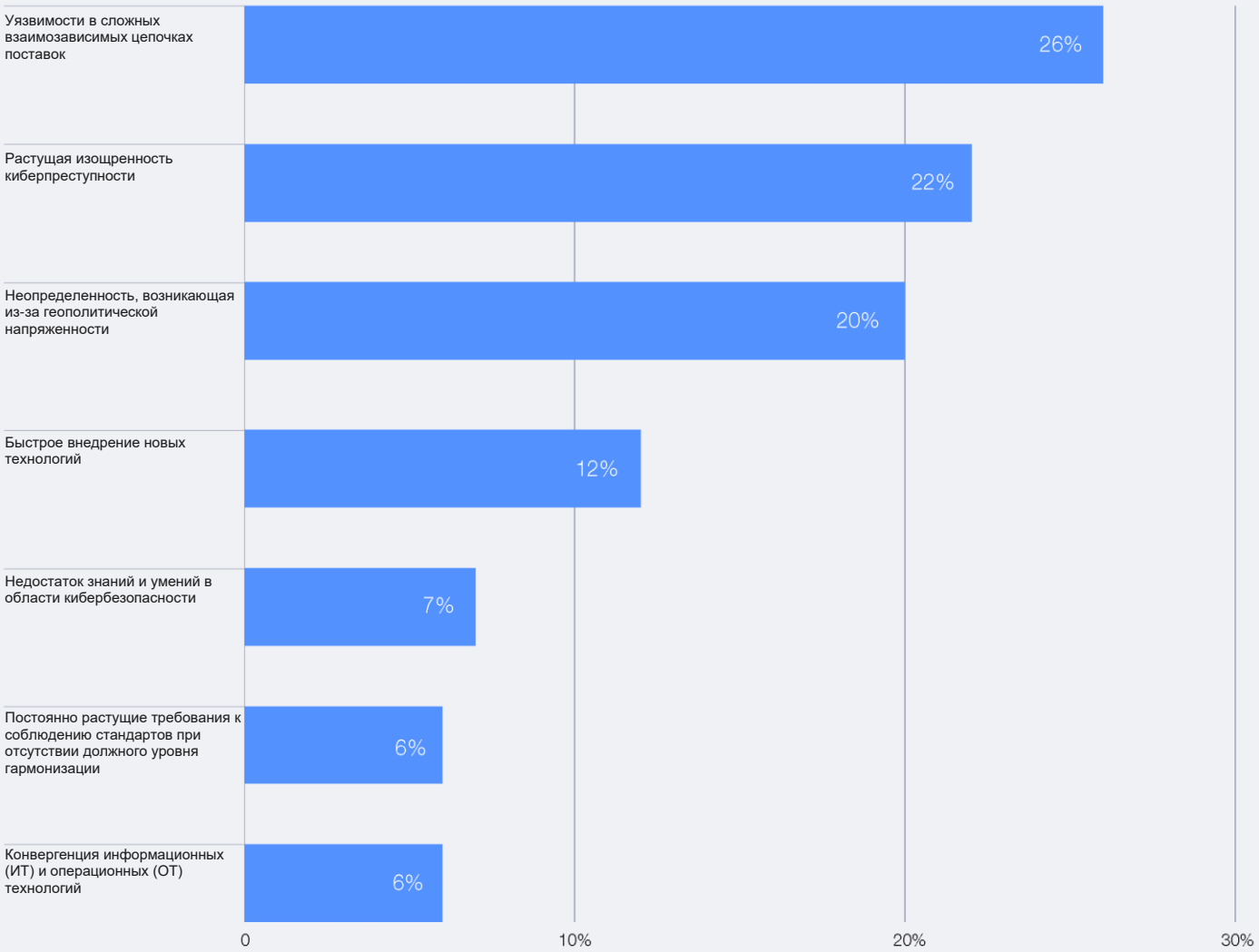
С момента первого выпуска Обзора мировых тенденций в сфере кибербезопасности в 2022 году была выявлена растущая обеспокоенность бизнеса и специалистов по кибербезопасности относительно состояния киберэкосистемы. На Ежегодной конференции по кибербезопасности в 2024 году эксперты в области кибербезопасности отметили, что главной причиной растущей сложности в киберпространстве являются уязвимости во взаимосвязанных цепочках поставок.

В Обзоре на текущий год будет рассмотрено, как сложные взаимосвязи в цепочках поставок, геополитические риски, а также экономическое и социальное неравенство влияют на киберустойчивость экосистем.

> **С развитием цифровых технологий киберугрозы становятся все более сложными, особенно в условиях растущей взаимозависимости различных логистических цепочек и более масштабных экосистем. Чтобы причинить значительный вред, киберпреступникам достаточно провести одну успешную атаку. В то же время наша система коллективной защиты, включающая организации, поставщиков и глобальные сети, должна быть надежной и целостной. Для обеспечения безопасности энергетической инфраструктуры, которая снабжает энергией миллиарды людей по всему миру, требуются модели более тесного взаимодействия и открытость между всеми участниками процесса — как на местном, так и на международном уровнях. Это поможет снизить риски в цепочке поставок и цифровой экосистеме.**
> Амин Насер (Amin Nasser), президент и главный исполнительный директор Aramco

РИС. 9 **Проблемы, с которыми сталкиваются компании из-за киберугроз**

Какой аспект сложности представляет наибольшие проблемы для вашей организации?



Сложность взаимозависимостей в цепочке поставок

Усложнение цепочек поставок и снижение контроля со стороны организаций становится главным вызовом для руководителей. С точки зрения экосистемы это определяет основной киберриск.

В этом году 54 % крупных организаций считают, что главной проблемой на пути к киберустойчивости являются проблемы в цепочке поставок. Для сравнения управление рисками, связанными с третьими сторонами, не входит в пятерку основных проблем для небольших организаций.

ТАБЛИЦА 1 **Основные организационные проблемы, препятствующие киберустойчивости**

Небольшие организации	Средние организации	Крупные организации
01 **Сложный и меняющийся ландшафт угроз**	01 **Сложный и меняющийся ландшафт угроз**	01 Управление рисками, связанными с третьими сторонами
02 Нехватка квалифицированных специалистов	02 Управление рисками, связанными с третьими сторонами	02 **Сложный и меняющийся ландшафт угроз**
03 Недостаточная готовность к реагированию на возможные инциденты	03 Сложность сред (например, ИТ, ОТ, Интернет вещей)	03 Сложность сред (например, ИТ, ОТ, Интернет вещей)

Результаты опроса GCO показывают, что большинство людей опасаются уязвимостей в программном обеспечении, поставляемом сторонними организациями или вендорами. Также люди боятся кибератак, которые распространяют вредоносное ПО, чтобы использовать уязвимости в цепочке поставок.

Вслед за Указом Президента США №14028 «О повышении национальной кибербезопасности» (US Executive Order 14028: Improving the Nation’s Cybersecurity), в котором особое внимание уделяется Спецификации программного обеспечения (Software Bill of Materials, SBOM), требования, связанные с этой спецификацией, вводят другие стандарты и нормативные акты: Стандарт безопасности данных индустрии платежных карт (Payment Card Industry Data Security Standard, PCI DSS) и Закон ЕС о киберустойчивости. Выполнение этих требований поможет организациям лучше понять, какие ресурсы они используют, как их контролировать и как обеспечить их безопасность.

60 %

организаций указали, что на их стратегию обеспечения кибербезопасности повлияла геополитическая напряженность.

Еще одна важная проблема — неопределенность в цепочках поставок из-за различных зависимостей. Отсутствие прозрачности в масштабах всей экосистемы и неудовлетворительный контроль уровня защищенности поставщиков вызывают серьезную озабоченность организаций. В рамках фокус-группы на Ежегодной конференции по кибербезопасности 2024 года 41 % участников выразили мнение, что для усиления киберустойчивости цепочки поставок необходимо в первую очередь повышать прозрачность зависимостей от третьих сторон. Все труднее стало добиваться соблюдения стандартов безопасности от непосредственных поставщиков, не говоря уже о прочих поставщиках, от услуг которых организации зависят. GCO это подтверждает: 48 % опрошенных руководителей служб ИБ указали, что обеспечить соблюдение требований безопасности третьими сторонами — самая сложная задача при внедрении стандартов кибербезопасности. Ситуация часто усугубляется тем, что в разных отраслях нормативы безопасности могут различаться — это затрудняет внедрение более жестких требований по всей цепочке поставок.

Кроме того, организации все больше зависят от ограниченного числа критически важных поставщиков, зарекомендовавших себя как лидеры в своей области. Риск заключается в том, что эти поставщики становятся единой точкой отказа. Если по их вине в системе возникнет уязвимость, это может привести не только к сбоям в работе их обширной клиентской базы, но и к негативным последствиям для всей экосистемы. Кибератака или сбой в работе могут иметь далеко идущие и непредсказуемые последствия для сложной экосистемы. Это стало очевидным в 2024 году: проблемное обновление облачной системы безопасности CrowdStrike Falcon привело к глобальному сбою в работе ИТ, погрузившему в хаос предприятия и государственные учреждения по всему миру.

