

Гоар
Еприкян

ЦИФРОВОЙ ДВОЙНИК

Стр. 10

который спасает жизни

ТОП гаджетов

Стр. 17

для тех, кто живёт
технологиями

ФУТБОЛ 2026

Стр. 4

и высокие технологии

ЧЕГО МЫ ДОСТИГЛИ?

Стр. 60

Свидетели рождения
новой эпохи

ТЕХНОЛОГИИ

4 Футбол 2026: синергия спорта и высоких технологий

Как искусственный интеллект, «умный» мяч, цифровые двойники футболистов и системы кибербезопасности меняют футбол

10 Цифровой двойник, который может спасти жизнь человека

Есть старая медицинская истина: хороший врач лечит болезнь, великий – не допускает её появления. На протяжении тысячелетий эта мысль оставалась скорее идеалом, чем реальностью. Врачи учились всё точнее распознавать симптомы, совершенствовали методы лечения, создавали новые лекарства и хирургические технологии. Но почти всегда они начинали действовать уже после того, как болезнь успевала заявить о себе.

ГАДЖЕТЫ

17 ТОП гаджетов с AliExpress для тех, кто живёт технологиями

Ещё несколько лет назад AliExpress ассоциировался в основном с недорогими аксессуарами для смартфонов и компьютеров. Сегодня это одна из крупнейших площадок, где разработчики, инженеры, системные администраторы и другие специалисты ИТ-сферы находят не только полезные инструменты для работы, но и устройства, способные вдохновить на новые проекты и эксперименты.

АНАЛИТИКА

20 Утечки данных в организациях РФ в 2025 году

Структура реальных инцидентов, восприятие киберугроз и эффективность защитных мер

29 Какая технология сделает вас успешнее в ближайшие 5 лет

32 Стоимость интернета в мире

Средняя ежемесячная стоимость фиксированного широкополосного доступа в интернет в 2026 году.

34 Как люди используют ИИ на работе

35 10 самых распространённых способов, которыми хакеры похищают криптовалюту

Большинство потерь криптовалюты связано не со взломом кошельков, а с уязвимостями в программном коде и инфраструктуре.

36 Атаки на веб-приложения российских компаний

В первом полугодии 2026 года атаки на веб-приложения российских компаний стали более массовыми, автоматизированными и точечными. Злоумышленники все чаще стремятся не просто нарушить доступность сервиса, а получить доступ к данным, учётным записям и критичным бизнес-процессам через уязвимости приложений и API.

ПРАВО

40 Правовое регулирование искусственного интеллекта в России

В настоящей статье расскажем о том, что такое большие фундаментальные модели (БФМ) и как они соотносятся с ИИ, какие виды таких моделей существуют, а также о том, при каких условиях их разработчики могут заручиться мерами государственной поддержки.

СОБЫТИЯ

42 CISO Форум 2026

Итоги главной клубной встречи лидеров информационной безопасности

46 Системные программисты России беспокоятся о профильном образовании

Круглый стол «Преподавание системного программирования в вузах страны. Проблемы и решения», состоявшийся в рамках XIII Научно-практической конференции OS DAY 2026 в РЭУ им. Плеханова в июне, стал площадкой для откровенного разговора экспертов российской ИТ-отрасли и преподавателей вузов о состоянии отечественной системы высшего образования.

49 Главные итоги ЦИПР-2026

Более 13 тысяч участников, 350 подписаний, полсотни стран

ОПЫТ

52 Смартфон – это уже не телефон. Это ключ от вашей цифровой жизни

60 Когда однажды нас спросят, чего достигло наше поколение

История обладает удивительной особенностью: она почти никогда не предупреждает современников о том, что именно в этот момент они становятся свидетелями рождения новой эпохи.

РЕШЕНИЯ

64 Невидимые технологии: почему будущее цифровых платежей зависит не только от банков

КОМИКСЫ

68 Флешка с «сюрпризом» и любопытная Бринти

ИТ-ГОРОСКОП

70 Осенний бизнес-гороскоп – 2026 для ИТ-компаний

КРОССВОРД

75 Сканворд

От редактора

Дорогие читатели!

Этот выпуск посвящён технологиям, которые всё глубже входят в нашу жизнь и меняют представление о возможностях человека. На страницах журнала мы говорим о цифровой безопасности, искусственном интеллекте, медицине будущего, современном спорте и полезных устройствах.

Смартфон сегодня – это ключ к банковским приложениям, документам, переписке и личным аккаунтам. В материале о мобильной безопасности рассказываем о современных угрозах и настройках iPhone и Android, которые помогают сохранить контроль над своей цифровой жизнью.

Статья об искусственном интеллекте предлагает задуматься, что история однажды назовёт главным достижением нашего поколения. Возможно, именно нам выпало превратить мечту о мыслящей машине в повседневную реальность – и одновременно заново определить роль и ответственность человека.

Материал о цифровых двойниках показывает, как математические модели органов уже помогают планировать операции, сравнивать способы лечения и оценивать риски. Разбираемся, смогут ли такие технологии в будущем предупреждать заболевания до появления первых симптомов.

«Умный» мяч, VAR нового поколения, цифровые двойники игроков, ИИ-аналитика и кибербезопасность меняют чемпионат мира по футболу 2026 года, но главным героем спорта по-прежнему остаётся человек.

Для любителей практических экспериментов мы подготовили подборку интересных гаджетов с AliExpress – от цифровых микроскопов до программируемых мини-компьютеров и тестеров кабелей.

Читайте, исследуйте и открывайте вместе с нами цифровой мир, в котором технологии расширяют человеческие знания и возможности.

С уважением,
редакция журнала CIS

Главный редактор: Станислав Понарин.
Директор по маркетингу: Валерия Рябина.
Дизайн и вёрстка: Алексей Дмитриев.
Корректор: Оксана Макаренко.
Отдел рекламы и распространения: magazine@sovinfosystems.ru.
Сайт: www.cis.ru.
Регистрация журнала: федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.
Номер свидетельства: ПИ № ФС 77-69584.
Дата регистрации: 02.05.2017.
Наименование СМИ: Современные Информационные Системы.
Форма распространения: печатное СМИ, журнал.
Территория распространения: Российская Федерация.
Адрес редакции: 108811, г. Москва, вн. тер. г. поселение Московский, Киевское шоссе 22-й км. (п. Московский), домовладение 4, строение 2, помещение 68Н/2.
Язык: русский.
Периодичность: 4 раза в год (1 раз в квартал).

За содержание рекламного объявления ответственность несёт рекламодатель. Перепечатка, использование или перевод на другой язык, а так же иное использование произведений, равно как их включение в состав другого произведения (сборник, как часть другого произведения, использование в какой-либо форме в электронной публикации) без согласия издателя запрещены.

Предоставляя (бесплатные) текстовые и иллюстративные материалы для их публикации в данном издании общества с ограниченной ответственностью «Современные инфосистемы» отправитель даёт своё согласие на использование присланных им материалов путём их распространения через любые виды электронных (цифровых) каналов, включая интернет, мобильные приложения, смартфоны и т.д.

Фото на обложке: Гоар Еприкян.

Тираж 5000 экз. (отпечатанный тираж).

Журнал предназначен для лиц старше 16 лет.

© 2026, CIS (Современные Информационные Системы).

Футбол 2026: синергия спорта и высоких технологий

Как искусственный интеллект,
«умный» мяч, цифровые
двойники футболистов
и системы кибербезопасности
меняют футбол



Как технологии изменили большой футбол

Когда-то для проведения футбольного матча были нужны поле, ворота, мяч, две команды и судья со свистком. Современному чемпионату мира требуется инфраструктура, по сложности сопоставимая с крупной технологической корпорацией. За привычной телевизионной картинкой работают высокоскоростные камеры, оптоволоконные сети, центры обработки данных, системы компьютерного зрения, мобильные приложения, генеративный ИИ и специалисты по кибербезопасности.

Чемпионат мира по футболу 2026 года проходит сразу в трёх странах – США, Канаде и Мексике. В нём участвуют 48 сборных, а программа включает 104 матча в 16 городах. Необходимо синхронно управлять стадионами, тренировочными базами, отелями, транспортом, билетами, аккредитациями, телетрансляциями и цифровыми сервисами. Одновременно организаторы должны защищать всю эту инфраструктуру от технических сбоев, кибератак, мошенников и физических угроз.

При таком масштабе футбольный матч становится лишь видимой частью огромного цифрового механизма. Данные собираются практически непрерывно: камеры следят за футболистами и мячом, датчики фикси-

руют касания, алгоритмы создают трёхмерную копию происходящего, а аналитические платформы превращают миллионы разрозненных значений в понятные выводы.

Технологии меняют и саму природу спортивной конкуренции. Раньше тренерские штабы во многом полагались на собственный опыт, видеозаписи и наблюдения нескольких аналитиков. Теперь команда может получить цифровую модель соперника, определить повторяющиеся схемы атак, найти зоны свободного пространства и сопоставить статистику с конкретными видеозаписями. Побеждает не тот, у кого больше данных, а тот, кто быстрее превращает их в правильные решения.

При этом технология не забывает голы и не выходит на поле вместо футболиста. Она помогает заметить то, что человеческий глаз может пропустить. Она сокращает путь от наблюдения до вывода, делает судейство точнее, лечение безопаснее, а просмотр матча – доступнее. Чемпионат мира 2026 года показывает, что современный футбол окончательно превратился в союз человеческого таланта и сложнейших информационных систем. Некоторые из этих многочисленных технологических новшеств мы рассмотрим в этой статье.

Мяч, который фиксирует 500 измерений в секунду



Официальный мяч чемпионата мира получил название TRIONDA. На первый взгляд это обычный футбольный мяч с необычным дизайном. Но внутри него находится инерциальный датчик, который работает с частотой 500 Гц. Это означает, что система может получать до 500 измерений движения в секунду.

Датчик фиксирует ускорение, вращение и мельчайшие изменения положения мяча. Главное его предназначение – с высокой точностью определить момент касания. Для полуавтоматической системы опреде-

ления офсайда это критически важно. Даже несколько кадров разницы способны изменить решение, если нападающий и защитник одновременно движутся в противоположных направлениях.

«Умный» мяч помогает установить, когда именно был сделан пас, произошло ли едва заметное касание и изменил ли футболист траекторию мяча. Эти данные передаются в систему VAR – это **Video Assistant Referee** (видеоассистент судьи) и сопоставляются с изображением камер. В результате судьи получают не только видеозапись, но и независимый цифровой источник информации.

Однако мяч не принимает окончательное решение. Датчик не назначает пенальти и не отменяет гол. Он предоставляет измерения, которые помогают арбитрам точнее восстановить картину произошедшего. Последнее слово по-прежнему остаётся за человеком.

Особенностью TRIONDA стала и новая четырёхпанельная конструкция. Глубина швов и геометрия поверхности рассчитаны так, чтобы сделать полёт устойчивее, а сцепление – предсказуемее при разной влажности. Получается, что перед нами одновременно спортивный снаряд, аэродинамическая конструкция и подключённое устройство интернета вещей.

Спорный эпизод



Обычная видеозапись ограничена расположением реальных камер. Если нужный момент оказался закрыт телом футболиста или стойкой ворот, оператор не может перенести камеру в прошлое и выбрать другой ракурс. Но это может сделать трёхмерная реконструкция.

Система объединяет изображения стадионных камер, координаты игроков, данные оптического трекинга и информацию от подключённого мяча. На их основе в реальном времени создаётся виртуальная модель происходящего. После этого эпизод можно рассматривать практически из любой точки.

VAR получает возможность увидеть ситуацию с позиции, в которой физической камеры не было, например: из-за спины защитника, с линии ворот или непосредственно позади голкипера. Особенно полезны такие ракурсы при проверке того, закрывал ли игрок обзор вратарю, касался ли он мяча и полностью ли мяч покинул пределы поля.

Трёхмерная реконструкция не заменяет оригинальную запись. Она является вычисленной моделью, а значит, должна использоваться вместе с другими источниками. Но, когда данные нескольких камер и датчиков совпадают, виртуальный ракурс способен показать пространственные отношения значительно нагляднее обычного повтора.

Футбольная трансляция постепенно перестаёт быть простым набором видеок кадров. Теперь это цифровая сцена, которую можно заново собрать, остановить, повернуть и рассмотреть изнутри.

VAR нового поколения: больше, чем видеоповтор



За аббревиатурой VAR скрывается сложная распределённая система. На чемпи-

онате мира 2026 года в Международном вещательном центре работают шесть централизованных помещений видеопомощи арбитрам. Туда поступают телевизионные ракурсы, записи специальных камер, координаты игроков, сигналы «умного» мяча и трёхмерные реконструкции.

Задача заключается не только в том, чтобы показать судье повтор. Сначала необходимо определить, какой именно эпизод следует проверить, синхронизировать данные из разных источников, выбрать подходящие ракурсы и убедиться, что речь идёт об одном и том же моменте.

В полуавтоматической системе определения офсайда камеры отслеживают положение частей тела игроков, а датчик в мяче уточняет время передачи. Алгоритм формирует предварительное уведомление, после чего специалисты VAR проверяют построение линий и правильность выбранных футболистов. Только затем информация передаётся главному арбитру.

Такой подход помогает быстрее разбирать очевидные эпизоды, но сохраняет человеческий контроль там, где требуется интерпретация правил. Машина способна измерить положение стопы с высокой точностью, но оценка умышленной игры рукой, опасности контакта или степени влияния на соперника всё ещё требует судейского решения.

VAR нового поколения – это пример системы поддержки принятия решений, а не автоматического судьи. Чем больше источников данных она объединяет, тем важнее становится понятный порядок проверки и ответственность людей, принимающих окончательное решение.

