сенсус

ЦИФРОВОЙ МАРКЕТПЛЕЙС

Цифровые решения – 2026 · аналитика по направлениям

Кибербезопасность, доверие и борьба с мошенничеством: защита догоняет скорость атак

Что говорили на форуме «Цифровые решения – 2026» об антифроде, атакующем ИИ, защите ИИ-агентов, подрядчиках и МСП, КИИ и биометрии: цифры, позиции регуляторов и бизнеса, барьеры и предложения.

Содержание

Ключевые показатели

Кратко

1. Антифрод как государственная инфраструктура

2. Платформы, операторы связи и человек как цель атак

3. Атакующий ИИ: скорость атак и порог входа

4. ИИ-агент как новый тип нарушителя

5. Цепочки поставок, подрядчики и малый бизнес

6. КИИ и регуляторика: «сначала ИТ, потом ИБ»

7. Доверенная разработка, криптография и международное измерение

8. Биометрия и цифровая идентификация

9. Киберустойчивость: реагирование и восстановление

10. Bug bounty, киберстрахование и кадры

11. Барьеры и предложения

12. Ключевые игроки темы

Выводы

Источники

Ключевые показатели

40 минут

От выхода исправления до атаки агентскими системами

Баранов Денис, Positive Technologies

870 млн

Мошеннических звонков пресечено в сети Билайна

С начала года, порядка; Анохин Сергей, Билайн

около 40

Участников подключено к ГИС «Антифрод»

Скворцова Татьяна, Минцифры России

более 60%

Доля социальной инженерии в успешных атаках на организации

Зиновкина Ирина, Positive Technologies

в 125 раз

Сокращение злоупотреблений на Авито за 6 лет

Юматова Наталья, Авито

17%

МСП с комплексной киберзащитой и шифрованием

Опрос малого бизнеса; Охрименко Алексей, Корпорация МСП

80%

Компании без нескольких специалистов по ИБ

Богомолов Егор, CyberED

около 5 млн

Атаки на РЖД за текущий год

Ташимов Борис, Минтранс России

55 млн

Уникальные пользователи Единой биометрической системы

Скворцова Татьяна, Минцифры России

0

Успешные атаки на 27,5 млн биометрических оплат в Сбере

Евсеев Олег, Сбер

1–4 млрд руб.

Российский рынок защиты ИИ-систем, сентябрь 2026

Оценка; Устинова Анна, «Ведомости»

90–95%

Доля атак, которую отражает отдельный дипфейк-детектор

Оценка; Марков Дмитрий, VisionLabs

2 из 30

Руководители, согласные на бесплатный тест защищённости

Новиков Алексей, Positive Technologies

до 30 млн руб.

Компенсация ущерба клиенту JSOC One при неотражённой атаке

Ляпунов Игорь, ГК «Солар»

Кратко

Кибербезопасность на форуме «Цифровые решения – 2026» обсуждали на пленарных дискуссиях, отраслевых конференциях и узких экспертных секциях: в основу обзора легли выступления более чем на 30 сессиях с участием Минцифры России, Минтранса России, Positive Technologies, «Лаборатории Касперского», ГК «Солар», Сбера, Авито, Ozon, Билайна и VK Tech. Фокус сместился с периметра и формального соответствия требованиям к скорости. Атака с применением ИИ-агентов может начаться через 40 минут после выхода исправления, а процессы защиты рассчитаны на дни (Баранов Денис, Positive Technologies).

Вторая линия – мошенничество как межотраслевая задача. К ГИС «Антифрод» подключено около 40 участников, с 1 марта 2027 года подключение станет обязательным (Скворцова Татьяна, Минцифры России). Социальная инженерия даёт более 60% успешных атак на организации (Зиновкина Ирина, Positive Technologies). Комплексную киберзащиту используют 17% малых компаний (Охрименко Алексей, Корпорация МСП), а в 80% компаний нет даже нескольких специалистов по ИБ (Богомолов Егор, CyberED).

1. Антифрод как государственная инфраструктура

1.1 ГИС «Антифрод» и консолидированная ответственность

Борьба с мошенничеством переходит от добровольного обмена данными к обязательной государственной системе. Председатель Правительства РФ Михаил Мишустин на главной пленарной сессии сообщил, что сформирована единая антифрод-платформа обмена данными банков, операторов связи и цифровых платформ в реальном времени. Татьяна Скворцова (Минцифры России) раскрыла детали. Система создана законом № 41-ФЗ. Приняты два пакета антифрод-мер (41-ФЗ и 210-ФЗ), третий находится на обсуждении. К ГИС подключено около 40 участников: большая четвёрка операторов, более 25 финансовых организаций и цифровые платформы. Запущено 11 сценариев взаимодействия, до конца года в плане – 34.

Аргумент в пользу обязательности Скворцова сформулировала прямо: добровольные каналы не накладывают ответственности на участников. «В добровольном порядке здесь, конечно, мы проблему не решим», – сказала она. Подключение станет обязательным с 1 марта 2027 года для операторов связи, кредитных организаций, цифровых платформ и ряда органов власти. До конца года Минцифры планирует подключить более 120 участников. Ограничение тоже названо: в России около 7 000 операторов связи, и подключить их всех за год не получится. Россия выбрала модель консолидированной ответственности, а не британскую, где основная нагрузка лежит на банках (Скворцова Татьяна, Минцифры России).

> Блокирование возможных случаев мошенничества, а не устранение уже их результата. – Татьяна Скворцова, Минцифры России

1.2 Статистика и спор о превентивной блокировке

Статистика мошенничества пошла вниз, но оценки расходятся. Мишустин говорил о сокращении киберпреступлений за 8 месяцев практически на треть. Алексей Борискин (ФГБУ «Центр экспертизы и координации информатизации») привёл данные МВД: после первого пакета мер число преступлений к концу года снизилось на 90 000. Олег Капранов (РОЦИТ) со ссылкой на МВД назвал снижение мошенничества за 8 месяцев на 29%, Скворцова – на 32% к прошлому году.