> **Укрепление устойчивости к угрозам имеет критически важное значение в современном взаимосвязанном ландшафте, где сложные цепочки поставок могут стать причиной бесчисленных проблем с кибербезопасностью. Необходимо налаживать сотрудничество, поскольку злоумышленники эксплуатируют уязвимости стороннего ПО. Только внедряя стандарты, опираясь на аналитические данные об угрозах и оснащая организации любого масштаба более эффективной защитой от киберугроз, можно устранить бреши и укрепить экосистему, чтобы не допускать нарушений, а также обеспечивать непрерывность бизнеса и гарантировать цифровое доверие.**
> Джордж Курц (George Kurtz), основатель и генеральный директор CrowdStrike

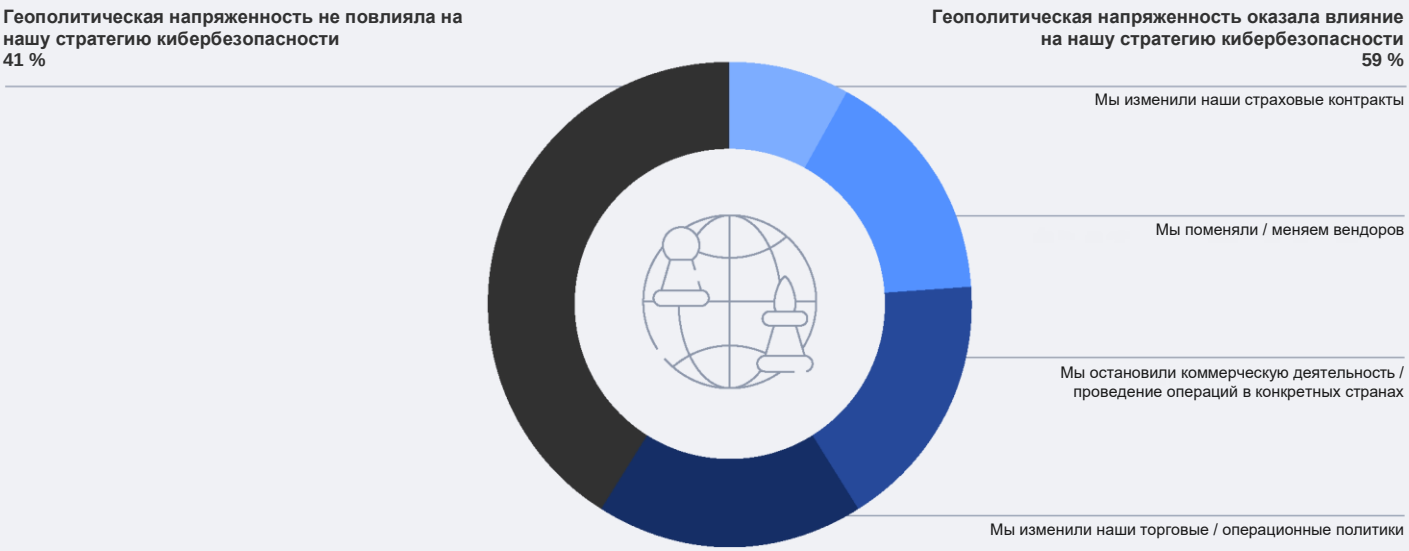
Поставщики облачных решений также играют решающую роль в повышении безопасности современных экосистем, предлагая защиту более высокого уровня, которого многие организации не могут достичь самостоятельно. С другой стороны, отдельные организации имеют ограниченный контроль над киберрисками, связанными с облачными сервисами, и должны управлять ими в рамках своей, более широкой стратегии. Из-за эффективности затрат многие организации предпочитают использовать облачные технологии, что требует ясного понимания модели общей ответственности, где роли и обязанности могут порой перекрывать друг друга. Организации переводят все больше рабочих нагрузок на платформы, предоставляющие программное обеспечение как услугу (SaaS), где клиент не может управлять конфигурациями. Это приводит к значительной концентрации рисков. Атака вирусов-вымогателей на крупного облачного провайдера может привести к проблемам для тысяч компаний, которые зависят от его услуг, и вызвать внезапные нарушения в их работе. Хотя компании такого уровня уделяют много внимания вопросам кибербезопасности, идеальных систем не существует. Компаниям следует вкладывать средства в собственные стратегии, направленные на повышение устойчивости бизнеса. Также важно иметь план действий на случай непредвиденных обстоятельств, чтобы не зависеть полностью от своих SaaS-партнеров.

Некоторые организации пытались решить эти проблемы доступными средствами, в частности, пересматривали степень подверженности рискам во всей сквозной цепочке поставок и внедряли методы безопасной разработки приложений, включая надежную оценку рисков и управление зависимостями. Другие указывали на важность стандартизации и сертификации для повышения доверия к сервисам, предоставляемым в цифровой экосистеме, признавая при этом, что штрафы, вероятнее всего, могут стать серьезным стимулом для достижения комплаенса. В целом, это отражает мнение, что с одной стороны ответственность за разработку безопасного ПО должна быть четко определена и прозрачна, чтобы привлекать разработчиков к ответственности за качество их работы, а с другой — руководители служб ИБ должны непрерывно обеспечивать достаточную устойчивость сред своих организаций. Эти усилия поддерживает Закон о киберустойчивости (Cyber Resilience Act, CRA), вступивший в силу во второй половине 2024 года и направленный на повышение кибербезопасности цифровых продуктов на всей территории ЕС.

Влияние геополитического риска на сложность экосистемы

Почти 60 % респондентов опроса GCO сообщили, что на их киберстратегии повлияла геополитическая напряженность. Более того, конфликты, продолжающиеся в 2024 году, по-прежнему влияли на регионы, не имеющие непосредственного отношения к ним: 18 % организаций скорректировали торговую или операционную политику, 17 % — полностью или частично прекратили деятельность в определенных регионах, а у 16 % изменился состав вендоров.

РИС. 10 | **Влияние геополитической напряженности на стратегию кибербезопасности**



Большую озабоченность вызывает распространение киберугроз со стороны государств: представители государств все чаще используют инструменты и наработки киберпреступности и наоборот. В ходе интервью, проведенных для этого отчета, руководители в области кибербезопасности сошлись во мнении, что геополитическая напряженность меняет картину в сфере кибербезопасности. Один из руководителей службы ИБ подчеркнул, что целью спонсируемых государством злоумышленников все чаще становятся не только атаки на правительства, но и разрушение экономики, подрыв критически важной инфраструктуры и создание хаоса в глобальных системах. Сейчас организации могут не только пострадать от прямых атак, но и получить дополнительный ущерб, если злоумышленники эксплуатируют уязвимости в цепочке поставок или общих сервисах.

В таких условиях для эффективного долгосрочного управления рисками решающее значение приобретает понимание геополитической динамики.

Руководители служб информационной безопасности осознают, что ситуация нестабильна, и признают, что не существует стандартных методов борьбы с геополитическими рисками. Похоже, что ситуация требует вернуться к традиционным подходам к управлению рисками. На первом этапе необходимо оценить проблемы с точки зрения их влияния на бизнес. Затем следует осуществлять управление рисками и, наконец, брать на себя любые оставшиеся риски. Поэтому для решения сложных задач, связанных с геополитическими рисками, необходима предельная согласованность функций по обеспечению безопасности и потребностей бизнеса.

ТИПИЧНЫЙ ПРИМЕР 2
Кибербезопасность Олимпийских игр в Париже

Обеспечение кибербезопасности Олимпийских игр в Париже было одним из главных приоритетов для французского правительства. В течение двух лет проводились тщательные аудиты, тестирования на проникновение и учения по управлению кризисными ситуациями, чтобы гарантировать защиту от кибератак. В результате, несмотря на значительное количество кибератак (больше, чем на любой из предыдущих Олимпийских игр), лишь немногие из них достигли успеха, и ни одна не смогла нарушить ход Игр или работу ключевых объектов инфраструктуры.
Однако несмотря на успешность применения данной модели киберзащиты, можно сделать два беспристрастных вывода. Во-первых, модель изначально была сфокусирована на защите конкретных важных объектов, ее нельзя распространить на все общество. Во-вторых, продолжается рост геополитической напряженности и количества кибератак, которые становятся все более сложными. Необходимо и далее настаивать на усилении мер по предотвращению киберугроз и стремиться к обеспечению коллективной киберустойчивости. Хотя нормативные акты и участие государства играют ключевую роль в обеспечении кибербезопасности, каждый должен внести свой вклад в этот процесс. Необходимо коллективно определить новые способы повышения информированности и вовлеченности всего общества.

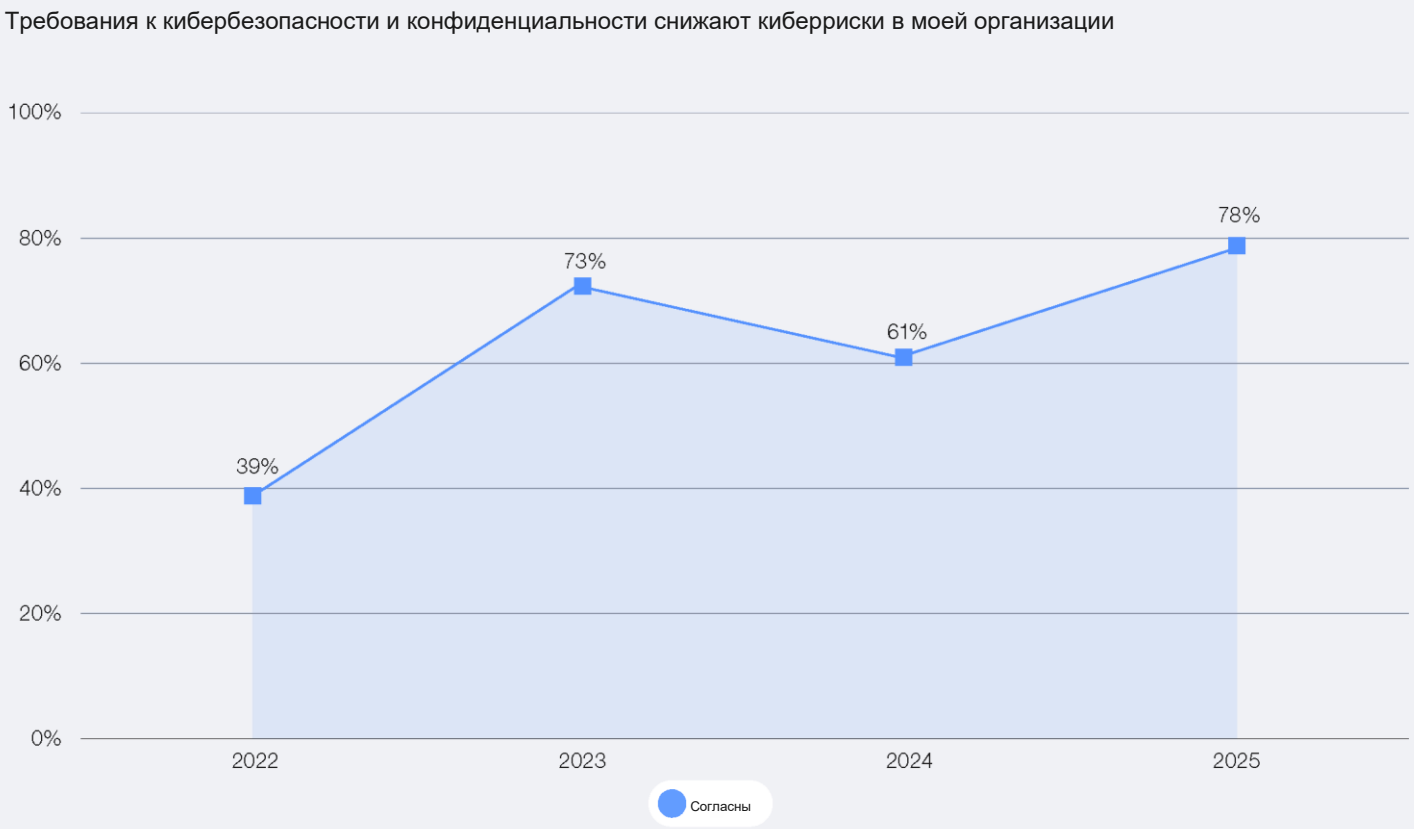
Винсент Штрубель (Vincent Strubel)
Генеральный директор Национального агентства кибербезопасности Франции