Цифровые двойники футболистов



Перед чемпионатом были отсканированы все 1 248 заявленных футболистов 48 сборных. Процедура занимала около секунды, но позволяла получить подробные размеры частей тела каждого игрока. На основе этих данных создавались персональные трёхмерные аватары.

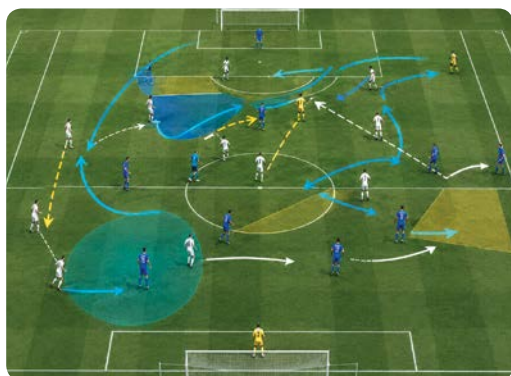
Это не просто красивые модели для телевизионной графики. Цифровой двойник помогает системе компьютерного зрения точнее распознавать плечи, голову, колени, стопы и другие части тела футболиста. Такая информация особенно важна при определении офсайда, когда одного игрока частично закрывает другой или несколько футболистов находятся почти на одной линии.

Раньше в телевизионной анимации спорного эпизода зритель видел условные компьютерные фигуры. Теперь система может показывать узнаваемые цифровые копии реальных участников матча. Положение тела, форма и внешние особенности футболиста делают реконструкцию понятнее.

Технология также снижает вероятность ошибки при идентификации игроков. На поле одновременно могут находиться несколько футболистов одного роста, в одинаковой форме и с похожей комплекцией. Персональная 3D-модель предоставляет алгоритму дополнительный набор признаков.

Цифровые двойники становятся связующим звеном между физическим матчем и его виртуальной копией. В будущем подобные модели могут использоваться значительно шире: для анализа техники движений, восстановления после травм, персонализированных тренировок и создания спортивных трансляций в виртуальной реальности.

ИИ-аналитик для каждой сборной



FIFA AI Pro – один из главных технологических экспериментов чемпионата. Это генеративный ИИ-помощник, предназначенный для тренеров и аналитиков всех участвующих сборных. Он работает с официальной статистикой FIFA, данными перемещений, видеозаписями и трёхмерными моделями матчей.

Система позволяет обращаться к сложной базе данных обычным языком. Аналитик может попросить показать атаки определённой команды через левый фланг, найти эпизоды высокого прессинга или сравнить

действия соперника до и после замены. В ответ ИИ формирует текстовые объяснения, графики, подборки видео и тактические наблюдения.

Главное значение FIFA AI Pro заключается не только в скорости. У богатых сборных давно существуют большие аналитические отделы, способные самостоятельно разрабатывать программное обеспечение и обрабатывать огромные массивы информации. У команд с меньшими бюджетами таких возможностей может не быть. Предоставляя один инструмент всем 48 сборным, FIFA в определённой степени выравнивает доступ к технологиям.

По данным организации, команды обращались к системе на 15 языках. Это особенно важно для международного турнира: специалист может формулировать запросы без необходимости переводить футбольные термины или осваивать сложный язык программирования.

ИИ не придумывает победную тактику по нажатию кнопки. Он помогает быстрее найти закономерность, но оценить её значение должны тренеры. Один и тот же показатель может быть признаком как силы, так и уязвимости команды. Поэтому ценность аналитика будущего определяется не количеством доступных графиков, а умением задавать правильные вопросы.

Как ИИ разбирает завершившийся матч



После финального свистка работа аналитических систем только начинается. FIFA AI Pro может автоматически сформировать постматчевый отчёт, описать основные тенденции, выделить повторяющиеся действия и связать статистические показатели с конкретными видеоэпизодами.

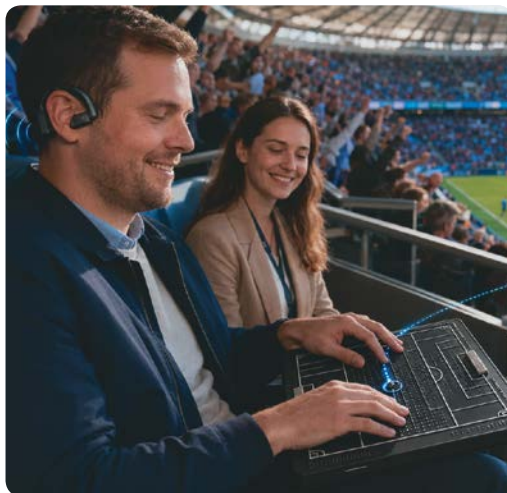
Вместо нескольких часов ручного просмотра специалисты получают первоначальную картину значительно быстрее. Если команда регулярно теряла мяч под определённым типом прессинга, система найдёт такие моменты и соберёт их в одну последовательность. Если защитник слишком

часто покидал свою зону, ИИ сопоставит его перемещения с возникшими опасными атаками.

Но система имеет принципиальное ограничение: она не используется для подсказок тренерам во время игры. Это сохраняет баланс между технологической аналитикой и непосредственным управлением командой. ИИ может помочь подготовиться к следующему матчу или разобрать завершившийся, но не подсказывает решение в режиме реального времени со скамейки.

В этом смысле технология напоминает очень быстрого помощника, способного просмотреть тысячи событий и подготовить материалы к совещанию. Решение о том, что менять в тренировках и тактике, остаётся за тренерским штабом.

Технологии для незрячих болельщиков



На отдельных матчах в Далласе, Нью-Йорке и Нью-Джерси, Сиэтле и Ванкувере используются тактильные футбольные планшеты. Устройство напоминает небольшую рельефную модель поля, на которой незрячий или слабовидящий болельщик может ощущать перемещение мяча в реальном времени.

Информация о матче преобразуется в тактильные сигналы. Пользователь понимает, в какой зоне находится мяч, в каком направлении развивается атака и насколько близко действие переместилось к воротам. Так статистические координаты, обычно предназначенные для аналитических платформ, превращаются в новый способ восприятия футбола.

Тактильный планшет особенно эффективен в сочетании с аудиодескрипцией. Один канал передаёт пространственное положение, другой описывает движения, эмоции и атмосферу. Болельщику больше не приходится постоянно спрашивать сопровождающего, что произошло на поле.

Это показательный пример того, как технологическая доступность перестаёт быть дополнительной услугой. Те же данные, которые используются для VAR и анализа матча, могут сделать футбол доступным людям, прежде почти исключённым из полноценного стадионного опыта.

Круговой обзор на 360



Guardian-iiS – мобильная система видеонаблюдения, обеспечивающая круговой обзор на 360 градусов без слепых зон. Комплекс можно сравнительно быстро развернуть возле стадиона или другого объекта, где необходимо временно усилить наблюдение.

Встроенная аналитика помогает операторам замечать необычную активность и контролировать обстановку вокруг арены. При этом ИИ не должен самостоятельно объявлять человека нарушителем. Его задача – выделить потенциально значимое событие и привлечь к нему внимание специалиста.

Преимущество Guardian-iiS заключается в мобильности. Чемпионат проводится в разных городах, а потоки людей меняются в зависимости от расписания матчей и мероприятий. Переносная система позволяет создавать дополнительный контур наблюдения там, где он необходим именно сегодня.

Видеоповтор спасает здоровье игроков



Система Tactical and Medical Replay предоставляет тренерским и медицинским штабам доступ к эпизодам с разных камер.

Если футболист получил удар по голове, неудачно приземлился или столкнулся с соперником, врач может быстро пересмотреть момент и оценить механизм травмы.

Игрок после жёсткого контакта не всегда способен точно описать произошедшее. Адреналин, шум стадиона и желание продолжить матч могут повлиять на его субъективную оценку. Видеозапись позволяет увидеть силу удара, положение головы и характер падения.

Особенно важна такая технология при подозрении на сотрясение мозга. Врач получает дополнительную информацию и может принять более обоснованное решение о необходимости обследования или замены. Повтор не ставит диагноз, но помогает не пропустить потенциально опасный эпизод.

Тренерский штаб использует ту же систему для тактического анализа. Таким образом, один массив видеоданных одновременно служит судьям, врачам и аналитикам, но каждый специалист рассматривает его с собственной точки зрения.

Миллиард отражённых киберугроз



За красивой цифровой оболочкой находится огромная поверхность для атак. Сайты, приложения, системы аккредитации, трансляции, отели, билетные платформы, транспортные сервисы и стадионные сети связаны множеством цифровых каналов.

По данным FIFA, к стадии четвертьфиналов системы безопасности нейтрализовали более одного миллиарда киберугроз. Организация не раскрывает их точную классификацию и архитектуру защиты, что вполне объяснимо: подробное описание оборо-

нительных механизмов могло бы помочь злоумышленникам.

Важно понимать, что миллиард угроз – не обязательно миллиард целенаправленных попыток взломать чемпионат. В подобную статистику могут входить автоматические сканирования, вредоносные запросы, боты, попытки подбора паролей, подозрительный трафик и другие события. Но даже с этой оговоркой показатель демонстрирует масштаб цифрового периметра.

Киберзащита чемпионата должна работать непрерывно. Во время решающего матча невозможно остановить вещательную сеть на несколько часов для обновления или длительного расследования. Системы обязаны обнаруживать угрозу, изолировать её и сохранять работу критически важных сервисов.

Когда футбол стал вычислительной системой

Главные технологические прорывы чемпионата мира 2026 года – это не отдельные эффектные устройства, а их объединение. FIFA AI Pro работает с официальными данными матчей. Персональные аватары помогают системе распознавать игроков. «Умный» мяч уточняет момент касания. Камеры создают координатную модель поля. Трёхмерная реконструкция позволяет увидеть эпизод с виртуального ракурса. VAR соединяет эти сведения, а человек принимает окончательное решение.

Та же взаимосвязанность характерна для инфраструктуры всего турнира. Цифровые идентификаторы, приложения, вещательные сети, системы доступности, видеонаблюдение и киберзащита образуют единый технологический организм. Отказ одного элемента может повлиять на многие другие, поэтому надёжность становится не менее важной, чем функциональность.

Футбол при этом не превращается в соревнование компьютеров. На поле по-прежнему решают скорость, характер, техника, физическая готовность и способность выдерживать давление. Но за пределами поля технологии помогают командам лучше понимать собственную игру и быстрее изучать соперника. Они не создают таланты, но позволяют использовать его точнее.

Чемпионат мира 2026 года показывает будущее большого спорта: человек остаётся главным героем, однако вокруг него уже действует сложнейшая цифровая система. Она видит больше человеческого глаза, запоминает каждый эпизод, сопоставляет миллионы событий и продолжает работать даже тогда, когда стадион пустеет после финального свистка.



Цифровой двойник,
который может спасти
жизнь человека

Есть старая медицинская истина: хороший врач лечит болезнь, великий – не допускает её появления. На протяжении тысячелетий эта мысль оставалась скорее идеалом, чем реальностью. Врачи учились всё точнее распознавать симптомы, совершенствовали методы лечения, создавали новые лекарства и хирургические технологии. Но почти всегда они начинали действовать уже после того, как болезнь успевала заявить о себе.

Даже самые современные методы диагностики долгое время оставались своеобразными фотографиями человеческого организма. Компьютерная томография, магнитно-резонансная томография, ультразвуковые исследования, лабораторные анализы – всё это позволяет чрезвычайно подробно изучить состояние пациента, но лишь в конкретный момент времени. Эти технологии прекрасно отвечают на вопрос, что происходит сейчас. Однако на вопрос, что произойдёт через год, пять или десять лет, медицина чаще всего могла отвечать лишь с определённой долей вероятности, опираясь на статистику, накопленный опыт и клинические наблюдения.

Сегодня эта ситуация начинает меняться не благодаря очередному лекарству, не из-за появления более совершенного томографа и даже не потому, что ИИ научился быстрее анализировать медицинские изображения – причина гораздо глубже. Впервые за всю историю медицины появляется возможность построить математическую модель конкретного человека и наблюдать за тем, как она изменяется вместе со своим реальным прототипом.

Ещё недавно подобная идея звучала как научная фантастика. Можно ли создать виртуальную копию человеческого сердца, проверить на ней несколько вариантов операции и только после этого пригласить пациента в операционную? Можно ли заранее увидеть, как организм отреагирует на новое лекарство? Способна ли компьютерная

модель предупредить врача о заболевании ещё до появления первых симптомов?

Сегодня подобные вопросы уже не кажутся фантастическими. Над ними работают ведущие университеты, исследовательские центры, разработчики медицинского программного обеспечения и производители высокотехнологичного оборудования. За сравнительно короткое время математическое моделирование человеческого организма прошло путь от лабораторных экспериментов до технологии, которая постепенно начинает входить в клиническую практику.

При этом речь идёт вовсе не о попытке заменить врача алгоритмом. Скорее, медицина получает новый инструмент – столь же революционный, каким когда-то стали рентгенография, компьютерная томография или магнитно-резонансная диагностика. Но если прежние технологии позволяли увидеть организм изнутри, то цифровые модели делают следующий шаг. Они помогают понять, как этот организм будет меняться под воздействием времени, лечения, образа жизни и окружающей среды.

Для специалистов в области информационных технологий эта история представляет особый интерес. Она родилась не благодаря одному великому открытию. Это пример того, как несколько независимых направлений науки неожиданно сошлись в одной точке. Высокопроизводительные вычисления, ИИ, инженерное моделирование, медицинская визуализация, облачные платформы и анализ больших данных долгие годы развивались параллельно. Лишь теперь стало очевидно, что вместе они способны изменить не только одну отрасль, но и само представление о современной медицине.

Всё чаще исследователи говорят, что XXI век станет эпохой персонализированной медицины. Однако за этим определением скрывается гораздо больше, чем подбор лекарств с учётом индивидуальных особенностей пациента. Речь идёт о принципиально новом подходе, при котором медицина постепенно переходит от наблюдения за болезнью к моделированию здоровья.