Есть и регуляторное противоречие. Платформы указывают, что закон о платформенной экономике разрешает блокировку день в день только для предотвращения нарушения закона, в остальных случаях нужно уведомить за 3 дня. Михаил Рыженков (Авито) спрашивает, относится ли срабатывание антифрода к первому случаю. Левон Айрапетян (Авито) предлагает точечно скорректировать регулирование, чтобы разрешить превентивные механизмы.

2. Платформы, операторы связи и человек как цель атак

2.1 Автоматический антифрод на масштабе

Машинная модерация стала основой защиты цифровых платформ. Наталья Юматова (Авито) сообщила, что за 6 лет компания инвестировала около 22 млрд руб. в безопасность, из них 7 млрд – за последний год. Число злоупотреблений сократилось в 125 раз, за последний год – на 55%. Каждый день на платформе совершается около 30 млрд действий, и все они анализируются моделями (Рыженков Михаил, Авито). Александр Васильев (Ozon) сообщил, что за 3 года число жалоб на мошеннические операции на площадке снизилось в 10 раз при росте оборота в 3 раза – до более чем 4 трлн руб. В этом году антифрод Ozon предотвратил 322 тыс. подозрительных операций на сумму около 1,5 млрд руб. По его словам, 98% случаев решаются автоматически, в 2% решение принимает человек.

Операторы связи перешли к перехвату звонков. Сергей Анохин (Билайн) сообщил, что с начала года в сети оператора пресечено порядка 870 млн мошеннических звонков, их переводят на ИИ-персонажей «киберсемьи». По данным Билайна, ИИ-ассистент «кибербабушка» проговорил с мошенниками более 140 тыс. минут за год, а собранные паттерны используются для обучения людей и антифрод-системы. МТС, по данным компании, требуется 15 секунд, чтобы распознать мошенника с нового номера. Григорий Кузнецов (Билайн) описал цель так: сделать мошеннические атаки бессмысленными или малоцелесообразными для самих мошенников.

2.2 Мошенники уходят в мессенджеры

Следующий фронт – мессенджеры. Операторы не видят данных внутри них, и, по словам Кузнецова, быстрого решения здесь нет: нужна плотная онлайн-интеграция с разработчиками мессенджеров. Максим Кабрера (Билайн) описал возврат фишинга в мессенджеры в виде трёхуровневых схем. Алексей Лукацкий (Positive Technologies)

отметил, что антифрод-меры переводят мошенников в неконтролируемые каналы: борьба идёт с каналом, а не с причинами. Евгений Руденко (Rambler&Co) советует «выработать у себя привычку, что общение в мессенджере – это как стоять и кричать на площади». Юматова фиксирует ещё один сдвиг: после победы над взломами и массовой регистрацией главным источником учётных записей для мошенничества стала их аренда.

2.3 Социальная инженерия, дети и дропперы

Технические меры не устраняют уязвимость человека – в этом сходятся почти все спикеры. Ирина Зиновкина (Positive Technologies) оценила долю социальной инженерии в более чем 60% успешных атак на организации и около 99% – на частных лиц. Елена Орлова (Wildberries) говорит, что ИИ удешевляет многошаговые персонализированные схемы, и мошенничество перестаёт быть делом картелей. Руденко добавил, что «на идеальное фишинговое письмо почти невозможно среагировать».

> Мошенничество может быть, не хочется так говорить, но в каждом доме. Каждый человек может воспользоваться искусственным интеллектом и какой-то общедоступной схемой попытаться кого-то обмануть. – Елена Орлова, Wildberries

Отдельный блок – дети и подростки. Елена Мулланурова («Аргументы и факты») привела данные МВД: за 8 месяцев число несовершеннолетних, совершивших киберпреступления, выросло на 28%. По данным Банка России, которые она назвала, в прошлом году было почти 700 000 счетов, связанных с дропперством, до 20% из них – на несовершеннолетних. Большинство родителей и подростков не знают, что за дропперство введена уголовная ответственность. Подросток ради 4 000 руб. получает уголовное дело и 80 часов исправительных работ. Мошенники запугивают детей и через них получают доступ к счетам родителей.

Предложения в этой части касаются распределения ответственности и просвещения. Руденко считает, что основную ответственность должны нести регуляторы, операторы, банки и платформы, а не граждане. Орлова предлагает перевести обучение ИБ на государственный уровень с обязательным предметом в школах и вузах. Николай Лишин (ФМБА России) предлагает зачёт по «информационному ОБЖ» для школьников. Кузнецов сравнил задачу с ремнём безопасности: водитель от него не стал умнее, но последствия сведены к минимуму.

3. Атакующий ИИ: скорость атак и порог входа

3.1 Сорок минут от исправления до атаки

ИИ резко ускорил атакующих – это самый частый тезис форума. Денис Баранов (Positive Technologies) на главной пленарной сессии сказал, что после выпуска исправления атака с применением агентских систем может начаться через 40 минут, тогда как человеческие процессы выстроены на дни. Алексей Новиков (Positive Technologies) добавил: «Никто не

ставит за 40 минут обновления безопасности у нас в России». По данным ЦСР, которые привела Екатерина Кваша (Центр стратегических разработок), число атак с использованием ИИ в мире выросло на 89% в 2025 году.

> У злоумышленников появилось абсолютное оружие за 20 баксов, которое может положить на лопатки 95 процентов компаний. – Егор Богомолов, CyberED

3.2 Один человек с роем агентов

Снизился и порог входа. Алексей Фетисов (Альфа-Банк) сказал: «Сейчас вчерашний школьник, вооружённый моделями, у которых удалили гардрейлы, к сожалению, достаточно профессионален». Белый хакер Дмитрий Серебрянников отмечает: атаки, которые раньше требовали команды из 5–10 человек, теперь проводит один человек с роем агентов. Анна Кулашова («Лаборатория Касперского») привела расследование атаки на южнокорейские компании, которую провёл один хакер с множеством ИИ-агентов. При этом Александр Шойтов (Минцифры России) и Кулашова уточняют: принципиально новых средств атаки ИИ пока не создал, он кардинально усиливает существующие и ускоряет поиск уязвимостей.