Повышение устойчивости экосистем к угрозам путем регулирования

Регулирование — важный фактор обеспечения киберустойчивости: 78 % опрошенных руководителей служб ИБ и 87 % генеральных директоров считают, что внедрение новых регуляторных требований к обеспечению кибербезопасности позволит повысить ее уровень и снизить киберриски в организациях. Руководители служб ИБ, постоянно имеющие дело с рисками экосистемы, подтверждают обоснованность нормативных актов, которые, устанавливая минимальные требования к кибербезопасности, помогают снизить риски и повысить доверие клиентов.

В то же время две трети участников опроса GCO указали, что их работу значительно усложняет различие региональных и глобальных требований к кибербезопасности в разных странах.

РИС. 11 **Влияние регулирования на снижение уровня киберрисков в организациях**



Директива NIS2 значительно повышает планку стандартов кибербезопасности на всей территории ЕС, требуя улучшения отчетности об инцидентах, усиления безопасности цепочек поставок и повышения ответственности советов директоров. По ту сторону Атлантики, в США, приняли Закон об отчетности о киберинцидентах в критической инфраструктуре (Cyber Incident Reporting for Critical Infrastructure Act, CIRCIA), который обязывает сообщать о киберинцидентах в Агентство по кибербезопасности и защите инфраструктуры (Cybersecurity and Infrastructure Security Agency, CISA). В Азиатско-Тихоокеанском регионе Япония и Сингапур ужесточают свои законы в области кибербезопасности: Закон Японии о защите персональной информации (Act on the Protection of Personal Information, APPI) и Закон Сингапура о кибербезопасности усиливают требования к операторам критической инфраструктуры. Кроме того, возможности контроля со стороны регуляторов по всем секторам и границам расширяют такие инициативы, как Закон о цифровой операционной устойчивости (Digital Operational Resilience Act, DORA), Общий регламент ЕС по защите данных (General Data Protection Regulation, GDPR), Нигерийский регламент по защите данных (Nigeria's Data Protection Regulation, NDPR) и Общий закон Бразилии о защите данных (Brazil's General Data Protection Law, LGPD).

Эта правовая база предписывает важные меры обеспечения кибербезопасности, но одновременно и создает проблемы, такие как управление перекрывающимися требованиями, достижение комплаенса в различных юрисдикциях и соблюдение различных сроков правоприменения. Точки соприкосновения между регулируемым и нерегулируемым секторами еще больше расшатывают киберустойчивость, поскольку отрасли со слабым надзором становятся лазейкой для атак на более укрепленные предприятия. Чтобы преуспевать в среде, которая регулируется все строже, организации должны внедрять целостные подходы к управлению рисками, согласовывать кибербезопасность со структурами управления и поощрять трансграничное сотрудничество.

69 %

респондентов считают нормативные акты слишком сложными или слишком многочисленными, или им трудно проверить, соблюдают ли требования сторонние поставщики.

Опрос GCO показал, что организации сталкиваются с трудностями при внедрении существующих правил кибербезопасности: более 69 % респондентов считают нормативные акты слишком сложными или слишком многочисленными, или им трудно проверить, соблюдают ли требования сторонние поставщики. По мере усиления регуляторного давления возникают опасения, что огромное число модифицированных и вновь вводимых требований приведет к усталости компаний от регулирования и не позволит достичь желаемой эффективности. Хотя нормативно-правовые акты устанавливают базовые стандарты и подчеркивают важность кибербезопасности, существует риск, что запутанное регулирование может помешать разработке индивидуальных стратегий, основанных на оценке вероятности нежелательных последствий. Чтобы достичь устойчивости, необходимо не только следовать установленным правилам, но и иметь возможность действовать вне их рамок. Чтобы глобально скоординировать нормативно-правовую базу и обеспечить применимость стандартов кибербезопасности в различных регионах, необходимо тесное сотрудничество государств и бизнеса. Это стимулировало бы согласованность и в то же время позволяло бы гибко адаптироваться к новым технологиям и возникающим угрозам.

> **Сегодня Европа, как и весь мир, сталкивается со все более сложным ландшафтом угроз и растущей геополитической нестабильностью. Солидарность партнеров-единомышленников в области кибербезопасности важна как никогда. Законодательство ЕС в области кибербезопасности, предоставляющее надежную правовую базу, основанную на доверии и сотрудничестве, направлено на международное сближение — это во многом совпадает с целью Ежегодной конференции по кибербезопасности в рамках Всемирного экономического форума.**
> Деспина Спану (Despina Spanou), координатор Еврокомиссии по кибербезопасности

Неравенство повышает риски экосистемы

По сравнению с отчетом 2024 г. в глобальной экономике кибербезопасности усугубилось неравенство. В Обзоре мировых тенденций в сфере кибербезопасности на 2025 год отмечается, что небольшие организации остаются в неравном положении: 35 % из них имеют недостаточную киберустойчивость.

РИС. 12 **Небольшим компаниям трудно обеспечить надежную защиту от киберугроз. В то же время крупные организации постоянно совершенствуют свои системы безопасности.**

В то же время число крупных организаций с недостаточной киберустойчивостью сократилось почти вдвое. Однако во все более взаимосвязанной экосистеме общая устойчивость часто определяется ее самыми слабыми звеньями.

Чтобы повысить устойчивость всей экосистемы, крупным, более устойчивым компаниям следует оказывать поддержку малым организациям с ограниченными возможностями. По мнению 71 % руководителей на Ежегодной конференции по кибербезопасности в 2024 году, малые организации уже достигли критической точки и больше не могут эффективно защищать себя от все усложняющихся киберугроз. Это подчеркивает настоятельную необходимость коллективных действий и отношения к обеспечению кибербезопасности как к стратегическому императиву для руководства. Вовлеченность руководства и контроль могут сыграть ключевую роль в повышении общей устойчивости. Опрос показал, что в 62 % организаций с высокой устойчивостью члены правления регулярно получали актуальную информацию о недавних киберинцидентах, тенденциях, уязвимостях и прогнозах рисков из внутренних или внешних источников; и всего лишь в 29 % организаций с низкой устойчивостью руководство также имело полную информацию.

ТИПИЧНЫЙ ПРИМЕР 3
Поддержка малых организаций в Швейцарии с помощью государственной национальной инфраструктуры

Три четверти швейцарских компаний зарабатывают менее полумиллиона швейцарских франков в год. Мы задались вопросом, как мы могли бы дать этим компаниям реальную возможность инвестировать в безопасность и обеспечить им достаточно защищенную базовую инфраструктуру? У нас много малых и средних организаций, которым не хватает ресурсов. Мы реализовали пилотный проект, призванный помочь швейцарской логистической компании управлять рисками цепочки поставок. В сотрудничестве с независимым Национальным институтом тестирования кибербезопасности (National Test Institute for Cybersecurity, NTC) мы исследуем цифровые продукты, которые не приносят немедленной экономической выгоды, но являются интересными для общества. В настоящее время мы запускаем проект, в рамках которого проверяем программное обеспечение с открытым кодом, используемое государственными учреждениями, и предоставляем разработчикам этого кода информацию об обнаруженных проблемах. Мы также инвестируем в наращивание потенциала, чтобы помочь членам советов директоров задавать правильные вопросы. Уже сейчас необходимо воспитывать руководителей, способных заботиться об устойчивости и учитывать фактор цепочки поставок при расчете общих рисков.