Если эта идея оправдывает ожидания исследователей, историки науки, возможно, однажды поставят

цифровые модели человека в один ряд с самыми значительными технологическими достижениями нашего времени.

Именно здесь начинается история, которая ещё далека от завершения. Она развивается сейчас – в исследовательских лабораториях, университетах, инженерных центрах и клиниках. И вполне возможно, что именно она определит, какой станет медицина уже в ближайшие десятилетия.

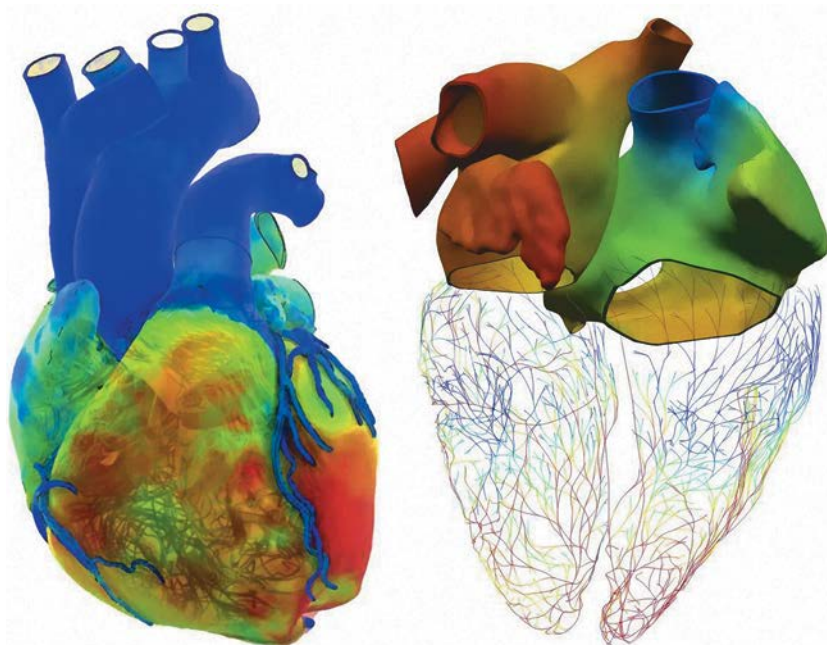
Когда медицина перестала довольствоваться снимками

История медицины во многом похожа на историю фотографии. Каждое новое поколение диагностических приборов позволяло увидеть человеческий организм всё подробнее. Сначала появился стетоскоп, подаривший врачам возможность слышать работу сердца и лёгких. Затем рентгеновские лучи впервые позволили заглянуть внутрь человека без хирургического вмешательства. Позже появились компьютерная и магнитно-резонансная томография, трёхмерная эхокардиография, молекулярная диагностика и десятки других технологий. Каждая из них открывала новое окно в мир, который прежде оставался скрытым.

Но при всём техническом совершенстве эти методы объединяло одно важное ограничение: они показывали организм только в момент исследования.

Даже самые детальные изображения оставались своеобразными фотографиями. Иногда сделанными с интервалом в несколько месяцев, иногда – в несколько лет. Между этими снимками проходила настоящая жизнь. Сердце продолжало сокращаться, сосуды постепенно менялись, клетки старели, иммунная система реагировала на инфекции, ткани восстанавливались после нагрузок. Большинство этих процессов происходило незаметно, пока однажды не превращалось в заболевание. Именно здесь медицина подошла к своему естественному пределу.

Человеческий организм невозможно понять окончательно, изучив его один раз. Это не неподвижный объект, а непрерывно изменяющаяся система, в которой каждую секунду происходят миллиарды взаимосвязанных процессов. Одни длятся доли секунды, другие – годы. Чтобы



Виртуальные двойники оживляют модели, объединяя взаимосвязанные системы одного органа. Здесь электрические импульсы распространяются по сети волокон, вызывая сердцебиение [справа] и напряжение мышечной ткани во время сокращений [слева].

действительно понимать происходящее, недостаточно время от времени делать новые снимки. Нужно научиться видеть сам процесс изменений.

Идея математического моделирования возникла задолго до того, как появились технологии, способные её реализовать. Инженеры давно привыкли строить виртуальные модели сложных объектов. До первого полёта самолёта рассчитывается его поведение в воздухе. До появления нового автомобиля анализируется прочность кузова и работа систем безопасности. Архитекторы заранее проверяют устойчивость будущих зданий к ветровым нагрузкам и землетрясениям. Компьютер позволяет многократно проигрывать различные сценарии, находить ошибки ещё на этапе проектирования и только потом переходить к созданию реального объекта. С человеком всё оказалось значительно сложнее.

Самолёт создаётся по чертежам. Организм развивается самостоятельно и непрерывно меняется на протяжении всей жизни. Автомобиль собирается из деталей с заранее известными характеристиками. Биологические ткани постоянно обновляются, реагируют на окружающую среду и никогда не ведут себя абсолютно одинаково.

Именно поэтому первые математические модели человеческого организма были очень скромными. Одни исследовательские группы рассчитывали кровотоки в крупных сосудах. Другие изучали механику сердечной мышцы. Третьи моделировали распространение электрических импульсов. Каждая работа помогала лучше понять отдельный процесс, но объединить их в единую систему долгое время не удавалось. Перелом произошёл постепенно.

Вычислительные мощности выросли на порядки. Алгоритмы стали точнее. Медицинские изображения – значительно детальнее. ИИ научился автоматически выделять анатомические структуры там, где раньше требовались часы ручной работы. Сначала каждое из этих достижений выглядело как очередной шаг вперёд. Позже стало ясно, что все они складываются в одну общую картину.

Впервые появилась возможность моделировать не отдельный орган, а конкретного человека с его собственной анатомией, физиологией и результатами обследований. Именно тогда в научной литературе всё чаще стало появляться понятие «цифровой двойник».

При этом сам термин нередко понимают неправильно. Многие представляют цифровой двойник как красивую

трёхмерную модель, которую можно вращать на экране компьютера. На самом деле визуализация – лишь внешняя оболочка технологии. Настоящая ценность скрыта гораздо глубже.

Цифровой двойник – это не изображение организма, а математическая модель его поведения. Она позволяет не просто показать сердце, сосуды или лёгкие, а рассчитать, как они будут работать после операции, как изменится кровоток при установке импланта, каким окажется влияние нового метода лечения спустя месяцы или годы. Компьютер перестаёт быть хранилищем медицинских данных и становится инструментом, который помогает исследовать развитие биологических процессов.

Именно здесь проходит граница между традиционной диагностикой и новой медициной. Современные методы обследования показывают врачу настоящее. Цифровое моделирование позволяет осторожно заглянуть в будущее не для того чтобы предсказать судьбу человека, а чтобы заранее сравнить несколько возможных сценариев и выбрать тот, который с наибольшей вероятностью окажется самым безопасным.

Эта идея и превратила цифровые двойники из инженерного эксперимента в одно из самых перспективных направлений современной медицины. Но прежде чем подобные модели начали использоваться в клиниках, исследователям предстояло решить задачу, которую ещё недавно считали почти невыполнимой. Нужно было создать виртуальный орган, поведение которого действительно совпадало бы с поведением его биологического прототипа. Таким органом стало человеческое сердце.

Цифровое сердце, которое впервые забилося

Если попросить инженера назвать самый сложный механизм, созданный природой, многие без колебаний ответят: человеческое сердце. На первый взгляд это утверждение кажется неожиданным. Современная техника знает объекты, состоящие из миллионов деталей: пассажирские авиалайнеры, атомные электростанции, космические аппараты. Однако сердце отличается от любого инженерного сооружения одной принципиальной особенностью. Оно не просто работает.

Оно непрерывно изменяется, мгновенно реагируя на любое состояние организма.

Достаточно подняться по лестнице, чтобы сердце увеличило частоту сокращений. Сильное волнение меняет ритм, давление и скорость кровотока. Во сне сердечно-сосудистая система работает совсем иначе, чем во время физической нагрузки, а даже обычное изменение положения тела заставляет её за считанные секунды перестроить свою работу. Все эти процессы происходят одновременно, непрерывно влияя друг на друга. Именно поэтому сердце долгие годы оставалось одной из самых сложных задач для математического моделирования.

Создать его цифровую модель означало значительно больше, чем построить точную трёхмерную копию органа. Исследователям необходимо было описать сразу несколько взаимосвязанных процессов: движение крови через камеры сердца, работу клапанов, сокращение сердечной мышцы, распространение электрических импульсов и влияние каждого из этих процессов на остальные. Любая неточность в одном элементе приводила к тому, что вся модель начинала вести себя иначе, чем настоящее сердце.

Поэтому первые исследования были весьма ограниченными. Одни научные группы занимались исключительно моделированием кровотока, другие – исследовали механику сердечной мышцы, третьи – сосредоточились на распространении электрических сигналов. Каждая такая работа помогала глубже понять отдельный процесс, однако объединить их в единую модель долгое время не удавалось. Главным препятствием оказалась не нехватка медицинских знаний, а вычислительные возможности.

Каждое сокращение сердца представляет собой чрезвычайно сложную последовательность физических процессов, происходящих одновременно. Чтобы воспроизвести всего несколько секунд его работы с высокой точностью, компьютеру приходится выполнять огромное количество вычислений. Ещё двадцать лет назад подобные расчёты занимали слишком много времени, чтобы использовать их в реальной клинической практике. Поэтому идея создания полноценной цифровой модели

сердца существовала значительно раньше, чем появились технологии, способные воплотить её в жизнь.

Ситуация начала меняться лишь тогда, когда сразу несколько направлений науки достигли необходимого уровня зрелости. Производительность вычислительных систем выросла на порядки, медицинская визуализация стала значительно точнее, методы численного моделирования приблизились к инженерной надёжности, а алгоритмы ИИ научились автоматически обрабатывать медицинские изображения, на подготовку которых раньше уходили многие часы ручной работы. По отдельности каждое из этих достижений выглядело как очередной шаг вперёд. Вместе они создали условия для появления технологии, которая ещё недавно казалась практически недостижимой.

Именно в этот период был запущен международный проект **Living Heart Project** – один из самых известных проектов в области цифрового моделирования сердца. Его участники поставили перед собой задачу, которая ещё несколькими годами ранее выглядела почти фантастической: создать математическую модель, способную воспроизводить не только анатомическое строение сердца, но и особенности его работы. Это принципиальное различие.

Трёхмерная модель отвечает на вопрос: **как выглядит сердце**. Цифровой двойник пытается ответить совсем на другой вопрос: **как оно будет работать при изменении условий**.

Как изменится кровоток после операции? Как поведёт себя новый сердечный клапан спустя несколько лет? Какая нагрузка возникнет на ткани после установки импланта? Как изменится работа сердца после перенесённого инфаркта? Ответить на подобные вопросы исключительно на основании медицинских изображений невозможно. Однако математическая модель позволяет воспроизвести различные сценарии и оценить их последствия ещё до того, как врач войдёт в операционную.

Важно понимать, что цифровой двойник не принимает решения вместо врача и не ставит диагноз. Его задача значительно скромнее и одновременно гораздо важнее. Он позволяет заранее сравнить несколько возможных вариантов лечения, увидеть

сильные и слабые стороны каждого из них и тем самым сделать будущую операцию более обоснованной.

Такой подход давно стал привычным для инженеров. Перед первым полётом нового самолёта конструкторы проводят тысячи виртуальных испытаний. Перед строительством моста моделируются ветровые нагрузки, температурные деформации и десятки аварийных сценариев. Реальные испытания при этом никто не отменяет, однако компьютер помогает заранее обнаружить ошибки, которые впоследствии могли бы обойтись слишком дорого. Медицина только начинает проходить этот путь. Разница заключается лишь в том, что объектом моделирования становится не самолёт и не промышленная установка, а живой человек.

Именно поэтому значение **Living Heart Project** оказалось значительно шире первоначальной задачи. Проект не просто позволил создать одну из самых совершенных моделей сердца – он доказал сам принцип. Если исследователям удалось достаточно точно воспроизвести работу одного из самых сложных органов человеческого организма, значит, подобный подход потенциально можно распространить и на другие системы организма.

Сегодня этот вопрос уже не относится к области научной фантастики: над ним работают исследовательские центры во всём мире. И хотя до создания полноценной цифровой модели всего организма ещё далеко, главный вывод уже сделан: человечество впервые показало, что сердце можно не только наблюдать и лечить, но и моделировать.

Именно с этого момента цифровые двойники перестали быть исключительно научным экспериментом. Они стали новой областью медицины, развитие которой только начинается.

От диагноза к прогнозу

На протяжении почти всей истории медицины врачи решали одну и ту же задачу – объясняли то, что уже произошло. Пациент приходил с жалобами, результаты анализов показывали отклонения, а диагностические исследования подтверждали изменения в организме. После этого начинался поиск причины и выбор наиболее эффективного лечения. Каждое новое поколение медицинского оборудования позволяло

обнаруживать заболевание всё раньше, однако сама логика оставалась неизменной: сначала происходили изменения, и лишь затем медицина получала возможность их увидеть. Сегодня этот принцип постепенно начинает меняться.

Представим человека, который чувствует себя совершенно здоровым. Он проходит ежегодное обследование, получает хорошие результаты анализов и спокойно возвращается к привычной жизни. Однако внутри организма уже могут происходить процессы, которые пока не видны ни самому человеку, ни врачу. Где-то медленно снижается эластичность сосудистой стенки, постепенно изменяется структура сердечной мышцы, незаметно развивается воспалительная реакция. Пока эти изменения не выходят за пределы физиологической нормы, они остаются практически неуловимыми. Болезнь словно существует в полумраке: она уже начала своё развитие, но ещё не стала событием, которое можно уверенно диагностировать.