3.3 Поток отчётов и защита машинами

Побочный эффект – поток сгенерированных отчётов об уязвимостях. На bug bounty-площадке Positive Technologies, по словам Новикова, число отчётов за примерно 4 месяца выросло втрое, многие написаны нейросетями. Google, по словам Кулашовой, отключил приём заявок из-за потока ложных отчётов. Общий вывод участников: защищаться от машин будут машины. Алексей Усанов (Positive Labs) прогнозирует: «Мы придём к тому миру, когда защищать нас может только полностью решение, построенное на базе искусственного интеллекта».

4. ИИ-агент как новый тип нарушителя

4.1 Скрытые инструкции, теневой ИИ и масштаб ошибок

Собственные ИИ-внедрения компаний стали отдельным источником риска, и агента предлагают включать в модель угроз. Главный сценарий – непрямая prompt injection. Валерия Воробьева (Альянс в сфере ИИ) и Дмитрий Лазаренко (VK Tech) описали агента с доступом к почте, который исполняет скрытые во входящем письме команды. Кулашова назвала это новой фишинговой схемой, в которой данные уходят злоумышленнику без участия человека. Большие языковые модели подвержены такой атаке независимо от происхождения.

> Если традиционную систему вы пытаетесь атаковать, найти уязвимость, то агента можно уговорить или уболтать. – Дмитрий Лазаренко, VK Tech

Второй риск – теневой ИИ. Сотрудники сами устанавливают агентов и пользуются внешними чатами, передавая конфиденциальные данные в облако. Антон Ефимов (ГК «Солар») рассказал о заказчике, где закупщики незаметно для ИБ запустили 30 агентов: «раскатали по тихой грусти 30 агентов на свои, и никто этого не заметил». О выносе корпоративных данных через самостоятельно оплаченные модели говорили представители Cloud.ru, «Норникеля» и Т-Банка. Кулашова предупредила, что ограничения локальной модели могут подтолкнуть сотрудников к личным аккаунтам во внешних сервисах. Спикеры секции по безопасности ИИ-моделей, по словам Дмитрия Служеникина (НТЦ ЦК), единодушны: к теневому ИИ нужно строить безопасный шлюз, а не запрещать его.

Третий риск – ответственность и масштаб. Дмитрий Никишов (Банк ДОМ.РФ) предупреждает, что массовое повторение внешне безобидных действий агента способно перерасти в масштабную проблему. Сергей Сергиенко (Минцифры России) указал, что агент с полномочиями в нескольких организациях становится точкой утечки данных всех этих организаций, а идентификации и CAPTCHA для защиты от агентов недостаточно.

4.2 Как контролируют агентов

Набор практических мер повторялся из сессии в сессию. Агентам выдают отдельные идентификаторы, назначают ответственного руководителя и предусматривают отзыв доступа (Лазаренко Дмитрий, VK Tech). Доступ ограничивают принципом минимальных привилегий, запросы журналируют, запрещённые данные блокируют фильтрами шлюза (Лискин Александр, «Лаборатория Касперского»). Применяют сегментацию сети, песочницы и LLM-шлюзы (Кулашова Анна, «Лаборатория Касперского»). Для масштабирования агентных систем Сергей Голицын (T1) предлагает MCP-шлюзы. Юрий Максимов (Positive Technologies) формулирует задачу иначе: контролировать соответствие действий агента поручению человека, а не только задавать запреты. Лазаренко настаивает на независимой проверке: «Тестировать должна другая модель и другой агент».

4.3 Рынок и нормы

Рынок средств защиты ИИ формируется. По оценке, которую привела модератор Анна Устинова («Ведомости»), российский рынок защиты ИИ-систем составлял 1–4 млрд руб. на сентябрь 2026 года. Лукацкий насчитал более 10 российских производителей AI Security Gateway. Лазаренко со ссылкой на прогноз считает, что через 5 лет порядка 10–15% ИИ-агентов будут защищать других агентов.

Нормативная база тоже меняется. Служеникин сообщил, что ГОСТ по безопасной разработке будет дополнен требованиями к безопасности технологий ИИ, а к приказу ФСТЭК № 117 готовятся изменения с требованиями к ИИ в госсистемах. Сергиенко предложил рассмотреть регистрацию агентов доверенной стороной с выдачей «паспорта» по аналогии с удостоверяющими центрами, особенно для КИИ. Служеникин считает, что требования стоит уточнять по отраслям и системам, а не сертифицировать технологию вне контекста.

5. Цепочки поставок, подрядчики и малый бизнес

5.1 Подрядчик как точка входа

Крупные компании защищены лучше, поэтому атаки идут через поставщиков. Баранов сказал, что в России через цепочки поставок атакуют вдвое чаще, чем в остальных странах, потому что цель – нанести неприемлемый ущерб, а не украсть. Фетисов говорит, что большинство успешных атак последних лет идёт через менее защищённого подрядчика. Кулашова фиксирует рост атак через доверенные отношения примерно с 2023 года.

Госсектор описал свою специфику. Михаил Абрамов (ФНС России) объяснил, что из-за зарплат по 79-ФЗ в госорганах не хватает внутренней экспертизы, и подрядчики получают доступ в инфраструктуру. Технических средств для разграничения их доступа с передачей экспертизы сотрудникам на рынке почти нет.