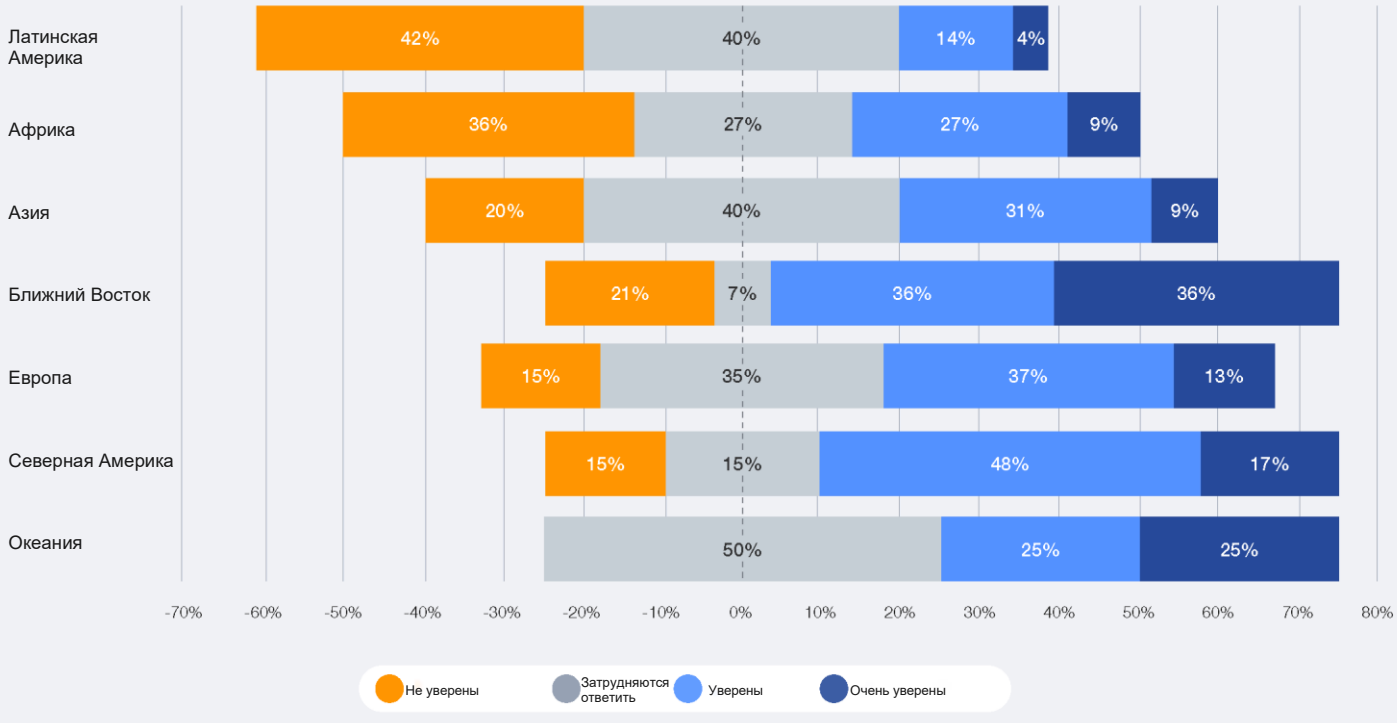
Флориан Шутц (Florian Schutz)
Директор национального центра кибербезопасности (National Centre for Cybersecurity, NCSC), Швейцария

Неравенство в сфере кибербезопасности не исчерпывается растущим разрывом между крупными и малыми организациями; необходим более целостный подход к проблеме. Существует неравенство между теми, у кого есть ресурсы для обеспечения безопасности своей цифровой среды, и теми, у кого их нет. К таким ресурсам относится доступ к инфраструктуре, финансовым ресурсам, к государственным структурам и квалифицированным сотрудникам, необходимым для создания надежной системы кибербезопасности. В свете этого важно учитывать не только различия между крупными и малыми организациями, но и два других момента.

1 **Развитые и формирующиеся экономики:** в *Обзоре мировых тенденций в сфере кибербезопасности на 2024 год* Всемирного экономического форума показано, что неравенство в обеспечении кибербезопасности, как правило, соответствует другим показателям мирового развития: меньше всего организаций, заявивших о своей киберустойчивости, находится на глобальном Юге, больше всего — на глобальном Севере. Это несоответствие подчеркивают и последние данные. В то время как в Европе и Северной Америке лишь 15 % организаций не уверены в готовности своих стран реагировать на крупные киберинциденты, нацеленные на критическую инфраструктуру, в Африке и Латинской Америке этот показатель достигает 36 % и 42 %, соответственно. В менее подготовленных регионах успешная атака на критическую инфраструктуру, такую как энергосеть или морской порт, может повлечь за собой масштабные сбои, что означает серьезные последствия для экономической стабильности и национальной устойчивости.

РИС. 13 **Неравенство между регионами**

Насколько вы уверены в том, что государство, в котором находится ваша организация, подготовлено к кибератакам на критическую инфраструктуру?

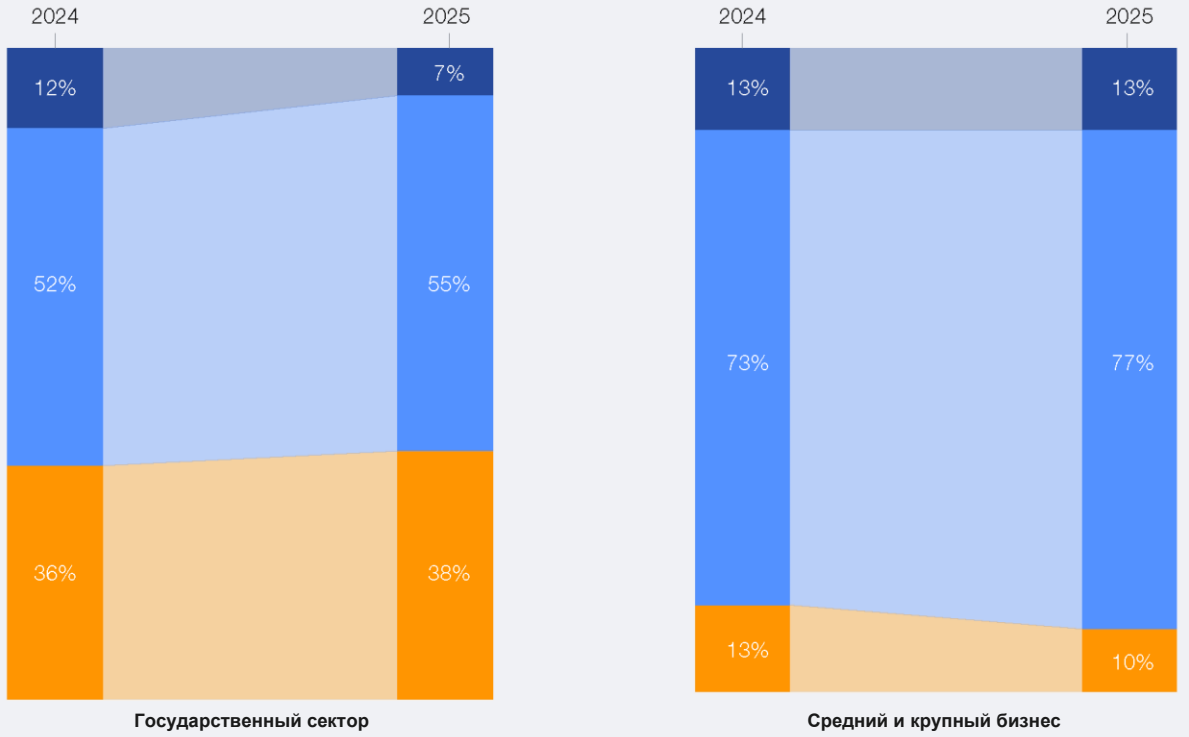


2 **Отраслевые различия:** при наблюдении за обеспечением безопасности бизнеса по секторам наиболее продвинутым является финансовый сектор. Это в значительной степени связано со средой, в которой этот сектор функционирует. Например, в США и Европе сочетание правил, специфичных для конкретной отрасли и для географического расположения, стимулирует развитие кибербезопасности посредством обязательств по соблюдению требований.

А такие секторы, как производство, напротив, все еще находятся на ранних стадиях построения культуры киберустойчивости. Ограничения в отношении ресурсов и инфраструктуры еще сильнее усугубляют эти различия, особенно в государственном секторе. В рамках опроса 38 % респондентов из государственного сектора считают свою устойчивость недостаточной — по сравнению с лишь 10 % средних и крупных организаций в частном секторе.

РИС. 14 **Уверенность государственного сектора, а также среднего и крупного бизнеса в отношении киберустойчивости.**

Как вы оцениваете способность вашей организации самостоятельно противостоять киберугрозам?



Эти аспекты разрыва в киберустойчивости также могут усилить проблемы, связанные с рабочей силой. Сегодняшний мировой спрос на специалистов по кибербезопасности превышает предложение. Хотя крупные организации — особенно те, которые находятся на развитых рынках, — вполне способны получить этот редкий ресурс, неравенство в трудовых ресурсах выходит за рамки организационных и географических различий.

Определенные секторы, такие как образование, государственная административная служба и здравоохранение, а также малый и средний бизнес (МСБ), несоразмерно страдают от нехватки специалистов по кибербезопасности.

> **Под руководством национальных институтов и центров передового опыта Бразилия делает значительные успехи в области кибербезопасности. Для устранения разрыва в уровне кибербезопасности, повышения устойчивости и обеспечения защиты национальной инфраструктуры недавно созданный Национальный комитет по кибербезопасности (National Cybersecurity Committee, CNCiber) разрабатывает новую Национальную стратегию кибербезопасности (E-Ciber) и предлагает создать соответствующую национальную управляющую службу. В E-Ciber первостепенное внимание будет уделяться обеспечению устойчивости ключевых служб и услуг, развитию межсекторального сотрудничества и инвестированию в образование по кибербезопасности. Управляющая служба будет отвечать за координацию и регулирование, а также проводить мониторинг национальных усилий по кибербезопасности в целях ее совершенствования.**
> Андре Луис Бандейра Молина (Andre Luiz Bandiera Molina), секретарь по информации и кибербезопасности Бразилии

ТИПИЧНЫЙ ПРИМЕР 4

Как компания KPMG помогла Министерству иностранных дел и международного развития (Foreign, Commonwealth and Development Office, FCDO) создать более безопасный и доступный цифровой мир.

В период с 2020 по 2024 годы компания KPMG поддерживала крупнейший в истории Великобритании зарубежный проект по развитию кибербезопасности. Министерство иностранных дел и международного развития Великобритании намеревалось повысить доступ к цифровым технологиям и улучшить кибербезопасность на пяти ключевых развивающихся рынках. Одна ветвь этого процесса была сосредоточена на том, чтобы повысить цифровую грамотность, кибербезопасность и устойчивость этих рынков.

Программа включала в себя консорциум из 21 поставщика в шести странах. Они совместно работали над решением проблемы значительного воздействия киберугроз на развивающиеся страны и предотвращения ущерба для граждан и бизнеса, в то время как компания KPMG занималась их координацией. Судьи прошли специальное обучение, чтобы лучше разбираться в киберпреступлениях. Это способствовало повышению защищенности малого бизнеса. Кроме того, была разработана национальная учебная программа по кибербезопасности, которая поможет улучшить знания в этой области. Сотрудники правительства прошли обучение по кибербезопасности. Был создан офис уполномоченного по защите данных. В Бразилии в проекте приняли участие 120 миллионов человек. Проект в Нигерии охватил более 10 % населения.