Именно поэтому исследователи всё чаще говорят, что главная ценность цифровых двойников заключается вовсе не в построении красивой трёхмерной модели органов. Настоящий прорыв состоит в другом – в возможности превратить медицинские данные в инструмент прогнозирования.

На первый взгляд идея кажется очевидной. Современная медицина уже располагает огромным объёмом информации о каждом пациенте, но проблема заключается не в ней, а в её стремительном росте.

Каждый новый метод исследования создаёт собственный массив данных, который существует отдельно от остальных. Томограф хранит изображения, лаборатория – результаты анализов, кардиограф – электрическую активность сердца, фитнес-браслет – сведения о пульсе, сне и физической активности. По отдельности эти данные чрезвычайно ценны, однако объединить их в единую картину долгое время было чрезвычайно сложно.

Именно здесь медицина встретилась с технологиями больших данных и ИИ. Они помогают обнаруживать взаимосвязи, которые невозможно удержать в поле зрения человека. Кардиолог спосо-

бен проанализировать результаты обследования, оценить строение сердца, состояние клапанов, особенности кровотока и лабораторные показатели. Алгоритм делает то же самое, но одновременно сопоставляет тысячи параметров, сравнивает результаты обследования разных лет, учитывает возраст пациента, особенности анатомии, сопутствующие заболевания и информацию, поступающую от носимых устройств, не потому что понимает медицину лучше врача, а потому, что способен работать с объёмом данных, который давно превысил возможности человеческой памяти и внимания.

Благодаря этому изменилась и сама технология создания цифровых моделей организма. Если ещё недавно построение персональной модели требовало недель кропотливой ручной работы, то сегодня интеллектуальные алгоритмы автоматически выделяют анатомические структуры, формируют геометрию органов и подготавливают данные для последующего моделирования.

Но главным достижением стала даже не скорость вычислений. Настоящий прорыв произошёл тогда, когда цифровая модель перестала быть статичным объектом. Теперь она может развиваться вместе со своим владельцем. Каждое новое обследование, каждый анализ и каждая запись электрокардиограммы становятся частью единой цифровой истории организма. Модель непрерывно уточняется, постепенно превращаясь во всё более точное отражение реальных процессов, происходящих внутри человека.

Именно в этот момент медицина впервые получает возможность задать вопрос, который ещё совсем недавно казался слишком смелым: не «что происходит с пациентом сейчас», а «что, вероятнее всего, произойдёт дальше». Разумеется, ни одна математическая модель не способна предсказывать будущее абсолютно точно. Человеческий организм слишком сложен, чтобы описать его безошибочно. Но между полной неопределённостью и точным прогнозом существует огромная область вероятностей. Именно здесь и начинают работать цифровые двойники. Они не заменяют врача и не принимают решения вместо него. Они позволяют заранее оценить несколько воз-

можных сценариев развития событий и понять, какой из них наиболее вероятен.

В этом и заключается главное отличие новой медицины от той, к которой мы привыкли. Если эта концепция полностью оправдана ожиданиями исследователей, главным её результатом станет изменение самой философии здравоохранения. Болезнь всё чаще будет восприниматься не как неожиданное событие, а как процесс, первые признаки которого удалось заметить задолго до появления симптомов.

Миллионы пациентов, которых никогда не было

Путь любого нового лекарства или медицинского устройства начинается задолго до того, как им воспользуется первый пациент. Обычно этот путь занимает многие годы. За это время исследователи создают десятки экспериментальных образцов, проводят тысячи лабораторных испытаний, анализируют огромные массивы данных и лишь затем переходят к клиническим исследованиям с участием добровольцев. Это один из самых сложных, продолжительных и дорогостоящих процессов современной науки.

При этом даже многолетняя работа не гарантирует успеха. Перспективный препарат может оказаться недостаточно эффективным, неожиданно проявить серьёзные побочные эффекты или не подтвердить ожидаемые результаты на завершающих этапах исследований. Похожая ситуация возникает и при разработке медицинских устройств. Имплант, успешно прошедший лабораторные испытания, иногда ведёт себя иначе в организме человека, чем предполагали инженеры. Каждая подобная ошибка означает потерю времени, огромных финансовых ресурсов и, что гораздо важнее, отсрочку появления новых методов лечения для пациентов, которые продолжают ждать.

Неудивительно, что учёные давно пытались найти способ заранее проверить как можно больше возможных сценариев, не подвергая людей лишнему риску. Именно здесь цифровые двойники начинают свою работу.

Представим лабораторию недалёкого будущего. Инженеры завершают разработку нового сердечного

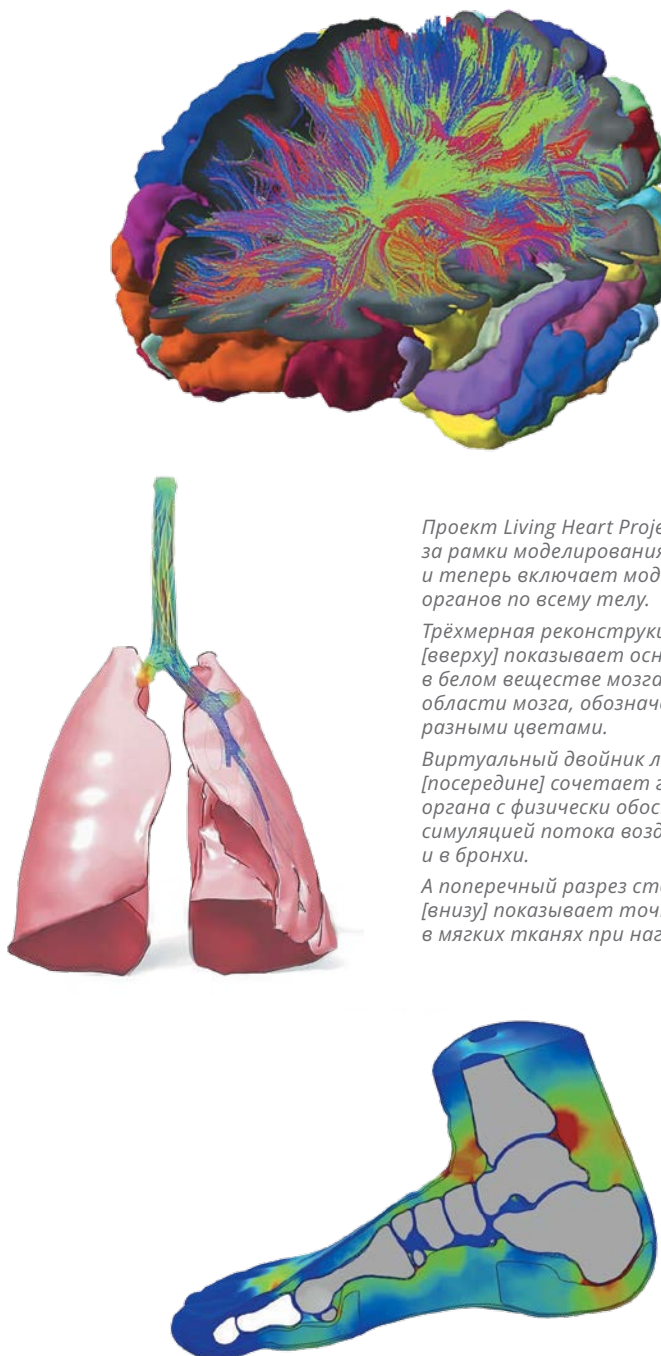
клапана. Ещё несколько лет назад следующим этапом стало бы изготовление опытного образца и длительная серия испытаний. Теперь работа начинается иначе. Сначала этот клапан устанавливают не реальному пациенту, а тысячам его виртуальных моделей.

Каждая из них отличается от остальных. Одна воспроизводит сердце молодого человека, другая – пожилого пациента, третья – учитывает последствия перенесённого инфаркта, четвёртая – моделирует врождённый порок развития, пятая – особенности строения сосудов конкретного человека. Компьютер последовательно просчитывает десятки тысяч сочетаний условий, анализирует изменение кровотока, распределение механических нагрузок и вероятность осложнений. Благодаря этому инженеры ещё до изготовления серийного образца получают возможность увидеть слабые места конструкции и устранить их задолго до встречи устройства с первым пациентом.

Аналогичные изменения постепенно происходят и в фармацевтике. Современные лекарственные препараты редко действуют одинаково на всех пациентов. Организм каждого человека обладает собственными особенностями обмена веществ, иммунного ответа, работы печени, почек и сердечно-сосудистой системы. Именно поэтому один и тот же препарат способен демонстрировать различную эффективность даже у людей с одинаковым диагнозом.

До недавнего времени подобные различия выявлялись главным образом во время клинических исследований. Теперь появляется возможность анализировать многие из них значительно раньше. Цифровые модели позволяют оценивать потенциальное поведение различных групп пациентов, сравнивать эффективность нескольких вариантов терапии и заранее искать факторы, способные повлиять на безопасность будущего лечения. Это не заменяет реальных испытаний, но помогает сделать их значительно более осмысленными.

Фактически медицина начинает использовать тот же подход, который давно стал привычным в инженерном мире – сначала испытания, потом использование.



Проект Living Heart Project вышел за рамки моделирования сердца и теперь включает моделирование органов по всему телу.

Трёхмерная реконструкция мозга [вверху] показывает основные пути в белом веществе мозга, соединяющие области мозга, обозначенные разными цветами.

Виртуальный двойник легких [посередине] сочетает геометрию органа с физически обоснованной симуляцией потока воздуха по трахее и в бронхи.

А поперечный разрез стопы пациента [внизу] показывает точки напряжения в мягких тканях при нагрузке.

При этом самое интересное заключается вовсе не в сокращении сроков разработки новых технологий. Каждый созданный цифровой двойник становится частью общего опыта. Каждая виртуальная операция, каждое моделирование кровотока, каждый расчёт делают последующие модели точнее. В отличие от большинства медицинских инструментов цифровые двойники способны постоянно совершенствоваться, накапливая новые знания вместе с развитием науки.

Именно поэтому всё больше специалистов рассматривают их не как отдельную технологию, а как основу будущей цифровой инфраструктуры

здравоохранения. Она будет объединять результаты исследований, клинический опыт, математические модели и ИИ в единую систему, которая со временем станет таким же привычным инструментом врача, как сегодня электронная медицинская карта или медицинская визуализация.

Но самый интересный вопрос возникает уже после этого. Что произойдёт, если цифровой двойник начнут создавать не тогда, когда человек заболел, а значительно раньше? Если математическая модель станет сопровождать его на протяжении всей жизни, постоянно уточняясь после каждого обследования, анализа и сигнала, поступающего от носимых устройств?

Именно здесь история цифровых двойников выходит далеко за пределы разработки новых лекарств и медицинской техники. Она становится разговором о будущем всей медицины.

Когда цифровая модель начинает жить вместе с человеком

Практически каждая технология проходит один и тот же путь. Сначала она кажется слишком сложной, дорогой и предназначенной лишь для узкого круга специалистов. Затем становится профессиональным инструментом. А спустя годы настолько прочно входит в повседневную жизнь, что люди перестают замечать её существование. Сегодня трудно представить, что ещё тридцать лет назад мобильный телефон считался роскошью, электронная почта – технической экзотикой, а спутниковая навигация использовалась преимущественно военными. Постепенно все эти технологии стали настолько привычными, что мы вспоминаем о них лишь тогда, когда они перестают работать. Похожий путь, вероятно, предстоит пройти и цифровым двойникам.

Пока математические модели организма создаются главным образом для решения сложных клинических задач. Они помогают планировать операции, исследовать работу сердца, разрабатывать медицинские устройства и оценивать различные варианты лечения. Однако всё чаще исследователи задают вопрос, который ещё недавно казался преждевременным: почему цифровая модель человека должна появляться только тогда, когда он уже заболел? Ведь история здоровья начинается задолго до первого диагноза.

Каждый человек постепенно оставляет за собой своеобразный цифровой след. Результаты диспансеризации, лабораторные анализы, томография, электрокардиография, данные стоматологических обследований, сведения о перенесённых заболеваниях – всё это уже хранится в электронном виде. К ним добавляются данные домашних тонометров, глюкометров, фитнес-браслетов и умных часов, которые фиксируют сердечный ритм, уровень физической активности, качество сна, насыщение крови кислородом и множество других параметров. По отдельности эти

сведения кажутся обычными медицинскими записями. Вместе они начинают рассказывать историю жизни организма.

Именно здесь возникает идея, что если все эти данные не просто хранить в электронной медицинской карте, а использовать для постоянного уточнения математической модели конкретного человека?

Важно понимать: речь идёт вовсе не о создании «второго человека» внутри компьютера. У цифровой модели нет сознания, памяти или собственной личности. Она не принимает решения и не существует отдельно от своего владельца. Это сложный математический инструмент, который непрерывно уточняется по мере поступления новой информации и помогает врачу лучше понимать процессы, происходящие в организме.

Именно поэтому многие специалисты всё чаще сравнивают цифрового двойника не с виртуальной копией человека, а с медицинской картой нового поколения. Разница между ними принципиальна. Традиционная история болезни рассказывает о прошлом: какие диагнозы были поставлены, какие операции проведены, какие лекарства назначались. Цифровая модель использует те же сведения иначе. Она помогает понять настоящее и оценить наиболее вероятные варианты будущего.

Такое изменение постепенно меняет и роль самого пациента. На протяжении веков медицина строилась вокруг болезни. Человек обращался к врачу, когда появлялась боль, ухудшалось самочувствие или обследование выявляло серьёзные отклонения. Новая модель предполагает иной подход. В центре внимания оказывается не болезнь, а здоровье. Чем раньше удастся заметить неблагоприятную тенденцию, тем выше вероятность остановить её ещё до появления первых симптомов.

Однако вместе с новыми возможностями возникают и новые вопросы.