Меры защиты – контрактные и технические. Андрей Устюжанин (ДОМ.РФ Технологии) предлагает закреплять требования к подрядчикам ещё в договоре: ограничения доступа, штрафы и ответственность за инциденты. Новиков предлагает крупным компаниям «взять шефство» над подрядчиками с правом на аудит и пентест. В Роскосмосе, по данным корпорации, действует нулевое доверие к подрядчикам: они передают исходные коды, а установку после проверки делает внутренний DevOps. Елена Бочарова («Киберпротект») отмечает разрыв: крупнейшие заказчики ПО предъявляют требования к поставщикам-МСП, но фактически их не проверяют.

5.2 МСП: экономика защиты

Защита для малого бизнеса стоит дорого, а последствия атак тяжелее. Кваша сообщила, что 82% российских МСП сталкивались с киберинцидентами, а в пилотной оценке ЦСР в 4 из 5 отраслей доступность киберустойчивости для МСП низкая. Алексей Охрименко (Корпорация МСП) привёл опрос: средний индекс цифрового развития малого бизнеса – около 2,5 балла из 5, комплексную киберзащиту и шифрование используют 17% респондентов. Наименьшие оценки защищённости – у торговли, бытовых услуг и строительства. По статистике «Лаборатории Касперского», которую привела Кулашова, примерно половина МСБ после успешной атаки лишается бизнеса.

> Крупный бизнес не может просто взять и переложить это на МСП, сам должен тоже, в том числе этим заниматься. – Екатерина Кваша, Центр стратегических разработок

Максим Никандров (iGrids) показал экономику защиты на своём примере. Вход в систему защиты стоил 10–12 млн, ежегодные расходы – 3 млн с ростом 15% в год. По его условной оценке, при сохранении стоимости защиты из технологического сегмента МСП может уйти до 80% компаний.

5.3 Безопасность как свойство сервиса

Из разговора о МСП вырос общий тезис: малый бизнес не будет строить защиту сам. Шойтов считает, что держать службу ИБ в каждой малой компании нет смысла и нужен аутсорсинг. Игорь Ляпунов (ГК «Солар») ожидает, что МСП будет покупать кибербезопасность как свойство ИТ-сервиса у оператора связи или облачного провайдера. По его словам, «Солар» запустил платформу JSOC One с контрактом от 3 млн руб. в год и обязался компенсировать заказчику ущерб до 30 млн руб., если не отразит атаку. Новиков предложил провайдерам модель встроенной безопасности с гарантией компенсации при взломе клиента.

Звучали и предложения к государству. Игорь Вербицкий (Яндекс 360) предложил налоговые послабления для МСП, достигших определённого уровня защищённости. Федор Севастьянов («Бастион») – задавать требования ключевым отраслевым подрядчикам и одновременно создавать доступные сервисы киберзащиты. Бочарова предложила опросник самодиагностики и короткий курс минимальной защиты для МСП с Корпорацией МСП и Минэкономразвития. По её прогнозу, в 2027 году появится горячая линия для МСП при киберинциденте.

6. КИИ и регуляторика: «сначала ИТ, потом ИБ»

6.1 Требования есть, исполнения нет

Регуляторы говорили прежде всего о дисциплине исполнения: требования и методики есть, но владельцы систем их не выполняют. Шойтов на пленарной сессии назвал системной проблемой подход, при котором защита догоняет уже созданные системы: «Сначала IT, потом за этим должна идти информационная безопасность. Это очень дорого, это наш менталитет». По его словам, требования, методики и средства защиты даны, но владельцы систем не выполняют даже простейших мер. Ефимов оценил, что примерно у 95% компаний ИБ догоняет ИТ. Игорь Качалин (НТЦ ЦК) заметил: если бы предполагаемый визит хакера в информационную систему вызывал такой же трепет, как визит прокуратуры или Счётной палаты, отношение к кибербезопасности изменилось бы.

> Мы же дали все требования, методики, все средства есть, коллеги, вот не сделаны простейшие вещи. – Александр Шойтов, Минцифры России

6.2 Безопасность с этапа проектирования

Ответ – проектирование безопасности с начала. Кулашова описала кибериммунитет: цели безопасности задаются при проектировании, доверенная вычислительная база минимизируется. Система без заложенной модели угроз и криптографии, по её словам, – как самострой, который рано или поздно сносят. Павел Торопин («Норникель») рассказал,

что security by design в новых ИТ-проектах снизил затраты. Аэрофлот после крупного инцидента закладывает требования ИБ в каждый проект и не пускает в эксплуатацию системы с рисками (Попов Денис, Аэрофлот).

6.3 Транспорт: донастройка КИИ

Транспорт стал примером отраслевой донастройки КИИ. Борис Ташимов (Минтранс России) сообщил, что РЖД зафиксировали около 5 млн атак за год, причём за полгода – больше, чем за весь предыдущий год. Все объекты транспорта отнесены к КИИ, и фокус защиты, по его словам, нужно сузить до действительно критичных. В закон о КИИ внесены изменения, Минтранс готовит подзаконные акты. Минэнерго провело в одном из регионов контролируемую кибератаку на отрасль, Минтранс планирует перенять этот опыт.

7. Доверенная разработка, криптография и международное измерение

7.1 Российская криптография и подпись кода

Отечественная криптография уже лежит в основе массовых государственных сервисов, но полной цепочки доверия пока нет. Качалин напомнил, что удалённое электронное голосование и цифровой рубль построены на российских криптомеханизмах. В эксперименте по подписи кода показано, что любое российское средство защиты подходит и для подписи, и для проверки, и все они взаимозаменяемы. В рабочую группу по подписи кода входит более 80 разработчиков ПО и СЗИ. Качалин признаёт, что до полной цепочки доверия – от прикладного ПО до драйверов и аппаратной платформы – ещё далеко.