Программа дала существенные и устойчивые результаты, и созданный в ее рамках план теперь рассматривается для других рынков, включая Украину и Индию.

2.4 Состояние киберустойчивости

Киберустойчивость, как способность организации минимизировать влияние значительных киберинцидентов на основные цели и задачи, требует постоянной бдительности и неустанного планирования.

Признавая, что стопроцентная безопасность недостижима, организации должны разрабатывать адаптируемые стратегии, способствующие повышению не только их собственной устойчивости, но и устойчивости более широкой экосистемы, от которой они зависят.

Ответ организаций на киберугрозы

63 %

организаций назвали сложный и меняющийся ландшафт угроз самым большим препятствием на пути к киберустойчивости.

Около 72 % организаций заявили, что их киберугрозы увеличились за последние 12 месяцев, а 63 % назвали сложный и меняющийся ландшафт угроз самым большим препятствием на пути к киберустойчивости. Организации должны постоянно готовиться к реагированию на киберугрозы. При этом на фоне быстрого внедрения и изменения технологий нельзя забывать об основах кибергигиены — в том числе об устойчивом акценте на фундаментальных практиках и о процессе управления уязвимостями.

Сотрудничество государственного и частного секторов становится все более ценным в области реагирования на современные киберугрозы.

Среди опрошенных организаций 50 % считают обмен информацией и разведывательными (оперативными) данными наиболее эффективной мерой международного сотрудничества. Например, с помощью команд реагирования на цифровые чрезвычайные ситуации (Computer Emergency Response Teams, CERT) или центров обмена информацией и анализа (Information-sharing and Analysis Centres, ISAC). По мере того как кибератаки становятся всё более изощренными и трансграничными, специалисты в области кибербезопасности обращаются к международному сотрудничеству, основанному на экосистемном подходе. Этот подход позволяет обеспечить коллективную защиту от хорошо подготовленных преступных группировок. Хотя обмен информацией и разведывательными (оперативными) данными играет критически важную роль, передовые игроки на Ежегодной конференции по кибербезопасности в 2024 году пришли к выводу, что такие усилия все еще фрагментарны и потому недостаточно эффективны.

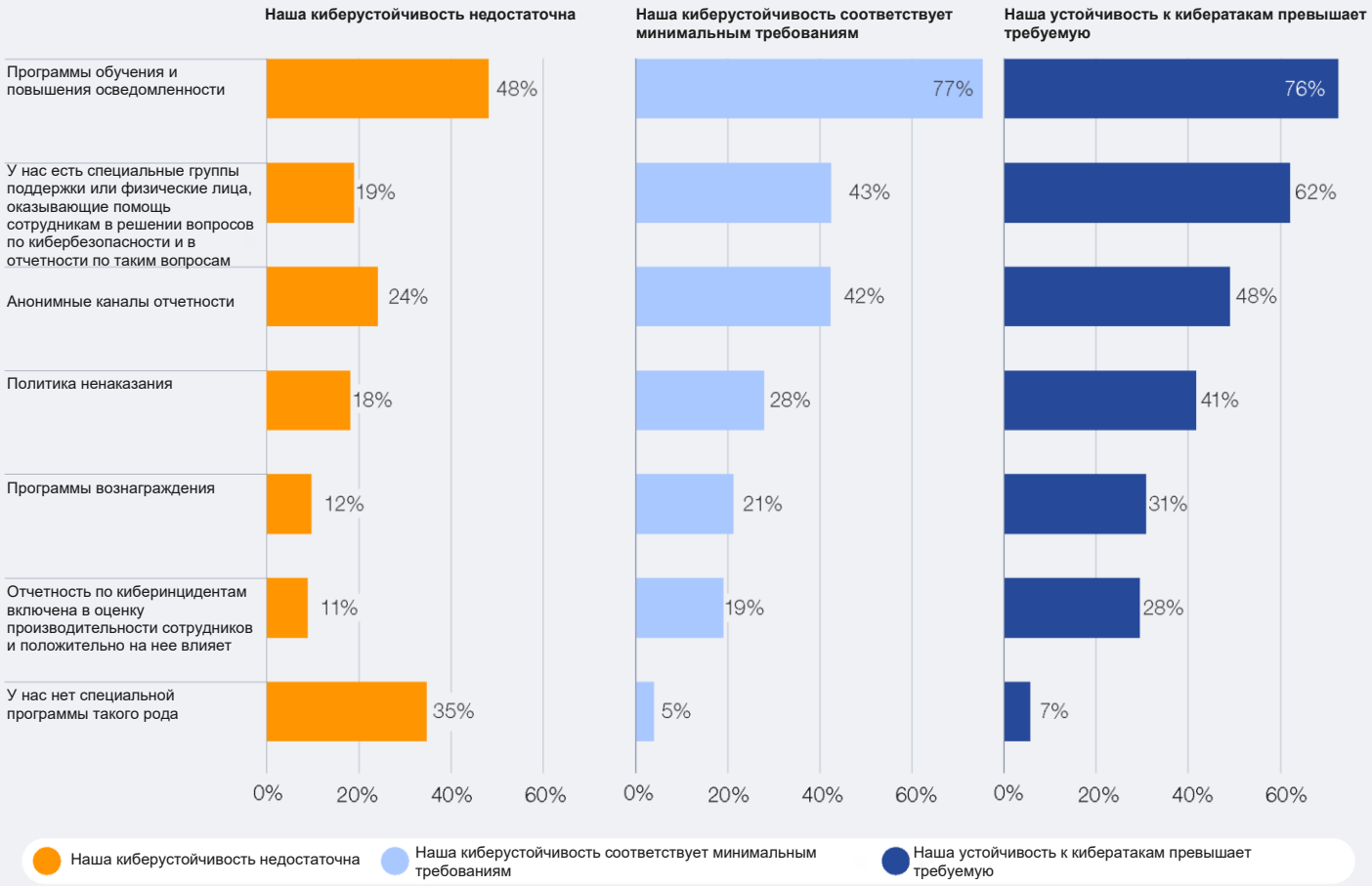
Реагирование на инциденты и управление ими

Сегодня организации сталкиваются с постоянно растущими киберугрозами, что ставит под сомнение их способность самостоятельно обеспечить быстрый и эффективный ответ на киберинциденты.

Неотъемлемой частью эффективного реагирования на инциденты является культура безопасности, в которой подчеркнуты открытость и прозрачность. Организации с высоким уровнем устойчивости применяют стимулы для отчетности по инцидентам путем различных мер поддержки: 76 % предоставляют обучение и повышение осведомленности в области кибербезопасности, 62 % располагают командами поддержки, а 48 % используют анонимные каналы отчетности. Такая среда способствует сотрудничеству и коллективному защитному мышлению, а это крайне важно для решения сложных и комплексных угроз.

РИСУНОК 15 | **Стимулы для отчетности по киберугрозам и инцидентам**

Какими способами ваша организация стимулирует сотрудников сообщать об ошибках, инцидентах и рисках в области безопасности?



ТИПИЧНЫЙ ПРИМЕР 5
Развитие навыков реагирования на киберинциденты в кооперативных банках Индии

Индийская кооперативная банковская система использует подход к банковскому делу, ориентированный на сообщества, особенно это касается сельских и сельскохозяйственных сообществ. Эти банки используют стратегические услуги от коммерческих банков для своих клиентов: они экономически эффективны для небольшого объема транзакций, легко реализуемы и требуют меньшего времени. Таким образом повышаются финансовая инклюзивность, экономическая стабильность и рост на уровне местных сообществ.

Из-за растущей сложности киберугроз кооперативные банки, испытывающие нехватку ресурсов сталкиваются с серьезными проблемами в области кибербезопасности. Отсутствие обученного персонала и недостаток уверенности при реагировании на инциденты делают эти банки уязвимыми к кибератакам. Для решения проблемы команда CERT India внедрила структурированную программу, реализованную в течение восьми месяцев с участием 40 идентифицированных кооперативных банков и включавшую киберучения для сотрудников банков. Программа обеспечила неразрывную связь между знаниями и когнитивным процессом, тем самым поощряя критическое мышление при решении проблем в управлении инцидентами.

Для оценки совокупной устойчивости этих банков киберучения были сопоставлены с четырьмя компонентами устойчивости: предвидеть, выдерживать, восстанавливаться и развиваться. Далее было вычислено взвешенное суммирование компонентов, продемонстрировавшее значительное улучшение устойчивости после реализации программы.

Санджай Бахл (Sanjay Bahl)
Генеральный директор, Индийская команда реагирования на цифровые чрезвычайные ситуации

Официальные процессы реагирования на кибер-инциденты стали неотъемлемой частью организаций; согласно опросу GCO, только 13 % опрошенных компаний не имеют возможности управлять киберинцидентами.

Наиболее распространенные элементы включают в себя сценарии реагирования на киберинциденты, кризисные учения и внутренние возможности реагирования. В этом отчете респонденты подчеркивают, что своды правил имеют решающее значение для эффективного управления угрозами, и выступают за гибкие пути реагирования в зависимости от типа инцидента, а также структурированные ответы, учитывающие масштаб и последствия сбоя.