Если математическая модель знает о человеке практически всё: особенности строения его сердца, результаты анализов, образ жизни, привычки, качество сна и уровень физической активности – кто должен владеть этой информацией? Где она будет храниться? Как защитить

её от утечек и кибератак? Кто сможет использовать такие данные в научных исследованиях? Как убедиться, что алгоритм не допустил ошибку при анализе столь чувствительной информации?

Эти вопросы уже невозможно считать второстепенными. По мере развития цифровой медицины они становятся столь же важными, как совершенствование самих вычислительных моделей. Именно поэтому рядом с врачами, инженерами и специалистами по ИИ всё чаще работают эксперты по ИБ, криптографии, цифровому праву и защите персональных данных. Будущее цифровых двойников зависит не только от развития вычислительных технологий, но и от того, насколько надёжно общество сумеет защитить самую личную информацию, которой обладает человек, – сведения о собственном здоровье.

История технологий уже не раз проходила через подобные этапы. С распространением Интернета появились новые правила хранения и передачи данных. Развитие электронных платежей потребовало создания современных систем защиты финансовой информации. Сегодня похожие процессы начинают происходить и в медицине. Только теперь предметом защиты становятся уже не банковские счета и документы, а цифровое описание самого человека.

Именно поэтому цифровые двойники следует рассматривать значительно шире, чем очередную медицинскую разработку. На наших глазах формируется новая экосистема, в которой медицина объединяется с прикладной математикой, программной инженерией, ИИ, высокопроизводительными вычислениями и информационной безопасностью. Возможно, именно такое сотрудничество различных отраслей станет одной из главных особенностей медицины XXI века.

И если этот путь окажется успешным, то мы перестанем воспринимать его как технологическое чудо и будем относиться к нему так же естественно, как сегодня относимся к компьютерной томографии или ультразвуковой диагностике.

Пожалуй, именно тогда изменится не только медицина – изменится само представление человека о собственном здоровье.

ТОП гаджетов с AliExpress для тех, кто живёт технологиями



Ещё несколько лет назад AliExpress ассоциировался в основном с недорогими аксессуарами для смартфонов и компьютеров.

Сегодня это одна из крупнейших площадок, где разработчики, инженеры, системные администраторы и другие специалисты ИТ-сферы находят не только полезные инструменты для работы, но и устройства, способные вдохновить на новые проекты и эксперименты.

Многие из этих гаджетов помогают автоматизировать повседневные задачи, ускорить диагностику оборудования, организовать рабочее место или собрать собственную домашнюю лабораторию без серьёзных затрат.

Мы выбрали самые интересные устройства, которые наверняка понравятся программистам, электронщикам, специалистам по информационной безопасности, техноблогерам и всем, кто искренне увлечён современными технологиями.



Цифровой USB-микроскоп

Незаменимая вещь для пайки, ремонта электроники и изучения мелких деталей. С его помощью можно рассмотреть дорожки на плате, качество пайки, маркировку микросхем, повреждения разъемов и микротрещины. Для инженера это рабочий инструмент, для техноблогера – способ делать красивые крупные планы, а для любителя электроники – новый уровень контроля над своими проектами.



USB Data Blocker

Маленький, но очень важный аксессуар для людей, которые думают о цифровой безопасности. Он вставляется между кабелем и USB-портом и физически блокирует передачу данных, оставляя только зарядку. Это полезно в аэропортах, гостиницах, конференц-залах и любых общественных местах, где приходится пользоваться чужими USB-портами. Для специалиста по информационной безопасности такой переходник – почти символ здоровой паранойи.



USB-логический анализатор

Один из самых недооценённых инструментов начинающего инженера. Он помогает понять, что происходит между микроконтроллером и периферией: как идут данные по UART, SPI, I2C и другим цифровым интерфейсам. Когда устройство «почти работает», но датчик не отвечает, дисплей показывает «мусор», а прошивка ведёт себя странно, логический анализатор часто быстрее всего выводит разработчика на причину проблемы.



Meshtastic LoRa-модуль

Meshtastic-модули на базе LoRa интересны тем, что позволяют строить автономные текстовые сети без сотовой связи и интернета. Такие устройства используют энтузиасты радиосвязи, туристы, инженеры, участники экспедиций и просто люди, которым интересно изучать альтернативные способы передачи данных. Для технологического сообщества это хороший пример того, как открытое ПО, доступное железо и радиосвязь превращаются в самостоятельную инфраструктуру.





M5Stack Cardputer

Один из самых необычных мини-компьютеров последних лет. Внешне он напоминает маленький карманный терминал с экраном и клавиатурой, но внутри скрывается полноценная платформа для экспериментов на базе ESP32. Устройство рассчитано на разработчиков, инженеров и энтузиастов IoT: на нём можно писать собственные утилиты, делать прототипы, тестировать Wi-Fi- и Bluetooth-проекты, создавать мини-приложения и обучающие демонстрации. Производитель описывает Cardputer как компактную программируемую платформу для прототипирования и IoT-разработки, а версия Cardputer-Adv получила ESP32-S3, экран 1,14 дюйма и клавиатуру на 56 клавиш.



FNIRSI FNB58 USB-C Tester

Вещь, которая быстро становится обязательной в рюкзаке любого техногика. Он подключается между зарядным устройством и смартфоном, ноутбуком, пауэрбанком или другим гаджетом и показывает напряжение, силу тока, мощность, протокол быстрой зарядки и другие параметры. Это особенно полезно, когда нужно понять, почему ноутбук заряжается не на полной мощности, действительно ли кабель поддерживает Power Delivery или не обманывает ли производитель зарядного устройства. FNIRSI указывает, что FNB58 оснащён цветным TFT-дисплеем, USB-A, Micro-USB и Type-C интерфейсами, а также аппаратной поддержкой анализа PD-протоколов.



USB-C кабель-тестер

USB-C кабели давно стали слишком сложными, чтобы оценивать их «на глаз». Один кабель поддерживает только зарядку, другой – передаёт данные, третий – умеет Power Delivery, четвёртый – подходит для монитора, а пятый – выглядит дорого, но работает как самый простой провод. Кабель-тестер позволяет проверить распиновку, наличие e-marker чипа, поддержку быстрой зарядки и качество соединения. Это полезно для сервисных инженеров, техноблогеров и всех, у кого дома уже накопилась коробка одинаковых на вид, но совершенно разных кабелей.



Dockcase Smart NVMe SSD Enclosure

Обычный внешний корпус для SSD – это просто коробка с разъёмом. Dockcase Smart NVMe SSD Enclosure выглядит куда интереснее: у него есть дисплей, на котором отображается состояние накопителя, температура, подключение и параметры работы. Для системного администратора, инженера техподдержки или человека, который часто переносит большие объёмы данных, такой корпус удобнее стандартного бокса. Dockcase заявляет поддержку M. 2 NVMe SSD форматов 2230, 2242, 2260 и 2280, скорость до 10 Гбит/с и защиту от потери питания на несколько секунд.



Утечки данных в организациях РФ в 2025 году

Структура реальных инцидентов, восприятие киберугроз
и эффективность защитных мер



Цель исследования

Настоящее исследование проведено компанией «Астерит» с целью выявления реальной картины утечек данных в российских организациях по итогам 2025 года, а также оценки разрыва между воспринимаемыми угрозами и фактическими мерами защиты, предпринимаемыми бизнесом. Дополнительным фокусом анализа стало исследование практических барьеров, препятствующих выстраиванию надёжной защиты, и оценка реального спроса на технологии ИИ как инструмента замещения роли специалиста ИБ в системах кибербезопасности.

1. Самый опасный способ кибератаки

Согласно опросу, респонденты исследования самые опасными способами кибератак считают методы, эксплуатирующие человеческий фактор. Руководители и специалисты ИТ и ИБ воспринимают наиболее критичным сценарием не сложный технический эксплойт, а хорошо спланированную комбинацию из этих трёх векторов, часто с последующим использованием вредоносного ПО или целевой атаки (рис. 1).

Зависимость от размера ИТ-инфраструктуры

С ростом размера организации акценты у опрашиваемых смещаются. Напротив, в небольших организациях доминирует фокус на массовых векторах, таких как вредоносные программы (до 45%) и DDoS-атаках (почти до 30% опрошенных).

Отраслевые закономерности

В финансовом и банковском секторах наряду с социальной инженерией (48% и 57% опрошенных соответственно) и фишингом (43% и 55%) высоко оценивают опасность от APT-атаки (43% и 52%). В ритейле и медийных компаниях социальная инженерия набирает до 80%, а в строительстве и на транспорте на первый план по опасности выходит фишинг (47% и 70%).

2. Киберинциденты: что реально происходит в инфраструктурах российских организаций

Киберинциденты, с которыми организации уже столкнулись, лучше всего демонстрируют реальный уровень угроз и эффективность действующей системы защиты. Такой срез позволяет сопоставить ожидания и реаль-

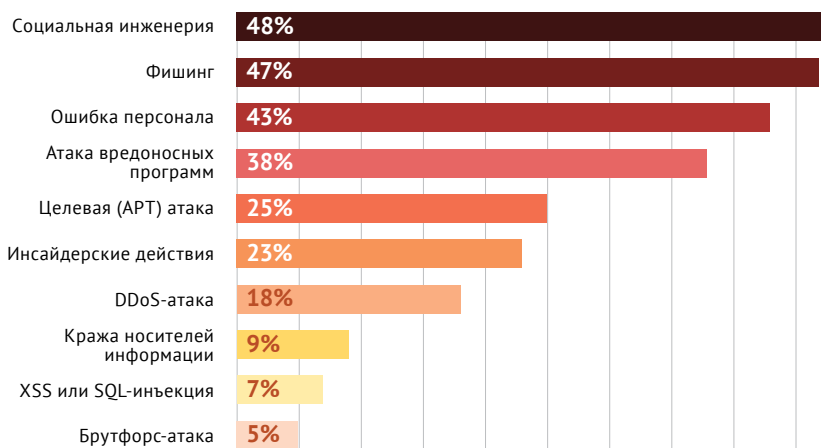


Рис. 1. Рейтинг способов кибератак по уровню воспринимаемой опасности.

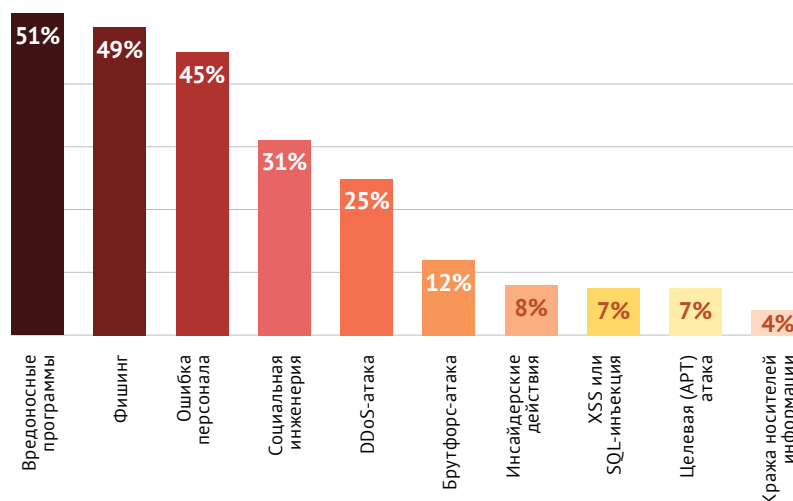


Рис. 2. Рейтинг наиболее распространённых ИБ-инцидентов в инфраструктурах организаций РФ.

ность: какие сценарии действительно материализуются в инциденты, а какие пока остаются в зоне теоретических рисков.

Анализ полученных ответов показывает, какие типы инцидентов стали для респондентов «рутинной» частью операционной деятельности, а какие по-прежнему остаются редкими, но потенциально критичными эпизодами. В итоге статистика инцидентов превращается в практический ориентир, по которому можно судить о реальной эффективности архитектуры безопасности и управлении человеческим фактором (рис. 2).

Согласно ответам респондентов, наиболее часто в профессиональной деятельности организации сталкивались с инцидентами, связанными с атакой вредоносных программ

(51%), фишингом (49%) и ошибками персонала (45%). При этом целевые APT-атаки, XSS/SQL-инъекции, инсайдерские действия, брутфорс-атаки и кража носителей информации встречаются заметно реже (от 4% до 12%), оставаясь скорее «точечными» сценариями по сравнению с массовыми заражениями и почтовыми атаками.

Фактически картина инцидентов подтверждает ранее выявленную доминанту человеческого фактора и почтовых каналов: большинство реально произошедших событий так или иначе связано с действиями пользователей (запуск вредоносного ПО, переход по фишинговой ссылке, ошибка при работе с данными). Относительно низкая доля зафиксированных APT, инсайдерских инцидентов и атак на веб-приложения может объясняться как их меньшей

частотой, так и ограниченной видимостью: отсутствие развитых средств мониторинга и расследования приводит к тому, что часть сложных атак остаётся за пределами отчётной статистики.

Зависимость от размера ИТ-инфраструктуры

При анализе в разрезе размера ИТ-инфраструктуры выявлена чёткая закономерность: доли атак вредоносных программ и фишинга растут по мере укрупнения организаций – с 47% и 37% в сегменте до 250 ПК до 59% и 67% в инфраструктурах свыше 5000 ПК соответственно. Ошибки персонала остаются высокими во всех сегментах (40–52%), достигая пика в диапазоне 500–999 ПК (52%), тогда как XSS/SQL-инъекции невысоки (3–12%) и заметнее проявляются в среднекрупных организациях.

Отраслевые закономерности

Отраслевой срез также демонстрирует значимые различия. В химической и энергетической отраслях, несмотря на критическую важность инфраструктуры, основной массив инцидентов также связан с массовыми почтовыми кампаниями и человеческим фактором на рабочих местах.