> Криптография должна быть арматурой, которая должна пронизывать всё здание информационной системы от фундамента до крыши. – Игорь Качалин, НТЦ ЦК

7.2 Безопасная разработка и новая поверхность атаки

Безопасная разработка становится сертифицируемой практикой. Cloud.ru сертифицировал процесс безопасной разработки по требованиям регулятора (Лобоцкий Михаил, Cloud.ru), Яндекс, по словам Служеникина, одним из первых прошёл сертификацию по ГОСТу. Максим Тятюшев (СберТех) сообщил, что группа по ИБ генеративной разработки (9 компаний и 19 экспертов) публикует базовые принципы из 13 пунктов, и просит учесть их в следующей версии ГОСТа о безопасном конвейере разработки. WB ID переходит от долгоживущих ключей подписи кода к короткоживущим и отзываемым (Венгер Олег, WB ID).

Импортозамещение создало новую поверхность атаки. Новиков отметил, что за год было много инцидентов с эксплуатацией уязвимостей нулевого дня российских вендоров. Николай Прянишников («Группа Астра») говорит о смещении атак на системный уровень –

ядро ОС и гипервизоры. Полина Давыдова (ассоциация «Цифровой транспорт и логистика») привела данные: доля зарубежных решений в кибербезопасности сократилась почти в 15 раз.

7.3 Международное измерение

Отдельная сессия была посвящена международному сотрудничеству. Ольга Мельникова (МИД России) сообщила, что Конвенцию ООН против киберпреступности поддержали 95 участников, ратифицировали 3 страны, для вступления в силу нужно 40 ратификаций. Минцифры предлагает партнёрам совместные киберучения и центры ИБ.

Алексей Дегтярев (Сбер) описал последствия массового отзыва сертификатов безопасности: российские компании около 2 месяцев находились под давлением. CA/Browser Forum, по его словам, объединяет более 70 удостоверяющих центров. Следующим шагом, по его прогнозу, может стать отзыв сертификатов подписи кода. Он предлагает кросс-сертификацию Национального УЦ с международным центром и удостоверяющий центр стран БРИКС. Антон Назаркин (Positive Technologies) указал на отсутствие у России инструментов поддержки экспорта ИТ, сравнимых с американскими, японскими и китайскими.

8. Биометрия и цифровая идентификация

8.1 Масштаб ЕБС и сервисов

Биометрия масштабируется и обсуждается одновременно как инструмент антифрода и как объект атак. Скворцова привела масштаб: в ЕБС 55 млн уникальных пользователей Госуслуг, накоплено 90 млн биометрических образцов. Проведено 400–450 млн транзакций, значительная часть – биоэквайринг. На базе ЕБС работают 53 сервиса в 30 сферах. Проезд в метро по биометрии используется 50 млн раз в год. В коммерческих биометрических системах хранится 100 млн векторов. Отрасль регулируют закон № 572 и более 50 подзаконных актов.

Владислав Поволоцкий (ЦБТ) сообщил, что через оплату лицом совершено более 400 млн транзакций при нулевом уровне мошенничества, дистанционно открыто около 400 тыс. счетов без случаев фрода. Он ожидает почти полного покрытия финансово активного населения в ближайшие 1–2 года. По его данным, 57% граждан доверяют биометрии или нейтральны, около 20% будут относиться отрицательно всегда. Скворцова связала снижение мошенничества на 32% в том числе с биометрией.

В транспорте внедрение идёт медленно. По данным Скворцовой, подготовка биометрического прохода в Пулково заняла около 5 лет, по биометрии совершено чуть более 1 700 посадок в Пулково и 850 в Шереметьево. Экспериментальный режим действует только в этих двух аэропортах. Минцифры готовит дорожные карты для ещё 10 аэропортов.

8.2 Атаки и дипфейки

Олег Евсеев (Сбер) сообщил о 0 успешных атак на оплату по биометрии при 27,5 млн транзакций. 80% атак на терминалы Сбера – попытка предъявить фото с экрана смартфона. Без дополнительного фактора оплата проходит только до 10 000 руб. Станислав Смышляев (КриптоПро) сказал, что за 10 лет развития ЕБС не было ни одного существенного инцидента, а при её создании за 3 года КриптоПро нашла уязвимости примерно в десятке зарубежных протоколов-кандидатов.

> Голос и письмо – это больше не доказательства. – Петр Хенкин, Сбер

Угрозы описывали конкретно. Дмитрий Марков (VisionLabs) напомнил, что раньше самой дорогой атакой была силиконовая маска примерно за 350 000 руб. Теперь в интернете доступно около 2 000 бесплатных инструментов создания дипфейков. Отдельный детектор, по его оценке, отражает от 90% до 95% атак, поэтому нужна комплексная защита устройства, канала и серверной части, а биометрия должна дополнять другие факторы. В тестировании новой модели 48% участников считали, что по видеосвязи общаются с живым человеком (Коваленко Дмитрий, МИЭМ). «Лаборатория Касперского» нашла 24 уязвимости в биометрическом терминале одного производителя (Лискин Александр, «Лаборатория Касперского»).

8.3 Спор о требованиях

Главная линия разногласий – уровень регуляторных требований. Лукацкий считает, что требования ФСБ к биометрии подняты «до космических высот», модель угроз сфокусирована на криптографии и закрывает рынок для большинства. Криптография, по его оценке, составляет от силы 10% вопросов безопасности. Он же сообщил, что в даркнете уже продаются записи в ЕБС. Смышляев возражает: требования нужно сначала задавать высокими и затем точечно снижать, повысить их потом невозможно. Евсеев признал, что стоимость криптозащиты, аттестации и сертификации осложняет экономику биометрических проектов.

Платформы указывают на пределы обязательной идентификации. Рыженков сообщил, что Авито через Госуслуги добровольно верифицировал более 3 млн пользователей, и верифицированные получают примерно на 20% больше заказов. Но около 40% граждан в опросе, который он привёл, ответили, что уйдут на другие площадки, если их обяжут верифицироваться. Он отметил и обратную проблему: платформа не может ограничить пользователя, отказавшегося от биометрической проверки, даже если аккаунт, вероятно, захвачен.