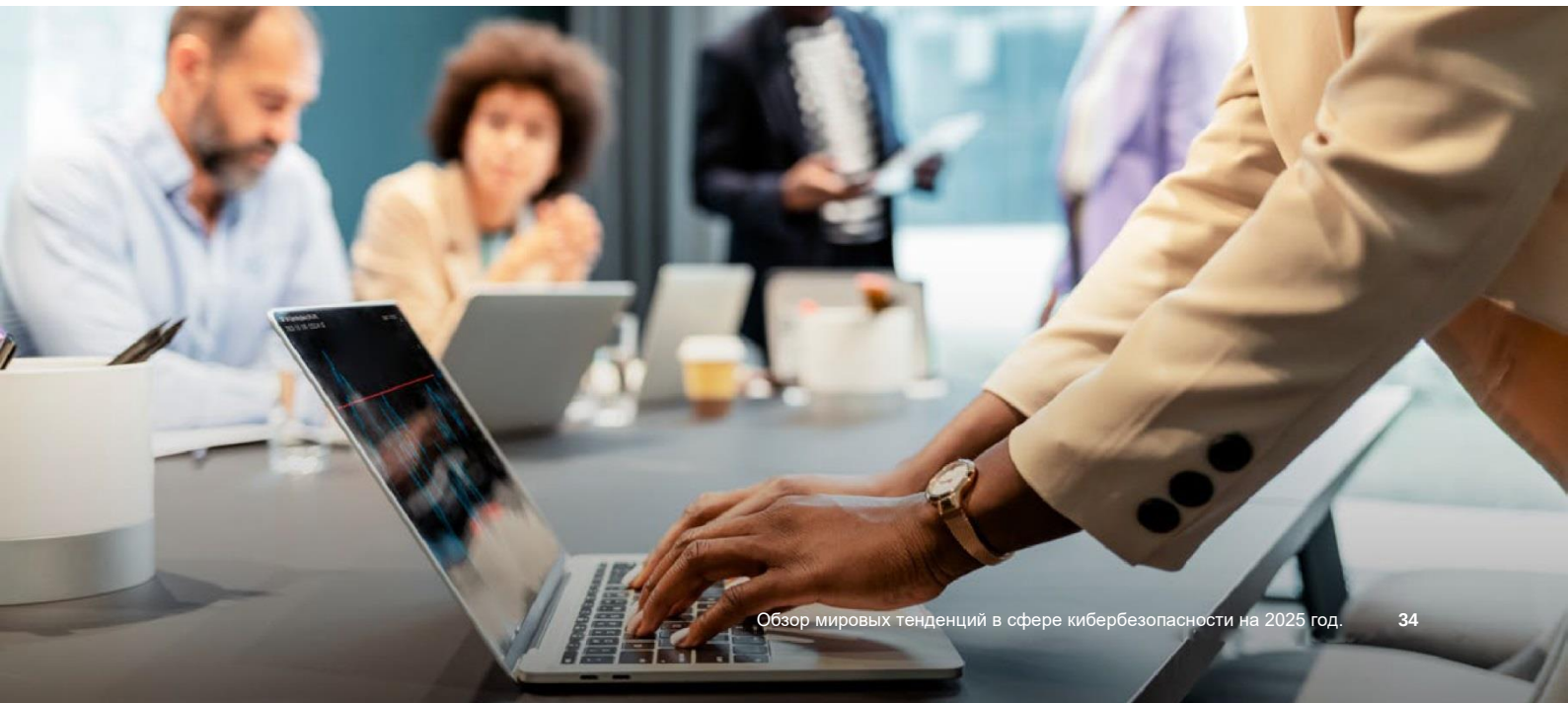
Киберстрахование

Страхование — важный инструмент в списке стратегий управления рисками, которые организации могут использовать для решения соответствующих проблем. Причем предложения по киберстрахованию в последние годы постоянно развиваются. Эксперты отрасли оценивают, что размер глобального рынка киберстрахования вырастет с 14 млрд долларов в 2023 году до 29 млрд долларов в 2027 году. Согласно опросу, наличие какой-либо формы страхования помогает организациям стать более киберустойчивыми: среди организаций, классифицированных как высокоустойчивые, только 7 % заявили, что не имеют киберстрахования.

Тем не менее киберстрахование, по-видимому, приносит больше пользы крупным организациям, чем малым, — возможно, по той причине, что они с большей вероятностью могут себе это позволить. В ходе опроса 71 % крупных компаний заявили, что их киберстрахование полностью покрывает потенциальные потери, вызванные киберугрозами. В то же время только 35 % малых организаций разделяют эту уверенность. Это, в свою очередь, способствует увеличению разрыва в уровне кибербезопасности: малые организации оказываются в более уязвимом положении.

РИСУНОК 16 **Как уверенность в киберстраховании варьируется в зависимости от размера организации**

Высказанная уверенность в киберстраховании, по размерам компании



Сложности на стыке ИТ и ОТ

Обеспечение безопасности среды ОТ является важной областью, на которую также влияет растущая сложность киберугроз. Хотя слияние ИТ и ОТ имеет признанный потенциал, эти сферы остаются различными по своим характеристикам и ролям. При этом команды ИТ и ОТ традиционно работают на разных концах технологического стека и потока данных. Они, как правило, имеют разные подходы к кибербезопасности. Отсутствие сотрудничества по формальной стратегии конвергенции ИТ/ОТ препятствует безопасной цифровизации промышленных сред.

Стратегическое планирование для обеспечения безопасности ОТ обычно осуществляется на протяжении длительных периодов и часто зависит от высокоспециализированных исполнителей. Следовательно, такое планирование лишено той гибкости в условиях срока службы и инвестиций в производственные системы, какую обычно демонстрируют системы ИТ. Киберустойчивость организации является суммой устойчивости всех ее частей. Иными словами, ИТ и ОТ больше нельзя рассматривать изолированно при разработке целостных стратегий управления рисками.

ТИПИЧНЫЙ ПРИМЕР 6

Комплексный подход Schneider Electric к кибербезопасности операционных технологий (ОТ)

Продукция Schneider Electric является неотъемлемой частью ряда жизненно важных поставщиков инфраструктуры, таких как электростанции, солнечные фермы, критически важные постройки и центры обработки данных, функционирующие в условиях все более связанных сред. С учетом роли этих секторов для национальной и глобальной устойчивости кибербезопасность является первоочередной задачей.

Schneider Electric использует принцип «Обеспечение безопасности через проектирование»: жизненные циклы безопасной разработки и независимые испытания на возможность проникновения в систему. При этом делается акцент на обеспечении безопасности заводов.

Кроме того, Schneider Electric придерживается принципа «Обеспечение безопасности через операции». Он включает в себя постоянный мониторинг и обнаружение угроз в режиме реального времени, что крайне важно для защиты операционных сред на протяжении всей производственно-сбытовой цепочки. При этом на каждом этапе четко очерчены обязанности по поддержанию мер безопасности.

Сюда также входят регулярные оценки и обновления безопасности для гарантии устойчивости системы к постоянно меняющимся киберугрозам.

Ключевая инициатива, разработанная в сотрудничестве с BitSight, направлена на выявление незащищенных протоколов ОТ в интернете, которые, подобно «открытым дверям» в критически важные системы, могут представлять угрозу безопасности. В рамках этой инициативы клиенты и представители власти активно участвуют в снижении связанных с этим рисков.

Эти усилия со стороны Schneider Electric демонстрируют готовность совместной работы со всеми заинтересованными сторонами и задействуют передовые технологии безопасности для создания более защищенной и надежной операционной среды для клиентов.

Нехватка специалистов по кибербезопасности

Нехватка специалистов по кибербезопасности по-прежнему является ключевой проблемой для организаций, стремящихся повысить свою устойчивость. Сектор кибербезопасности сталкивается со значительным недостатком кадров: по разным оценкам, не хватает от 2,8 до 4,8 млн специалистов. Острая нехватка специалистов делает киберландшафт еще опаснее: более двух третей организаций уязвимы к сложным кибератакам и утечкам данных из-за отсутствия критически важных навыков.

Согласно опросу, проведенному GCO, 39 % организаций считают, что недостаток квалифицированных специалистов является серьёзным препятствием на пути к устойчивости. Однако лишь 14 % организаций утверждают, что располагают всеми необходимыми кадрами для достижения целей в области кибербезопасности.

Разрыв в навыках с 2024 по 2025 годы увеличился на 8 % и в основном затронул государственный сектор, в котором 49 % организаций указали, что у них нет кадров для достижения целей в сфере кибербезопасности. Это на 33 % больше по сравнению с 2024 годом.

Навыки по управлению ИИ и защите от создаваемых им угроз приобретают все большую важность для следующего поколения специалистов в сфере кибербезопасности. Хотя ИИ не заменит специалистов по кибербезопасности, он станет дополнительным ресурсом в этой сфере. Это одно из решений проблемы нехватки квалифицированных специалистов не только за счет увеличения автоматизации, но и за счет подготовки кадров, способных эффективно использовать ИИ для достижения положительных результатов в сфере кибербезопасности.

РИСУНОК 17 **Как организации решают проблему нехватки специалистов по кибербезопасности**

Около 91 % участников фокус-группы на Ежегодной конференции по кибербезопасности в 2024 году пришли к выводу, что ИИ создаст новые роли в области кибербезопасности и повысит эффективность реагирования на инциденты. Тем не менее 67 % отметили нехватку инвестиций в навыки ИИ в своих организациях, что свидетельствует о разрыве между текущим состоянием обучения и изменяющейся реальностью. Вследствие этого компании должны взять на себя обязательства по обеспечению кадров необходимыми компетенциями в области ИИ и по постоянному обновлению образовательных программ для отражения динамичного ландшафта киберугроз и новых технологий.

Важным аспектом того, как ИИ может оптимизировать трудовые ресурсы и обучение для обеспечения кибербезопасности, является его способность переводить сложные данные о киберугрозах на естественный язык. Это может помочь уменьшить зависимость от технически подкованных аналитиков для понимания среды. В недавнем отчете Института безопасности и технологий (Institute for Security and Technology, IST) говорится:

«В целом, большие языковые модели (LLM) значительно упростили процесс понимания данных для всех сотрудников службы безопасности. Однако их влияние было особенно заметно в расследованиях аналитиков Уровня 1 из Центра обеспечения безопасности. Они стали быстрее выявлять и точно определять подозрительные действия».