3. Практики расследования киберинцидентов в российских организациях

По данным опроса, в 2025 году расследование по факту выявленного киберинцидента проводилось в 77% российских организаций. Это свидетельствует о том, что в большинстве компаний процесс расследования уже внедрён в стандарт реагирования и не является разовой активностью, «когда есть ресурсы» (рис. 3).

Сравнение с 2024 годом показывает устойчивую практику: год назад анализ инцидентов стартовал в 79% случаев, и без разбора оставался 21%. При этом пятая часть организаций, не проводящих постинцидентный анализ, остаётся зоной риска: без ретроспективного анализа они не получают обратной связи о слабых местах и рискуют повторять схожие сценарии атак.

Зависимость от размера ИТ-инфраструктуры

Чем крупнее ИТ-инфраструктура, тем выше доля расследуемых инцидентов. У самых больших заказчиков

Рис. 3.
Расследование выявленных инцидентов в 2025 году

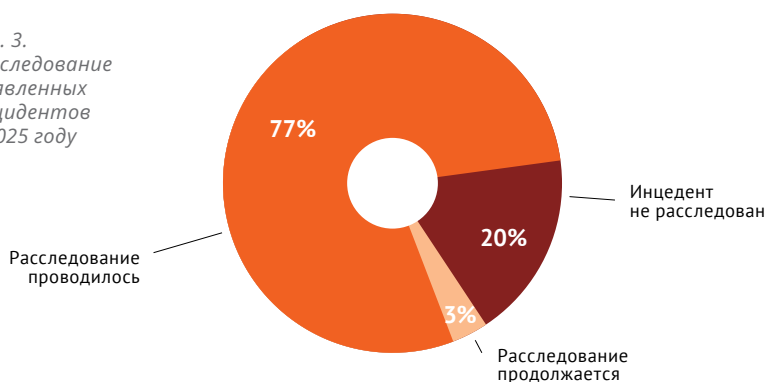
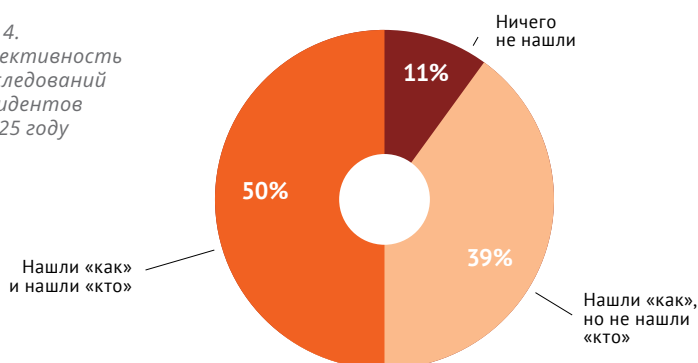


Рис. 4.
Эффективность расследований инцидентов в 2025 году



заметно чаще встречаются длительные расследования (7% против 3–5% в других сегментах), что связано со сложными многоэпизодными кейсами.

Отраслевые закономерности

Наиболее пристальное отношение к разбору инцидентов демонстрируют банковский (100% расследований), нефтегазовый (92%) и финансовый секторы (90%). Медийная отрасль выделяется тем, что 20% инцидентов находятся в статусе «расследование продолжается» при полном отсутствии кейсов без разбора.

4. Идентификация нарушителей и сценариев атак при расследовании инцидентов

Согласно результатам опроса, лишь в половине случаев (50%) расследование выявленных киберинцидентов оказывается полностью результативным: специалистам удаётся установить и способ атаки, и конкретного виновника. Ещё в 11% кейсов не удаётся выявить ни механику атаки, ни личность злоумышленника – такие инциденты фактически остаются без ключевых выводов, что ограничивает возможность точечной настройки защиты (рис. 4).

Зависимость от размера ИТ-инфраструктуры

Эффективность расследований закономерно растёт с увеличением инфраструктуры: среди организаций с числом ПК до 250 полный ответ («как» и «кто») получают 42%, в сегменте 250–499 ПК – 54%, при 500–999 ПК – 55%, а в крупнейших Enterprise-инфраструктурах (свыше 5000 ПК) – 59%. Однако во всех сегментах сохраняется значительная «серая зона» (от 33% до 43%), где восстанавливают лишь технический сценарий без атрибуции нарушителя.

Отраслевые закономерности

Лидерами по доле полноценно раскрытых инцидентов стали банковский сектор (71%), ЖКХ (68%), научные организации (67%), металлургия (65%) и транспорт (63%).

Динамика 2024–2025 годов

Сравнение результатов опроса в 2025 с ответами в 2024 году показывает заметный прогресс: доля расследований, в которых установлены и способ атаки, и виновник, выросла с 47% до 50%. При этом процент полностью безрезультатных расследований практически не изменился (10% в 2024 году против 11% в 2025-м), что свидетельствует о сохранении ядра сложных или плохо наблюдаемых

инцидентов, но в целом подтверждает постепенное укрепление практик атрибуции и постинцидентного анализа в российских организациях (рис. 5).

5. Восприятие критичности утечек данных в российских организациях

Анализ ответов участников исследования показал, что для подавляющего большинства российских компаний утечка данных находится в зоне стратегических рисков. Таким образом, индифферентное отношение к утечкам становится маргинальным, а защита данных – одним из ключевых драйверов развития корпоративной кибербезопасности (рис. 6).

Зависимость от размера ИТ-инфраструктуры

Рассматривая ответы в разрезе принадлежности респондентов к разным размерам ИТ-инфраструктуры оказалось, что оценка «критично, но не смертельно» лидирует во всех сегментах, однако её доля меняется: от 57% в компаниях до 250 ПК до максимума 70% в группе 500–999 ПК, после чего снижается до 62% в крупнейших инфраструктурах (свыше 5000 ПК). Такая динамика объясняется тем, что с ростом бизнеса организации лучше понимают масштаб ущерба, но крупные игроки чаще воспринимают утечку как «очень болезненную», а не однозначно фатальную, в отличие от средних компаний (рис. 7).

Отраслевые закономерности

Отраслевые различия также существенны. Наименее драматичную оценку дают образование, ЖКХ и часть потребительского сегмента: здесь выше доля ответов «неприятно» и «почти никто не заметит», что отражает меньшую насыщенность чувствительными данными и более низкий уровень зрелости в оценке долгосрочных последствий.

6. Ожидания рынка от ужесточения ответственности за утечки данных

Согласно опросу ИТ/ИБ-специалистов российских организаций, мнения о влиянии ужесточения законодательной ответственности на число утечек данных разделились практически поровну: 43% респондентов уверены, что количество инцидентов «безусловно сократится», тогда как 45%

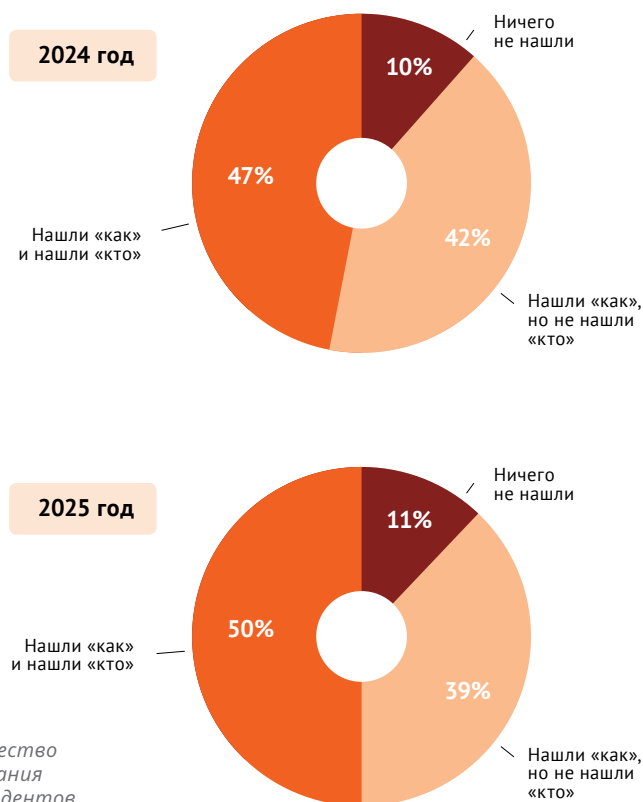


Рис. 5. Качество расследования киберинцидентов в 2024–2025 годах.

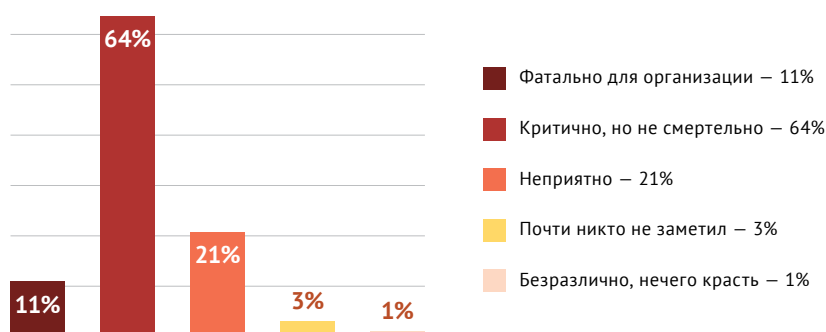


Рис. 6. Степень критичности утечки данных.

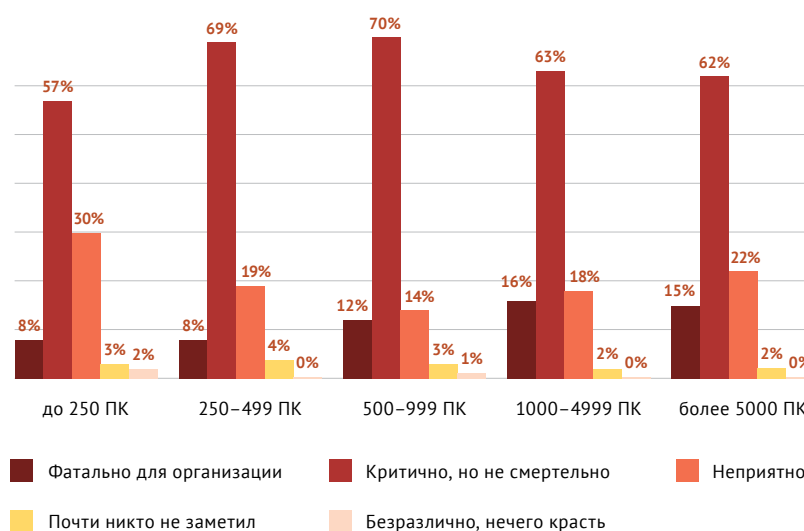


Рис. 7. Восприятие критичности утечек данных в организациях разного размера.

полагают, что это «не повлияет на количество» утечек. Эффект от ужесточения, по мнению участников, будет существенным только при сочетании с развитием внутренних практик информационной безопасности (рис. 8).

Зависимость от размера ИТ-инфраструктуры

По мере роста масштаба ИТ-инфраструктуры скепсис относительно влияния ужесточения ответственности заметно усиливается. В крупнейших Enterprise-инфраструктурах (более 5000 ПК) скептицизм максимален: 51% не ожидают эффекта, лишь 32% верят в сокращение, при этом здесь самая высокая доля тех, кто прогнозирует дальнейший рост утечек (18% против 10–13% в остальных сегментах) (рис. 9).

Отраслевые закономерности

Ожидания сильно различаются и по отраслям. Отдельно выделяются горнодобывающая отрасль и химия: здесь большинство ожидают не только отсутствия эффекта, но и дальнейшего роста числа утечек (56% и 27% соответственно).

7. Наиболее распространённые каналы утечки данных

Респонденты исследования считают главными каналами утечки конфиденциальной информации электронную почту (54%) и интернет-каналы в широком смысле (52%). Таким образом, доминируют пользовательские и сетевые каналы, тесно связанные с человеческим фактором (рис. 10).

Каналы утечек данных: взгляд заказчиков из разных сегментов

В малых организациях (до 250 ПК) почта и интернет находятся на одном уровне (по 52%). Бумажные носители и резервные копии остаются на периферии во всех сегментах (15–20% и 3–8%).

Каналы утечек данных: взгляд заказчиков из разных отраслей

Почти во всех отраслях электронная почта и интернет остаются ключевыми каналами, но их значимость различается. В потребительском секторе и финансах, помимо почты и интернета, респонденты явно выделяют смартфоны (46–48%), что отражает размытость границ между корпоративной и личной средой.