9. Киберустойчивость: реагирование и восстановление

9.1 Скорость реакции

Пленарная сессия о кибербезопасности сместила фокус с вопроса «взломают ли» на вопрос «что будет после». Новиков описал разрыв: пока ИТ-служба 3 дня блокирует учётную запись по тикету, хакеры успевают зашифровать инфраструктуру и украсть данные. После инцидента внимание бизнеса держится примерно до 10-го месяца. По его прогнозу, через полгода 90% российских компаний перестанут успевать реагировать на атаки. Он предлагает дать ИБ-службам право останавливать бизнес-процессы и провести учения: вытащить из ЦОДа 15 жёстких дисков и посмотреть на восстановление. «Хакеру достаточно одной оплошности для того, чтобы получить доступ внутрь компании», – напомнил Новиков.

> Вопрос не стоит так: взломают ли? Наверное, вопрос стоит так: когда это произойдёт и что вы будете после этого делать? – Павел Торопин, «Норникель»

9.2 Ошибки восстановления

Ошибки восстановления повторяются. Ляпунов говорит, что взломанные компании часто восстанавливаются внутри скомпрометированной инфраструктуры, и злоумышленник продолжает уничтожать бэкапы. Правильный путь – маленькая чистая зона, куда переносят данные и пересоздают системы с нуля. Кулашова привела пример жертв шифровальщиков, которые платят выкуп повторно через 2 месяца и ещё раз через месяц со скидкой. Андрей Зотов (Beeline Cloud) советует хранить копии отдельно от основной инфраструктуры и дополнять их учениями. По его словам, если восстановлением начали заниматься после инцидента, шансы на успех «абсолютно непредсказуемы». VK Tech встроила в продукт неудаляемые резервные копии, которые не может удалить даже администратор (Лазаренко Дмитрий, VK Tech).

9.3 Автоматизация защиты

Защитники тоже автоматизируются. В Yandex Cloud агентная система ускорила аудиты безопасности в 6 раз (Сидоров Евгений, Yandex Cloud). ИИ-агент Билайна проверяет устранение уязвимостей за 30 минут вместо недели работы пентестера (Волков Алексей, Билайн).

10. Bug bounty, киберстрахование и кадры

10.1 Bug bounty и белый хакинг

Государство расширяет практику вознаграждений за найденные уязвимости. Мишустин заявил, что вознаграждение за уязвимость на Госуслугах достигает 1 млн руб., и эту практику нужно расширять. Шойтов сообщил, что Минцифры около 5 лет проверяет

Госуслуги пентестами и через bug bounty, и уровень находимых уязвимостей снижается. Он предложил давать неидентифицированным исследователям фиксированный набор ИИ-агентов в изолированной среде, а ручную работу оставить идентифицированным. Баранов отметил, что 30% российских вендоров уже используют bug bounty и кибериспытания.

Спрос со стороны бизнеса остаётся низким. По словам Новикова, на бесплатное тестирование защищённости белыми хакерами соглашаются 2 из 30 руководителей, а некоторые вендоры отказываются давать решения на пилот, узнав, что их проверят на уязвимости.

10.2 Киберстрахование

Рынок страхования киберрисков, по оценке части участников, не сложился. Владимир Скворцов (АльфаСтрахование) представил страхование как элемент архитектуры защиты: полностью защититься невозможно. В кейсе регионального ритейлера шифровальщик перевёл магазины на бумагу, ущерб оценивается в 100 млн руб. при полисе дешевле 10 млн, лимит выплаты – 1 млрд руб. Он предлагает, чтобы рядом с дипломом директора по ИБ лежал полис киберстрахования. Оппоненты возражают: Александр Ковалевский (ИКС Безопасность) говорит, что доступного страхования киберрисков в России нет, а Абрамов – что ни одна страховая не готова застраховать деятельность ФНС.

10.3 Кадры

Кадровый дефицит назвали почти все. В 80% компаний нет даже нескольких специалистов по ИБ (Богомолов Егор, CyberED). Дмитрий Коваленко (МИЭМ) говорит, что хороших специалистов уже не хватает, их перекупают, а демографический спад сократит число выпускников. Малый бизнес, по словам Бочаровой, последний в очереди за кадрами. С этого года в «Код будущего» добавлено направление ИБ (Казанцева Анастасия, Минцифры России), а Кулашова предлагает вывести олимпиаду по кибербезопасности на государственный уровень.

> Нужно бежать быстрее последнего, кто бежит от медведя, а не быстрее самого медведя. – Егор Богомолов, CyberED

11. Барьеры и предложения

Большинство названных барьеров – организационные и регуляторные, а не технологические; спикеры адресовали предложения регуляторам, крупным заказчикам и самим службам ИБ.