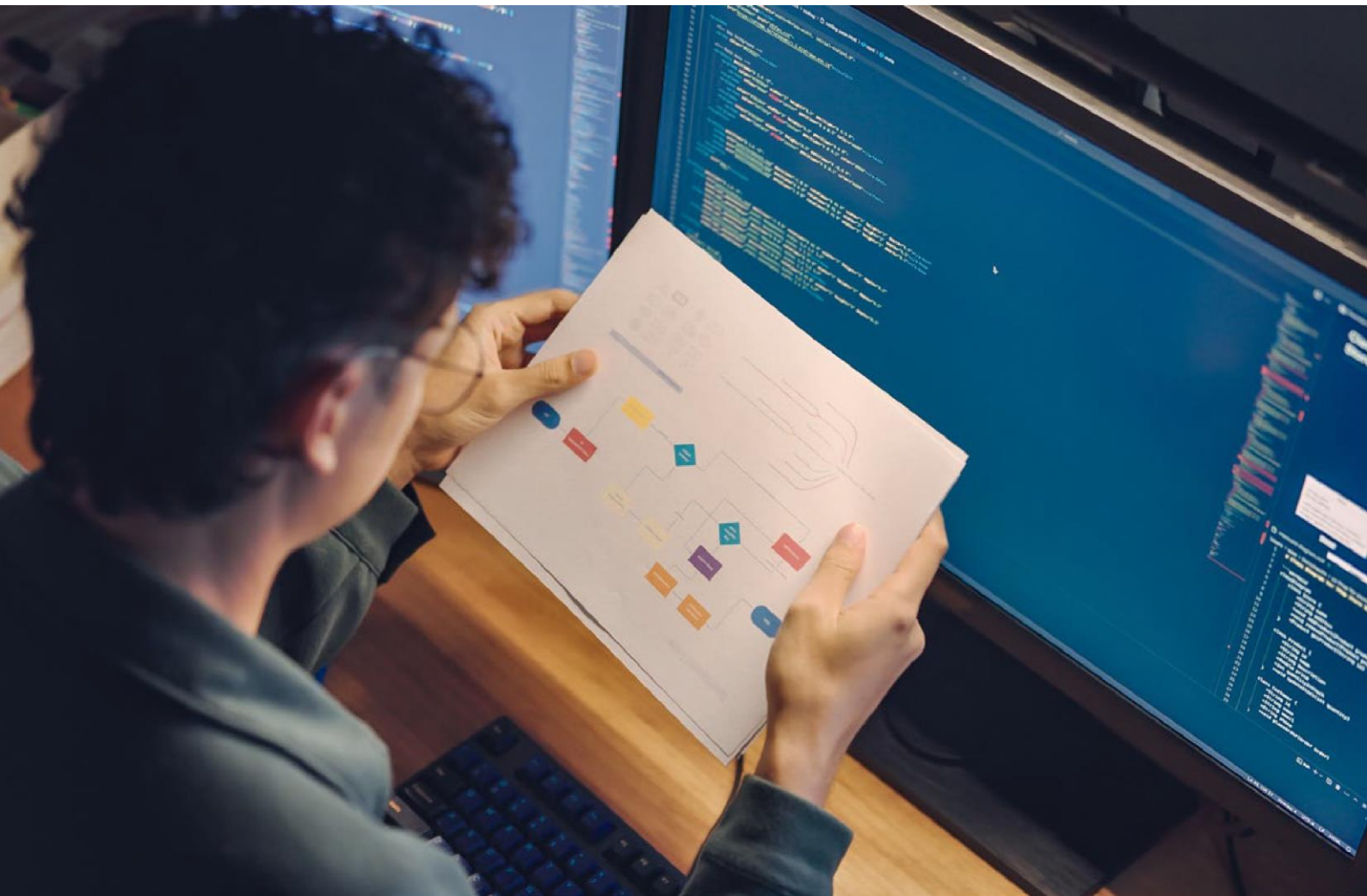
Несмотря на растущие требования, касающиеся кибербезопасности, только 23 % компаний в 2025 году выходят за рамки традиционных для этой сферы профессий, привлекая специалистов из нетрадиционных областей, таких как коммуникации, юриспруденция и финансы. Кибербезопасность становится все более сложной сферой, увеличивается ее важность для бизнеса, а также потребность в специалистах, способных обеспечить связь между техническими аспектами и результатами бизнеса. Для привлечения заинтересованных сторон и принятия обоснованных решений целесообразно использовать сторителлинг, который позволяет переводить сложные вопросы кибербезопасности на понятный повседневный язык.

МОДУЛЬ 2 ***Стратегическая кадровая программа в сфере кибербезопасности***

В апреле 2024 года Всемирный экономический форум опубликовал *Стратегическую кадровую программу в сфере кибербезопасности*. Она предлагает реальные подходы, которые помогут организациям формировать устойчивые кадровые резервы. Программа нацелена на привлечение большего количества специалистов в области кибербезопасности. Это достигается за счет более глубокого понимания специфики их работы, устранения барьеров на пути к трудоустройству и расширения кадрового разнообразия. В статье обсуждается, как обеспечить студентов и специалистов необходимыми навыками для успешной карьеры в данной сфере. Также предлагается пересмотр практики найма, чтобы решить такие проблемы, как завышенные требования к кандидатам и несогласованность между менеджерами по подбору персонала и кадровыми отделами (HR).

Также исследуются более эффективные способы удержания кадров для формирования корпоративной культуры, которая будет вдохновлять и мотивировать сотрудников.

По мере усложнения цифрового ландшафта бизнес должен адаптировать свою структуру к новым технологиям, таким как генеративный ИИ (GenAI), чтобы сохранить ее актуальность и гибкость.



Важно не только привлечь сотрудников, но и удержать их. Согласно отчету компании Gartner за 2023 год, к 2025 году почти половина руководителей в сфере кибербезопасности сменит работу, а 25 % перейдут на совершенно другие должности из-за стресса, связанного с текущей деятельностью. Выгорание является серьезной проблемой при удержании кадров, особенно с учетом высоких и постоянно меняющихся требований к специалистам в этой сфере.

Согласно исследованию компании Proofpoint, 66 % руководителей служб информационной безопасности считают, что компании ожидают от них слишком многого, причем более половины за последние полгода сталкивались с выгоранием лично или наблюдали его у коллег. Отдел кибербезопасности должен уделять большое внимание благополучию своих сотрудников и учитывать человеческий фактор в процессах принятия решений, чтобы избежать выгорания и способствовать удержанию кадров.

> **Технологии проникли во все аспекты нашей жизни, и в эпоху ИИ количество угроз быстро растет, усиливая потребность в самых совершенных мерах кибербезопасности. Необходимо активно сокращать растущий дефицит кибернавыков за счет обучения, переобучения, набора и удержания соответствующих специалистов. Технологический сектор играет важную роль, и компания Cisco гордится своей долгосрочной программой повышения квалификации Cisco Networking Academy, которая направлена на сокращение этого дефицита.**
> Чак Роббинс (Chuck Robbins), председатель совета директоров и генеральный директор Cisco

> **Сокращение дефицита специалистов в сфере кибербезопасности имеет решающее значение для защиты предприятий и решения проблемы глобальной нехватки рабочей силы. Такие программы, как Cyber Girls, крупнейшая в Африке инициатива по обучению женщин в области кибербезопасности, не только дают ключевые навыки, но и помогают улучшить благосостояние и экономические перспективы. Инвестиции в эти программы являются важным шагом к созданию более безопасного и инклюзивного цифрового будущего.**
> Конфидэнс Стэйвли (Confidence Staveley), основатель CyberSafe Foundation

МОДУЛЬ 3 Изменение роли руководителей служб ИБ

Киберпространство становится все более сложным и количество нормативных требований растет. В этих условиях советы директоров обращают большее внимание на киберриски, а руководство компаний все чаще обращается к руководителям служб ИБ, чтобы изучить киберугрозы, с которыми сталкивается организация. Опрос руководителей служб ИБ на Ежегодной конференции по кибербезопасности в 2024 году показал, что 60 % из них обсуждают кибербезопасность организации с советом директоров три-четыре раза в год. Для этого руководителям служб ИБ необходимо не только разбираться в технических аспектах своей сферы, но и рассматривать воздействие технических рисков на бизнес, оценивая киберугрозы с точки зрения финансовых потерь, государственного регулирования и доверия клиентов. Они должны предоставлять совету директоров и топ-менеджменту точные данные о том, как инвестиции в кибербезопасность обеспечивают финансовое благополучие бизнеса и его долгосрочную жизнеспособность.

Эффективные руководители служб информационной безопасности осознают, что киберугрозы представляют собой не только технические проблемы, но и серьезные бизнес-риски. Рассматривая киберинциденты в контексте устойчивого функционирования бизнеса, репутации и финансовых последствий, они помогают руководству компаний и советам директоров рассматривать кибербезопасность как часть общей картины рисков.

Например, некоторые руководители служб ИБ теперь оценивают киберриски с учетом их влияния на долю рынка, доверие к бренду, безопасность и соблюдение нормативных требований. Они показывают, что последствия таких инцидентов могут затронуть всю компанию, включая акционерную стоимость, рыночную долю, конкурентные позиции для слияний и поглощений, а также доверие клиентов. Такой подход побуждает генеральных директоров развивать стратегию устойчивости к киберинцидентам, которая не только предотвращает текущие угрозы, но и поддерживает стабильность бизнеса в долгосрочной перспективе.

Учитывая важность позиции руководителя службы ИБ, все больше внимания уделяется его месту в иерархии внутри компании, так как эта позиция определяет его влияние при разработке общей стратегии бизнеса. Почти 24 % руководителей служб ИБ, опрошенных в рамках Ежегодной конференции по кибербезопасности, напрямую подчиняются генеральному директору, что подтверждает растущую значимость этой должности.

3 Ориентирование в сложном киберпространстве

Руководители должны рассматривать кибербезопасность как стратегическую инвестицию, позволяющую обеспечить устойчивость компании перед лицом новых угроз.