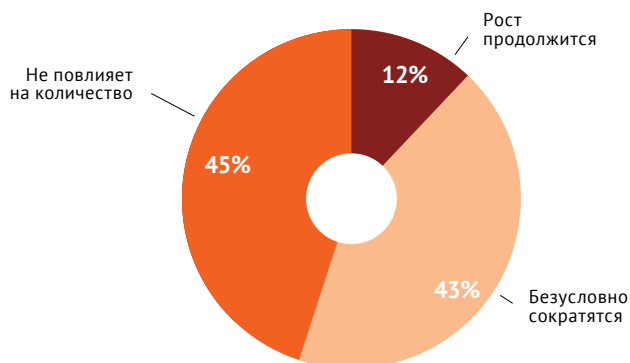


Рис. 8. Влияние ужесточения ответственности на количество утечек данных

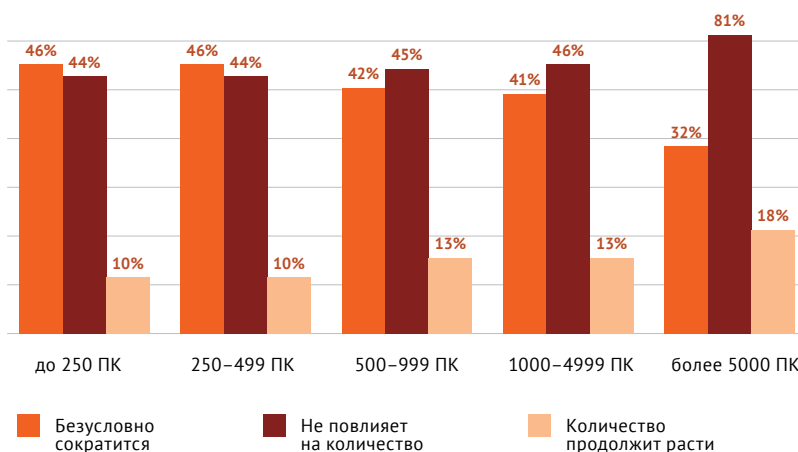


Рис. 9. Влияние ужесточения ответственности на количество утечек данных в разных сегментах респондентов

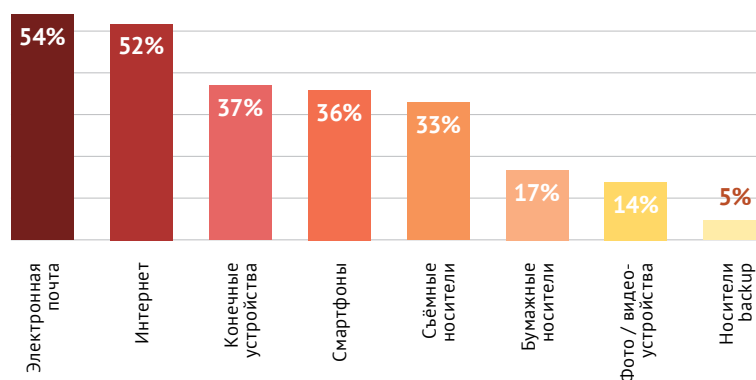


Рис. 10. Каналы утечки конфиденциальной информации глазами респондентов

8. Инструменты снижения риска утечки данных в российских организациях

В предыдущих разделах исследования были рассмотрены восприятие критичности утечек и доминирующие каналы компрометации данных. Это позволяет оценить фактический уровень зрелости практик предот-

вращения утечек и понять, насколько используемый стек решений соответствует заявленным угрозам.

Согласно опросу, ключевыми средствами снижения риска утечек для российских организаций остаются организационные меры (79%) и шифрование каналов и данных, включая VPN-решения (74%).

В целом выбор респондентов демонстрирует приоритет базовой «гигиены» – организационных практик, шифрования и классического периметра (рис. 11).

Применяемые инструменты защиты от утечек информации в организациях разных сегментов

В малом и среднем сегментах (до 500 ПК) основу защиты формируют организационные меры и шифрование (73–82% и 70–74% соответственно), тогда как доля DLP не превышает 29%, SIEM – 16%, WAF – 17%, PAM – 15%, EDR/XDR – 11%. В крупнейших Enterprise-инфраструктурах (свыше 5000 ПК), помимо оргмер и шифрования (по 83%), подавляющее большинство задействует NGFW (78%), DLP (69%) и SIEM (60%), и даже относительно нишевые технологии – WAF (52%), PAM (47%), EDR/XDR-решения (43%) – выходят на высокие значения.

Инструменты защиты от утечек информации в организациях разных секторов экономики

Практически во всех отраслях фундаментом защиты выступают организационные меры и шифрование (60–90%). Нефтегазовый сектор выделяется акцентом на аутентификацию/IDM (64%), DLP (55%) и аномально высокой долей MDM (27%).

9. Планы внедрения инструментов защиты от утечек информации в перспективе 1–2 лет

Согласно данным, полученным в текущей главе исследования, в горизонте ближайших 1–2 лет безусловным лидером среди планируемых мер предотвращения утечек становятся организационные инструменты (36% респондентов). Организационные меры превращаются в «склеивающий» слой, без которого инвестиции в технические средства не дают ожидаемого эффекта.

Второе место по приоритету занимает внедрение или развитие SIEM-систем (33%), что отражает стремление компаний повысить качество мониторинга событий информационной безопасности за счёт централизации и корреляции логов. Но стоит отметить, что системы централизованного управления мобильными устройствами (MDM) планируют внедрить

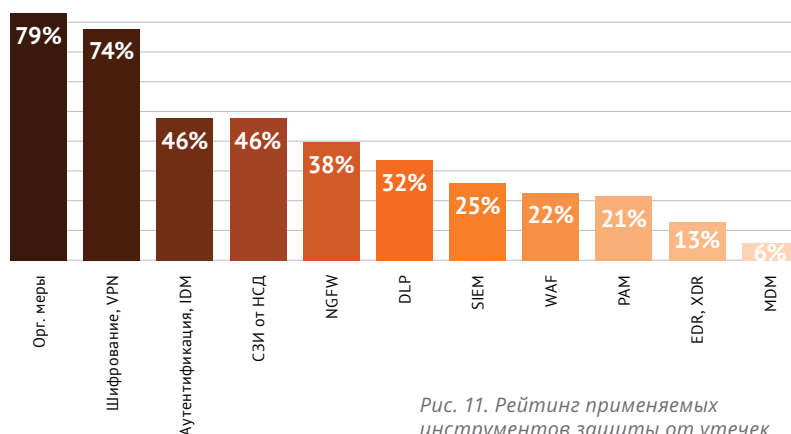


Рис. 11. Рейтинг применяемых инструментов защиты от утечек информации.

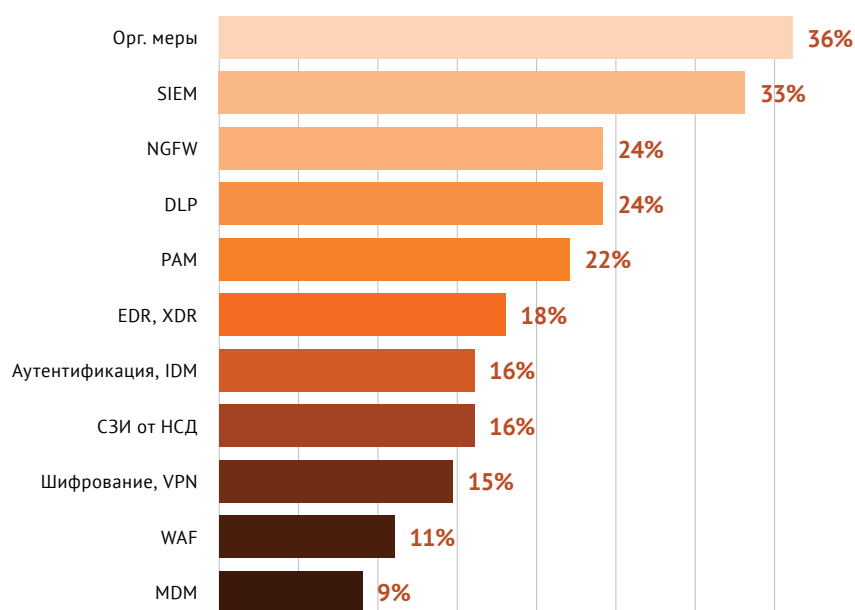


Рис. 12. Приоритетные технологии и меры предотвращения утечек данных в горизонте 1–2 лет.

в 1,5 раза больше респондентов относительно количества тех, кто уже их использует (9% относительно 6%) (рис. 12).

Планы заказчиков разных сегментов по внедрению мер защиты от утечек конфиденциальной информации в перспективе 1–2 лет

При анализе планов в разрезе размера ИТ-инфраструктуры выявляется закономерность: значимость организационных мер тем выше, чем меньше компания. Малые компании таким образом компенсируют дефицит зрелых технических средств и компетенций, тогда как крупные игроки больше полагаются на разветвлённый технологический стек.

С ростом размера инфраструктуры заметно возрастает интерес к SIEM и EDR/XDR решениям: в группе бо-

лее 5000 ПК эти показатели достигают 36% и 32% против 24% и 12% в сегменте до 250 ПК. При этом NGFW, шифрование/VPN и средства защиты от НСД демонстрируют стабильный уровень между сегментами, воспринимаясь как «гигиенический минимум».

Планы заказчиков различных отраслей экономики по внедрению мер защиты от утечек в перспективе 1–2 лет

Отраслевой разрез демонстрирует яркие акценты. Медийные компании выделяются высокими значениями сразу по нескольким технологиям: шифрование/VPN, NGFW, EDR/XDR и WAF набирают по 50%, столько же – оргмеры.

Среди других отраслей отмечается следующее: в госсекторе на первом месте организационные меры (47%),

за ними следуют NGFW (26%) и SIEM (25%); в машиностроении – SIEM (41%) и PAM (31%); в научных организациях – SIEM и NGFW (по 41%) при почти полном отсутствии планов по MDM (0%) и низком интересе к EDR/XDR (4%). В энергетике приоритет отдан PAM (37%) и EDR/XDR (29%) при низких значениях по шифрованию/VPN и NGFW (по 8%), что характерно для критической инфраструктуры с развитыми АСУ ТП.

10. Готовность ИТ/ИБ-бюджетов к задачам укрепления защиты конфиденциальной информации

В предыдущей главе респонденты обозначили приоритетные направления развития ИБ-ландшафта на ближайшие 1–2 года: от усиления защиты периметра до внедрения продвинутых средств мониторинга и аналитики инцидентов. Однако любые технологические планы упираются в ресурсные ограничения, поэтому логичным шагом исследования стала оценка того, насколько текущие бюджеты соответствуют заявленным задачам по укреплению киберзащиты и снижению рисков утечек конфиденциальных данных.

Согласно результатам опроса, лишь 31% российских организаций считают текущий уровень ИТ/ИБ-бюджета достаточным для минимизации рисков утечек. Это подчёркивает системный характер нехватки финансовых ресурсов для противодействия утечкам данных (рис. 13).

Посегментный анализ достаточности ИТ/ИБ-бюджета для снижения рисков утечек данных

Посегментный анализ по размеру ИТ-инфраструктуры выявил заметную закономерность: чем крупнее организация, тем выше доля тех, кто считает бюджет недостаточным и требует существенного роста затрат. Для сравнения: среди компаний с числом ПК до 250 таких 38%, а в сегментах 1000–4999 и более 5000 ПК – лишь по 21%.

Наиболее выраженный запрос на значимое увеличение бюджета (от 51% и выше) фиксируется у крупных заказчиков (1000–4999 ПК) и больших Enterprise-инфраструктур (более 5000 ПК): здесь суммарно 39% и 26% респондентов соответственно ожидают роста финансирования от 51% до свыше 100%. Исключе-

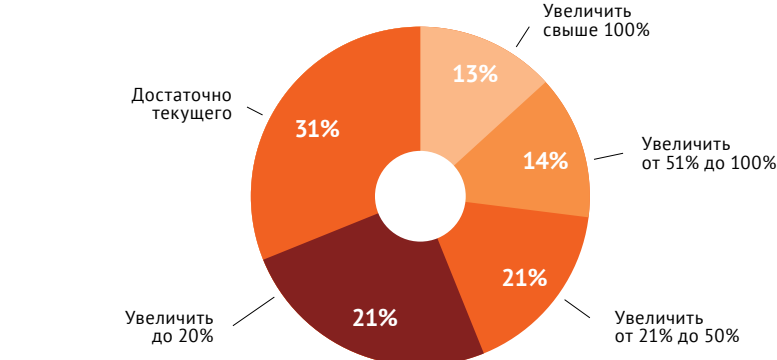


Рис. 13. Оценка достаточности ИТ/ИБ-бюджета для снижения рисков утечек данных.

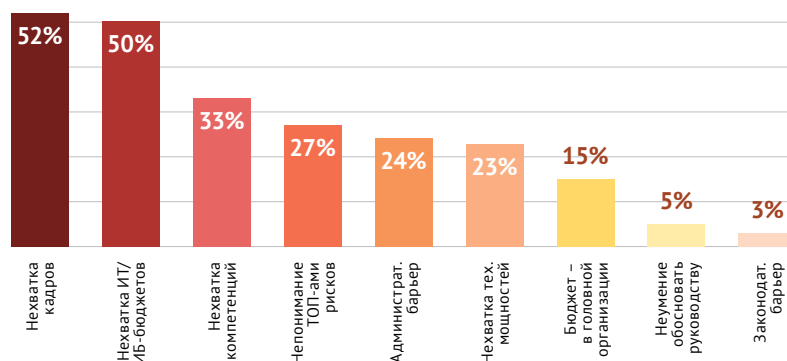


Рис. 14. Структура барьеров на пути к построению системы предотвращения утечек.

чением выглядит диапазон 500–999 ПК, где одновременно максимальна доля довольных бюджетом и умерен запрос на резкое наращивание.

Анализ достаточности ИТ/ИБ-бюджета для снижения рисков утечек данных по отраслям экономики

Отраслевой анализ также демонстрирует сильное расслоение. С другой стороны, наиболее острый дефицит бюджетов зафиксирован в образовательном секторе: лишь 8% представителей этой отрасли довольны текущим уровнем, тогда как 42% ожидают увеличения на 21–50%, а ещё 16% – на 51% и более.

Схожая картина наблюдается в государственном секторе (только 19% считают бюджет достаточным, 23% ожидают роста на 51–100% и 19% – на более чем 100%) и в горнодобывающей отрасли (14% удовлетворены, 57% совокупно ожидают увеличения на 21–50% и более). Высокотехнологический, металлургический, машиностроительный, химический и энергетический секторы демонстрируют смешанную картину: от 26% до 38% респондентов счи-

тают бюджет достаточным, однако заметные доли (22–31%) ожидают увеличения на 21–50% или на 51% и более, что говорит о потребности в дополнительной волне инвестиций в продвинутое средства защиты.

11. Барьеры при построении эффективной защиты от утечек в организациях РФ

Ранее были рассмотрены оценки респондентов относительно достаточности ИТ- и ИБ-бюджетов для реализации проектов по защите информации. Для целостного понимания ситуации исследование выявило иные барьеры: организационные, кадровые, регуляторные и технологические, которые мешают компаниям выстраивать эффективную защиту от утечек.