Барьер	Кто называет	Что предлагают (адресат)
Добровольный обмен антифрод-данными не создаёт ответственности	Татьяна Скворцова, Минцифры России	Обязательное подключение к ГИС «Антифрод» с 1 марта 2027 года, подключаться заранее (банки, операторы, платформы)
Закон о платформенной экономике ограничивает превентивную блокировку	Михаил Рыженков, Левон Айрапетян, Авито	Точечно скорректировать регулирование для превентивного антифрода (Минэкономразвития, законодатели)
Мошенничество уходит в мессенджеры, операторы не видят данных	Григорий Кузнецов, Билайн	Онлайн-интеграция с мессенджерами; отложенные транзакции и подтверждение доверенными лицами в ГИС «Антифрод» (банки, участники ГИС)
Атака начинается через 40 минут после исправления	Денис Баранов, Алексей Новиков, Positive Technologies	Пересобрать продуктовые линейки и процессы устранения уязвимостей (вендоры, ИБ-службы)
Агент исполняет скрытые инструкции и действует за рамками задачи	Дмитрий Лазаренко, VK Tech; Анна Кулашова, «Лаборатория Касперского»	Отдельные идентичности, минимальные привилегии, отзыв прав, независимая проверка действий (компании, внедряющие агентов)
Теневой ИИ и вынос данных во внешние модели	Александр Лискин, «Лаборатория Касперского»; Антон Ефимов, ГК «Солар»	Видимость используемых инструментов, корпоративные нейрошлюзы вместо запретов (службы ИБ)
Атаки через подрядчиков с привилегированным доступом	Алексей Фетисов, Альфа-Банк; Андрей Устюжанин, ДОМ.РФ Технологии	Требования и ответственность в договоре, право на аудит и пентест (крупные заказчики)
Защита для МСП слишком дорога	Максим Никандров, iGrids	Помочь выполнить требования без разрушения экономики бизнеса (Правительство, Корпорация МСП); налоговые стимулы (Игорь Вербицкий, Яндекс 360)
У МСП нет компетенций и кадров ИБ	Алексей Новиков, Positive Technologies; Елена Бочарова, «Киберпротект»	Коробочные решения, самодиагностика, курс минимальной защиты (вендоры, Корпорация МСП, Минэкономразвития)
Владельцы систем не выполняют простейших мер, ИБ догоняет ИТ	Александр Шойтов, Минцифры России	Security by design, ИБ-службам – право останавливать процессы (руководители компаний)

Барьер	Кто называет	Что предлагают (адресат)
Все объекты транспорта отнесены к КИИ, данные об атаках идут вручную	Борис Ташимов, Александр Кисляков, Минтранс России	Сузить фокус до критичных объектов; единый стандарт автопередачи данных об инцидентах (Минтранс, ФСТЭК, транспортные компании)
Требования к биометрии избыточны и закрывают рынок	Алексей Лукацкий, Positive Technologies	Не сводить регулирование к криптографии (ФСБ, ФСТЭК)
Отзыв сертификатов и непризнание национального УЦ	Алексей Дегтярев, Сбер; Олег Венгер, WB ID	Кросс-сертификация Национального УЦ, УЦ стран БРИКС (Минцифры, страны БРИКС)
Несовершеннолетних вовлекают в дропперство	Анна Кулашова, «Лаборатория Касперского»; Елена Муллануровa, «Аргументы и факты»	Рассказывать о живых примерах (медиа); обязательный предмет по ИБ в школах (Елена Орлова, Wildberries)

12. Ключевые игроки темы

Повестку направления задавали регуляторы, вендоры средств защиты, платформы, операторы связи и банки.

- **Минцифры России** – Татьяна Скворцова, Александр Шойтов, Сергей Сергиенко. Архитектура ГИС «Антифрод» и ЕБС, позиция регулятора по исполнению требований и агентам; около 40 участников ГИС, 55 млн пользователей ЕБС.
- **Positive Technologies** – Денис Баранов, Алексей Новиков, Алексей Лукацкий, Ирина Зиновкина. Тезис о 40 минутах от исправления до атаки, атаки через цепочки поставок, критика требований к биометрии.
- **«Лаборатория Касперского»** – Анна Кулашова, Александр Лискин, Юлия Шлычкова. Кибериммунитет, практики контроля ИИ-агентов, угрозы для МСП и детей; 24 уязвимости в биометрическом терминале.
- **ГК «Солар»** – Игорь Ляпунов, Антон Ефимов. Защита госсистем на выборах (более 4 000 попыток атак без успеха), JSOC One с компенсацией ущерба до 30 млн руб.
- **Авито** – Иван Гуз, Михаил Рыженков, Наталья Юматова. Сокращение злоупотреблений в 125 раз, 22 млрд руб. инвестиций в безопасность за 6 лет, спор о превентивной блокировке.
- **Ozon** – Александр Васильев, Анна Павлова. Первым из посреднических платформ подключился к ГИС «Антифрод»; 98% случаев решаются автоматически.
- **Билайн** – Сергей Анохин, Григорий Кузнецов, Алексей Волков, Андрей Зотов (Beeline Cloud). 870 млн пресечённых звонков, «киберсемья», восстановление после атак.

- **Сбер** – Олег Евсеев, Петр Хенкин, Алексей Дегтярев. Ноль успешных атак на биометрическую оплату, суверенные удостоверяющие центры.
- **VK Tech** – Дмитрий Лазаренко. Агенты как субъекты доступа, неудаляемые резервные копии, прогноз о защите агентов агентами.
- **НТЦ ЦК** – Игорь Качалин, Дмитрий Служеникин. Отечественная криптография, подпись кода (более 80 участников рабочей группы), изменения ГОСТа и приказа № 117.
- **Минтранс России** – Борис Ташимов, Александр Кисляков. Около 5 млн атак на РЖД, донастройка КИИ на транспорте.
- **ЦСР и Корпорация МСП** – Екатерина Кваша, Алексей Охрименко. Исследование киберустойчивости МСП: 82% сталкивались с инцидентами, 17% используют комплексную защиту.
- **АльфаСтрахование** – Владимир Скворцов. Киберстрахование как элемент архитектуры защиты, лимит 1 млрд руб. в кейсе ритейлера.