Кибератаки на учреждения Коста-Рики в 2022 году стали тревожным сигналом, указывающим, что необходимо коренным образом изменить взгляд на кибербезопасность: она должна пониматься как критически важная инвестиция в будущее, а не просто статья расхода. Эти кибератаки привели не только к повышению осведомленности о проблемах кибербезопасности, но и способствовали изменению разных структур, сделав кибербезопасность ключевой темой даже на уровне домохозяйств. Решая эти вопросы, мы осознали необходимость укрепления нашей инфраструктуры за счет сотрудничества с соседями, чтобы повысить ее устойчивость не только в Коста-Рике, но и по всему региону.
Паола Богантес Самора (Paula Bogantes Zamora), министр науки, инноваций, технологий и телекоммуникаций Коста-Рики

Обзор мировых тенденций в области кибербезопасности на 2025 год демонстрирует, что киберпространство становится все более сложным. Это связано с геополитической неопределенностью и растущей изощренностью киберпреступлений, которые часто выходят за рамки контроля руководителей компаний. Тем не менее, руководство должно понимать, как совокупные последствия усложнения киберпространства повлияют на безопасность компании и страны в целом.

Преодоление этих многочисленных трудностей — задача не из легких. Для этого потребуется нестандартный подход, и почти всегда необходимо привести финансовый аргумент, чтобы подчеркнуть цену бездействия в области кибербезопасности.

3.1 Экономические аспекты кибербезопасности

Так как в прошлом кибератаки были прямо связаны с более широким экономическим контекстом, особенно в случаях, когда они приводили к ощутимому ущербу для экономики в целом, руководители как в частном, так и в государственном секторе уделяют все большее внимание финансовым факторам и последствиям киберинцидентов. Рост организованной киберпреступности, крупномасштабные атаки на критическую инфраструктуру и быстрое внедрение технологий, влияющих на социальное и экономическое развитие, подтверждают, что обеспечение кибербезопасности имеет далеко идущие экономические последствия.

Также важно понимать, как киберпреступность размывает понятие экономической ценности. Из-за минимальных операционных затрат и потенциально высоких доходов киберпреступность становится очень прибыльным занятием. По оценкам Федерального бюро расследований США (Federal Bureau of Investigation, FBI), в 2023 году потери от киберпреступности превысили 12,5 млрд долларов. По мере того как киберпреступники становятся более организованными и используют инновационные технологии, многие компании прибегают к киберстрахованию, чтобы снизить финансовые последствия кибератак. Однако из-за растущего количества киберпреступлений страховщики изменяют размер страховых премий и условия покрытия, что делает защиту бизнеса более дорогостоящей.

В таких условиях руководители должны количественно оценить киберриски и их экономические последствия, чтобы согласовать инвестиции в кибербезопасность с основными бизнес-целями. При этом руководители, которые имеют ресурсы, должны помочь тем, кто не имеет таких возможностей, взяв на себя ответственность и обеспечив системный подход.

Одним из основных принципов киберэкономики является нахождение баланса между инвестициями в кибербезопасность и управлением разнонаправленными приоритетами бизнеса. Из-за того, что киберпространство усложняется, киберриски затрагивают все большее количество подразделений организаций, и успешные руководители должны умело ориентироваться среди этих рисков, так же как они ориентируются в конъюнктуре рынка. Несмотря на то что более 60 % опрошенных генеральных директоров и руководителей служб ИБ сообщают, что управление киберрисками интегрировано в систему управления рисками предприятия, многие все еще не могут точно оценить объем необходимых инвестиций. На сегодняшний день менее половины генеральных директоров считают, что их организации вкладывают достаточно средств в кибербезопасность.

Хотя упреждающие меры безопасности, такие как многофакторная аутентификация, межсетевые экраны и обучение в области безопасности, могут быть дорогостоящими, они значительно перевешивают финансовые потери от кибератак. Однако малые и средние предприятия, обладающие ограниченными финансовыми ресурсами, могут быть склонны избегать подобных затрат, если не получат убедительных доказательств их целесообразности. Интересно, что попытки выявить возможные меры стимулирования напоминают глобальные меры по борьбе с кризисными ситуациями в физическом мире, а именно на усилия по преодолению климатического кризиса. В разных странах мира разрабатываются стимулы, призванные побудить граждан использовать возобновляемые источники энергии. Например, предлагаются значительные субсидии для установки солнечных панелей или тепловых насосов. Было бы разумно, если бы правительство оказывало такую же поддержку малым и средним предприятиям, чтобы они могли лучше противостоять киберугрозам и внедрять активные меры безопасности.

Одним из основных препятствий для адекватных инвестиций в кибербезопасность является невозможность эффективной количественной оценки киберрисков из-за постоянно меняющегося ландшафта угроз, а также сложности оценки потенциального воздействия киберинцидентов. Однако компаниям очень важно оценить киберриски в финансовых терминах, чтобы эффективно распределить ресурсы и повысить устойчивость.

Экономический аспект кибербезопасности также связан со спросом на специалистов в этой сфере. Рынок вакансий в области кибербезопасности быстро растет, что дает возможность строить долгосрочные карьеры, выгодные с финансовой точки зрения.

Новые рабочие места не только улучшают качество жизни отдельных людей, но и способствуют общему экономическому росту отраслей и регионов.

Хотя киберэкономика — это сложная и обширная область, требующая дальнейшего изучения, идея о том, что устойчивость к киберинцидентам должна опираться на обоснованные экономические аргументы, представляется весьма убедительной. В настоящее время руководители уже не могут игнорировать эту концепцию. Заинтересованное руководство, разумные инвестиции и сформированная культура безопасности помогут обеспечить устойчивость организации в целом.

Заключение

Киберпространство становится всё более сложным и непредсказуемым, что ставит под угрозу устойчивость компаний и выявляет слабые места в их способности противостоять киберугрозам.

В таких условиях все труднее обеспечить безопасность, что усугубляет неравенство, то есть менее обеспеченные компании становятся более уязвимыми. Геополитическая напряженность побуждает организации пересматривать свои стратегии, балансируя между вопросами обеспечения безопасности и деятельностью на международном рынке. Такая напряженность часто приводит к целенаправленным атакам, когда спонсируемые государствами лица используют уязвимости для шпионажа и дестабилизации. В таких непредсказуемых условиях необходимы адаптивные стратегии, которые бы учитывали изменения глобальных рисков и цепочек поставок.

В то же время постоянную озабоченность вызывает тот факт, что киберпреступления становятся все более изощренными. Использование искусственного интеллекта (ИИ), так называемых «вирусов-вымогателей как услуги» (RaaS) и современных методов социальной инженерии приводит к тому, что современные угрозы становятся все более сложными и быстро опережают традиционные системы защиты. Чтобы справиться с этими растущими угрозами, необходимы не только передовые технологические решения, но также сотрудничество в разных отраслях и обмен знаниями.

Несмотря на все препятствия, основания для оптимизма все же имеются. Организации, которые практикуют упреждающее управление рисками, уделяют особое внимание сотрудничеству в области инфраструктуры и инвестируют в масштабируемые и справедливые решения, способствующие сокращению неравенства. Исправление системных уязвимостей, таких как зависимости от поставок и нехватка квалифицированных кадров, будет ключевым фактором для развития устойчивой цифровой инфраструктуры.

В конечном счете, чтобы решить насущные задачи, нам нужны не только технические новшества, но и свежий взгляд на проблему. Устойчивость к киберугрозам должна восприниматься как общая ответственность. Компании разных размеров должны взаимодействовать для создания взаимосвязанных сетей, которые являются основой цифровой экономики. Кроме того, руководство должно проявить решительность и сделать кибербезопасность главным приоритетом как внутри организаций, так и в их взаимодействии. Наряду с техническими показателями, необходимо разработать надежные критерии, основанные на экономических последствиях киберугроз. Формирование единой руководящей команды, в которой бизнес-лидеры и руководители служб ИБ разделяют общий взгляд на киберриски для организации, является важнейшим шагом к успешной борьбе с постоянно растущими и сложными киберугрозами.

Приложение: методология

Обзор мировых тенденций в сфере кибербезопасности (GCO) является основным источником данных для данного отчета. Он включает в себя 24 вопроса для всех респондентов (а также пять вопросов только для респондентов-руководителей служб ИБ) и семь дополнительных вопросов о демографии. Опрос был начат 2 сентября 2024 года и продолжался до 11 октября 2024 года. Всемирный экономический форум получил ответы от 409 участников опроса из 57 стран. После нормализации набора данных с использованием семи демографических вопросов для квалификационного отбора выборка составила 321 человека. Каждый из 321 участника заполнил анкету полностью.

Для получения более глубоких и качественных данных было проведено 43 индивидуальных интервью с руководителями высшего звена, отраслевыми лидерами и представителями науки. Вопросы интервью частично совпадали с вопросами опроса, а также дополняли его, что позволило провести более тщательный анализ уже имеющихся данных.

В июле 2024 года было проведено 90-минутное совещание с участием десяти членов Глобального совета будущего по вопросам кибербезопасности, лидеров мнений из академической среды, государственных структур, международных организаций, бизнеса и гражданского общества. Целью мероприятия было обсуждение тем, представленных в опросе Обзора мировых тенденций в области кибербезопасности. Кроме того, в октябре 2024 года состоялось 90-минутное совещание с участием 20 специалистов из Сообщества руководителей служб ИБ Всемирного экономического форума, по вопросам, рассмотренным в этом отчете. Дополнительные количественные данные были собраны в ходе опроса, который состоял из двух вопросов, адресованных участникам мероприятия.

Ежегодная конференция по кибербезопасности в рамках Всемирного экономического форума прошла с 11 по 13 ноября 2024 года. В течение нескольких встреч были получены сведения качественного уровня от более чем 170 руководителей, которые приняли участие в этом мероприятии. Количественные данные были собраны из ответов на шесть вопросов, заданных аудитории.

СТРЕМИМСЯ УЛУЧШИТЬ ПОЛОЖЕНИЕ ДЕЛ В МИРЕ

Всемирный экономический форум — это международная организация государственно-частного сотрудничества, целью деятельности которой является улучшение положения дел в мире.

В Форуме принимают участие крупнейшие деятели политики, бизнеса и других общественных институтов, которые формируют глобальную, региональную и отраслевую повестку.

Всемирный экономический форум
91-93 рут де ля Капит
CH-1223 Колоньи/Женева
Швейцария

Тел.: +41 (0) 22 869 1212
Факс: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org