Выводы

- **Антифрод стал государственной инфраструктурой.** К ГИС «Антифрод» подключено около 40 участников, с 1 марта 2027 года подключение станет обязательным, а ответственность распределяется между банками, операторами связи и платформами (Скворцова Татьяна, Минцифры России).
- **Статистика мошенничества снижается, но схемы меняют канал.** МВД фиксирует снижение на 29% за 8 месяцев (Капранов Олег, РОЦИТ) и на 32% к прошлому году (Скворцова Татьяна, Минцифры России); при этом фишинг возвращается в мессенджеры в виде многоуровневых схем (Кабрера Максим, Билайн).
- **Главная цель атак – человек.** Социальная инженерия даёт более 60% успешных атак на организации и около 99% – на частных лиц (Зиновкина Ирина, Positive Technologies); число несовершеннолетних, совершивших киберпреступления, за 8 месяцев выросло на 28% (Мулланурова Елена, «Аргументы и факты»).
- **ИИ сжал время на защиту до минут.** Атака может начаться через 40 минут после выхода исправления (Баранов Денис, Positive Technologies), а сложную атаку проводит один человек с роем агентов (Серебрянников Дмитрий, белый хакер). Принципиально новых техник ИИ пока не дал – он ускоряет известные (Шойтов Александр, Минцифры России).
- **ИИ-агент рассматривается как новый тип нарушителя.** Агента можно «уговорить» скрытой в письме инструкцией (Лазаренко Дмитрий, VK Tech), у одного заказчика закупщики без ведома ИБ запустили 30 агентов (Ефимов Антон, ГК «Солар»). ГОСТ по безопасной разработке и приказ ФСТЭК № 117 дополнят требованиями к ИИ (Служеникин Дмитрий, НТЦ ЦК).
- **Слабое звено – подрядчик и малый бизнес.** 82% МСП сталкивались с киберинцидентами (Кваша Екатерина, Центр стратегических разработок), комплексную защиту используют 17% (Охрименко Алексей, Корпорация МСП), а вход в систему

защиты для технологической компании обошёлся в 10–12 млн (Никандров Максим, iGrids).

- **Биометрия масштабируется, спор идёт о требованиях, кадров не хватает.** В ЕБС 55 млн пользователей и 90 млн образцов (Скворцова Татьяна, Минцифры России); требования к биометрии критикуют как избыточные (Лукацкий Алексей, Positive Technologies). В 80% компаний нет даже нескольких специалистов по ИБ (Богомолов Егор, CyberED).

Источники

- Сессия «Главная пленарная сессия „Результаты. Возможности. Перспективы“», Форум «Цифровые решения – 2026»
- Сессия «ИИ-агенты под контролем: как управлять рисками и строить доверенную инфраструктуру», Форум «Цифровые решения – 2026»
- Сессия «Регулирование ИИ: поиск баланса между развитием технологий и защитой интересов граждан», Форум «Цифровые решения – 2026»
- Сессия «Защита малого и среднего бизнеса от атакующего ИИ», Форум «Цифровые решения – 2026»
- Сессия «Управление данными: до и после ИИ-Агентов», Форум «Цифровые решения – 2026»
- Сессия «Пленарная сессия. Государство как цифровой сервис: где остановиться?», Форум «Цифровые решения – 2026»
- Сессия «Государственные данные для цифровых платформ», Форум «Цифровые решения – 2026»
- Сессия «Доступ разрешен: повышение эффективности ИИ-агентной экономики и новые стандарты ПО», Форум «Цифровые решения – 2026»
- Сессия «Конференция билайн. Дискуссионное шоу. Красная зона ИИ: технология готова – готовы ли мы?», Форум «Цифровые решения – 2026»
- Сессия «Конференция билайн. Облака в эпоху ИИ-атак: выжить, выстоять и восстановиться», Форум «Цифровые решения – 2026»
- Сессия «Новый контур платформенной экономики: от вступления закона в силу к практике», Форум «Цифровые решения – 2026»
- Сессия «От цифровой идентификации к цифровому доверию. Как государству и бизнесу выстроить единый контур», Форум «Цифровые решения – 2026»
- Сессия «Маршрут построен: „дорожная карта“ цифровизации пассажирского транспорта в России», Форум «Цифровые решения – 2026»
- Сессия «Суверенный ИИ: сколько независимости нужно заказчику», Форум «Цифровые решения – 2026»
- Сессия «Инновации нон стоп: как внедрять технологии на непрерывном производстве», Форум «Цифровые решения – 2026»

- Сессия «Пленарная сессия. Кибербезопасность сегодня: когда защита перестает быть надстройкой», Форум «Цифровые решения – 2026»
- Сессия «Как не допустить новую волну кибермошенничества?», Форум «Цифровые решения – 2026»
- Сессия «Кибербезопасность в эпоху платформенной экономики», Форум «Цифровые решения – 2026»
- Сессия «Международное сотрудничество в сфере информационной безопасности: форматы и практические механизмы взаимодействия», Форум «Цифровые решения – 2026»
- Сессия «На шаг впереди: переход от реагирования к предупреждению угроз», Форум «Цифровые решения – 2026»
- Сессия «Брак по расчету или союз по любви: образование, индустрия и технологии», Форум «Цифровые решения – 2026»
- Сессия «Доверие и безопасность в цифровой торговле: технологии, стандарты и защита участников рынка», Форум «Цифровые решения – 2026»
- Сессия «Периметр больше не спасает: почему фокус отрасли смещается в сторону защиты данных», Форум «Цифровые решения – 2026»
- Сессия «Профессия специалиста по информационной безопасности: содержание, навыки и карьерные перспективы до 2030 года», Форум «Цифровые решения – 2026»
- Сессия «Безопасная разработка и подпись кода: от теории к широкому применению», Форум «Цифровые решения – 2026»
- Сессия «Доверенная генеративная разработка: единые правила для отрасли», Форум «Цифровые решения – 2026»
- Сессия «Институт белого хакинга как составляющая стратегической киберустойчивости государства и бизнеса», Форум «Цифровые решения – 2026»
- Сессия «Когда код управляет движением: кибербезопасность современного транспорта», Форум «Цифровые решения – 2026»
- Сессия «Развитие системы противодействия киберпреступлениям: меры, координация и измеримые эффекты», Форум «Цифровые решения – 2026»
- Сессия «Безопасность ИИ-моделей: угрозы, методы защиты и подходы к регулированию», Форум «Цифровые решения – 2026»
- Сессия «Кибербезопасность и биометрия: в поисках идеального баланса», Форум «Цифровые решения – 2026»
- Сессия «Кадры для технологического суверенитета», Форум «Цифровые решения – 2026»