По итогам опроса ключевым барьером названа нехватка кадров (52% респондентов), что подтверждает системную проблему рынка: организации даже при наличии бюджетов не успевают закрывать вакансии по ИБ. Минимальное влияние имеют неумение обосновать проекты руководству (5%) и законодательные ограничения (3%) (рис. 14).

Барьеры в разных сегментах организаций

Анализ по сегментам размера инфраструктуры показывает, что в малых и небольших организациях (до 250 ПК и 250–499 ПК) главным стоп-фактором является дефицит бюджета – его доля выше, чем нехватки кадров. Это объясняется ограниченным общим финансовым ресурсом, где ИБ конкурирует с базовыми ИТ- и бизнес-задачами, а кадровый дефицит частично компенсируется меньшей сложностью инфраструктуры.

Начиная с сегмента 500–999 ПК и далее картина меняется: на первый план выходит нехватка кадров, которая опережает бюджетные ограничения и усиливается с ростом числа рабочих станций. Даже при сопоставимых бюджетах организации сталкиваются с тем, что кадровый дефицит становится главным «узким горлом».

Барьеры в разных отраслях

Разбивка по отраслям показывает, что нехватка кадров остаётся самым значимым барьером, но её выраженность сильно варьирует. По барьеру нехватки бюджетов сказано в предыдущей главе.

В ряде отраслей усиливается роль управленческих факторов. В энергетике, здравоохранении и образовании заметны барьеры нехватки компетенций, технических мощностей и зависимость от бюджета головной организации, ограничивающие локальные команды ИБ в инициативности.

12. Ожидания рынка от ИИ в задачах предотвращения утечек данных

В предыдущих главах исследования были подробно рассмотрены организационные и технологические подходы, позволяющие компаниям системно сокращать количество утечек данных и повышать управляемость инцидентами. В данном разделе представлены оценки ИТ- и ИБ-специалистов из российских организаций относительно способности ИИ существенно уменьшить вероятность утечек в реальных условиях эксплуатации корпоративных систем.

Обобщённые ответы респондентов демонстрируют сдержанный оптимизм: абсолютное большинство (44%) считает, что даже при внедре-

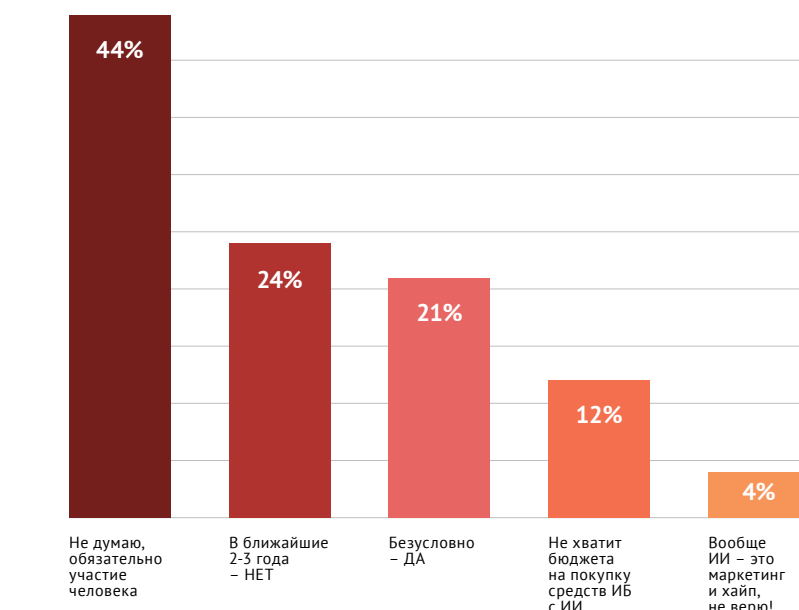


Рис. 15. Оценка снижения рисков утечек за счёт внедрения ИИ в безопасность.

нии ИИ ключевым остаётся обязательное участие человека в анализе инцидентов и принятии решений. Таким образом, рынок видит в ИИ прежде всего вспомогательное звено, усиливающее возможности SOC и служб ИБ, но не самостоятельный защитный контур (рис. 15).

Мнение представителей организаций разного масштаба о вероятности снижения утечек за счёт внедрения ИИ в безопасность

При анализе ответов в зависимости от масштаба ИТ-инфраструктуры выявляется чёткая закономерность: во всех сегментах (от малых компаний до крупнейших Enterprise с числом ПК более 5000) доминирует установка на необходимость участия человека – от 42–44% до 46% соответственно. При этом доля убеждённых сторонников ИИ, которые считают, что он «безусловно» снизит риски, постепенно растёт с 19% в организациях до 499 ПК до 24–25% в сегментах 1000–4999 и более 5000 ПК, что указывает на более высокий технологический опыт крупных игроков.

Одновременно в наиболее масштабных инфраструктурах заметно снижается доля респондентов, ссылающихся на нехватку бюджета для закупки средств ИБ с ИИ: с 12–16% в малых и средних сегментах до 5–10% в крупных. Крупные организации более трезво

оценивают временной лаг между внедрением ИИ и реальным снижением утечек, осознавая необходимость длительной настройки, адаптации нейросетевых моделей и выстраивания совместной работы аналитиков.

Позиция заказчиков разных отраслей экономики по эффективности внедрения ИИ для сокращения утечек

Отраслевой разрез также показывает значимые различия. Напротив, в горнодобывающем секторе, ЖКХ, транспортном, потребительском сегменте и ритейле уверенность в потенциале ИИ существенно снизить утечки доходит до 25–33% респондентов, при этом здесь же фиксируются более высокие значения по варианту «в ближайшие 2–3 года – нет» (до 33–35%).

Некоторые отрасли демонстрируют поляризованные мнения. В целом ожидания от ИИ в кибербезопасности зависят от регуляторного давления, цифровой зрелости и доступности компетенций: чем структурированнее контур ИБ, тем прагматичнее оценка и сильнее акцент на роли человека.

13. Искусственный интеллект и офицер безопасности: горизонты трёхлетней перспективы

Участники исследования не верят в полную замену офицера

безопасности системами с ИИ в ближайшие три года. Таким образом, отраслевой консенсус смещён в сторону совместной работы человека и интеллектуальных систем (рис. 16).

Мнение представителей организаций разного масштаба о вероятности замены офицера безопасности системами с ИИ в перспективе 3 лет

Во всех сегментах организаций по размеру ИТ-инфраструктуры доминирует убеждённость в эффективности симбиоза (65–71%), достигая максимума в группе 1000–4999 ПК (71%). При этом жёсткий скепсис (ИИ – это маркетинг) несколько выше в малых и средних сегментах (7–10%), а оптимизм (Конечно ДА!) остаётся маргинальным, немного чаще встречаясь у самых малых и самых крупных организаций (5% против 3% в среднем).

Позиция заказчиков разных отраслей экономики по вероятности замены офицера безопасности системами с ИИ в перспективе 3 лет

Наиболее яркие отличия наблюдаются в высокотехнологичном секторе и ритейле, где зафиксированы самые высокие показатели жёсткого отрицания (69% и 71% соответственно) при крайне низкой доле сторонников симбиоза (9% и 6%). В нефтегазовой, металлургической, строительной и химической отраслях сочетаются повышенный скепсис и относительно высокая доля симбиоза, что отражает консервативную позицию по замене человека ИИ при признании ценности автоматизации как вспомогательного инструмента.

Выводы

Ключевой вывод исследования – сохраняется разрыв между воспринимаемыми угрозами и фактическими мерами защиты, а также между ожиданиями от регуляторных и технологических инструментов и реальной практикой инцидент-менеджмента.

1. При этом при росте размера ИТ-инфраструктуры усиливается внимание к социальной инженерии, АРТ и инсайдерским сценариям.
2. Полностью результативными становятся лишь 50% расследо-

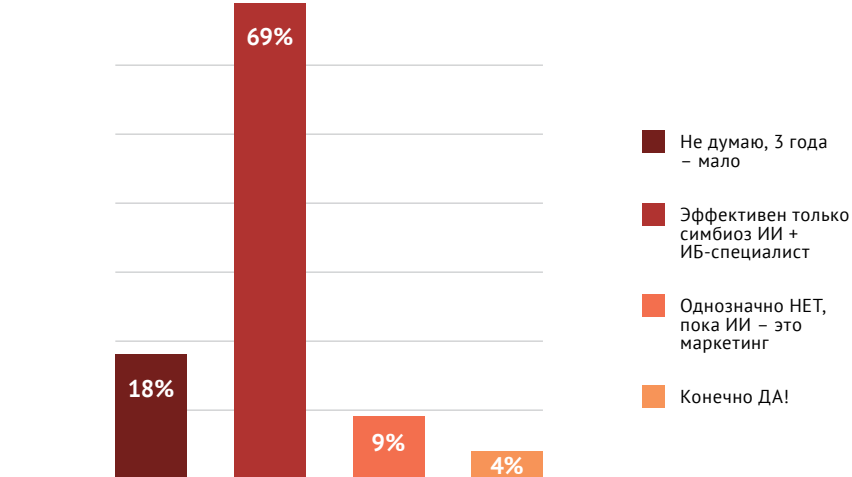


Рис. 16. Возможность замены офицера безопасности киберсистемами с ИИ в ближайшие 3 года.

ваний, а каждое десятое не даёт ни понимания механики атаки, ни установления нарушителя.

3. Утечки данных: каналы и степень восприятия риска. Утечка данных большинством респондентов воспринимается как критичный, но не смертельный риск, при этом полностью безразличное отношение почти отсутствует. Основными каналами утечек названы электронная почта, интернет-каналы, конечные устройства сотрудников, смартфоны и съёмные носители.
4. Защитные меры: фундаментом остаются организационные меры и шифрование, а продвинутые инструменты в меньшинстве. В защите от утечек чаще всего используются организационные меры и шифрование каналов и данных, включая VPN. Более продвинутые инструменты мониторинга и аналитики, такие как SIEM, WAF, PAM, EDR/XDR и MDM, распространены заметно меньше.
5. Барьеры эффективной кибербезопасности: в «клещах» кадров и финансирования. Почти 70% респондентов указывают на необходимость увеличения ИТ/ИБ-бюджетов, а ключевыми барьерами названы нехватка кадров и дефицит бюджетов. Дополнительно сдерживают развитие защиты нехватка компетенций и непонимание рисков со стороны топ-менеджмента.
6. Регуляторные ожидания: скепсис в крупном бизнесе. Рынок разделился в оценке влияния ужесточения ответствен-

ности за утечки: часть ожидает снижения инцидентов, почти столько же не видит влияния. В крупных и Enterprise-организациях скепсис усиливается, и одни лишь штрафы и формальные требования не воспринимаются как достаточный инструмент.

7. Роль искусственного интеллекта: сдержанный оптимизм и симбиоз, а не замена. Большинство респондентов считают, что ИИ должен использоваться только вместе с человеком и усиливать возможности SOC и ИБ-служб. Наиболее реалистичным сценарием на ближайшие три года считается симбиоз нейросетевых технологий и ИБ-специалистов, а не замена сотрудника.

Общая картина: организации осознают критичность утечек данных и доминирование человеческих векторов атак, но сталкиваются с дефицитом кадров, бюджетов и компетенций. Регуляторные ужесточения воспринимаются со скепсисом, а ИИ рассматривается скорее как усилитель работы специалистов, чем как их замена.



«Астерит» – федеральный интегратор систем информационной безопасности и инфраструктурных решений с Центром компетенций в Екатеринбурге и офисами в Москве, Санкт-Петербурге и Новосибирске.

asterit.ru



Какая технология сделает вас успешнее в ближайшие 5 лет

Технологии стремительно меняют мир, а вместе с ним – и требования к современным специалистам. Искусственный интеллект, кибербезопасность, робототехника, облачные платформы и другие направления уже сегодня открывают новые карьерные возможности. Но какая технология лучше всего подходит именно вам?

Пройдите наш небольшой тест, отвечая только «Да» или «Нет» и переходя по стрелкам схемы. В конце вы узнаете, какое направление технологий наиболее соответствует вашему складу мышления, почему оно может стать вашим преимуществом в ближайшие пять лет и на какие знания и навыки стоит сделать упор уже сейчас.



А. Системный архитектор

Вам подходит направление, в котором необходимо видеть цифровую систему целиком: понимать бизнес-логику, инфраструктуру, безопасность, масштабирование, базы данных и взаимодействие отдельных сервисов.

Почему это может сделать вас успешнее: компаниям всё чаще нужны специалисты, которые умеют не только создавать отдельные программы, но и проектировать устойчивые цифровые экосистемы.

- **Плюсы:** стратегическая роль, высокий уровень влияния, хороший карьерный потенциал.
- **На что сделать упор:** архитектура программного обеспечения, облачные платформы, базы данных, микросервисы, безопасность и интеграции.

В. Разработчик ядра Linux

Вам близки фундаментальные технологии: операционные системы, драйверы, память, процессоры, системные вызовы, сети и оптимизация производительности.

Почему это может сделать вас успешнее: специалистов низкого уровня значительно меньше, чем прикладных разработчиков, а их знания необходимы для серверов, облачных платформ, устройств и критически важных систем.

- **Плюсы:** редкая экспертиза, высокая техническая ценность, понимание компьютеров на фундаментальном уровне.
- **На что сделать упор:** языки C и Rust, Linux, архитектура процессоров, драйверы, сети, отладка и управление памятью.

С. Разработчик игр

Вам подходит направление, в котором программирование соединяется с воображением, визуальным искусством, физикой, звуком, сценариями и интерактивностью.

Почему это может сделать вас успешнее: игровые технологии используются не только в развлечениях, но и в образовании, медицине, рекламе, промышленном моделировании, VR, AR и профессиональных симуляторах.

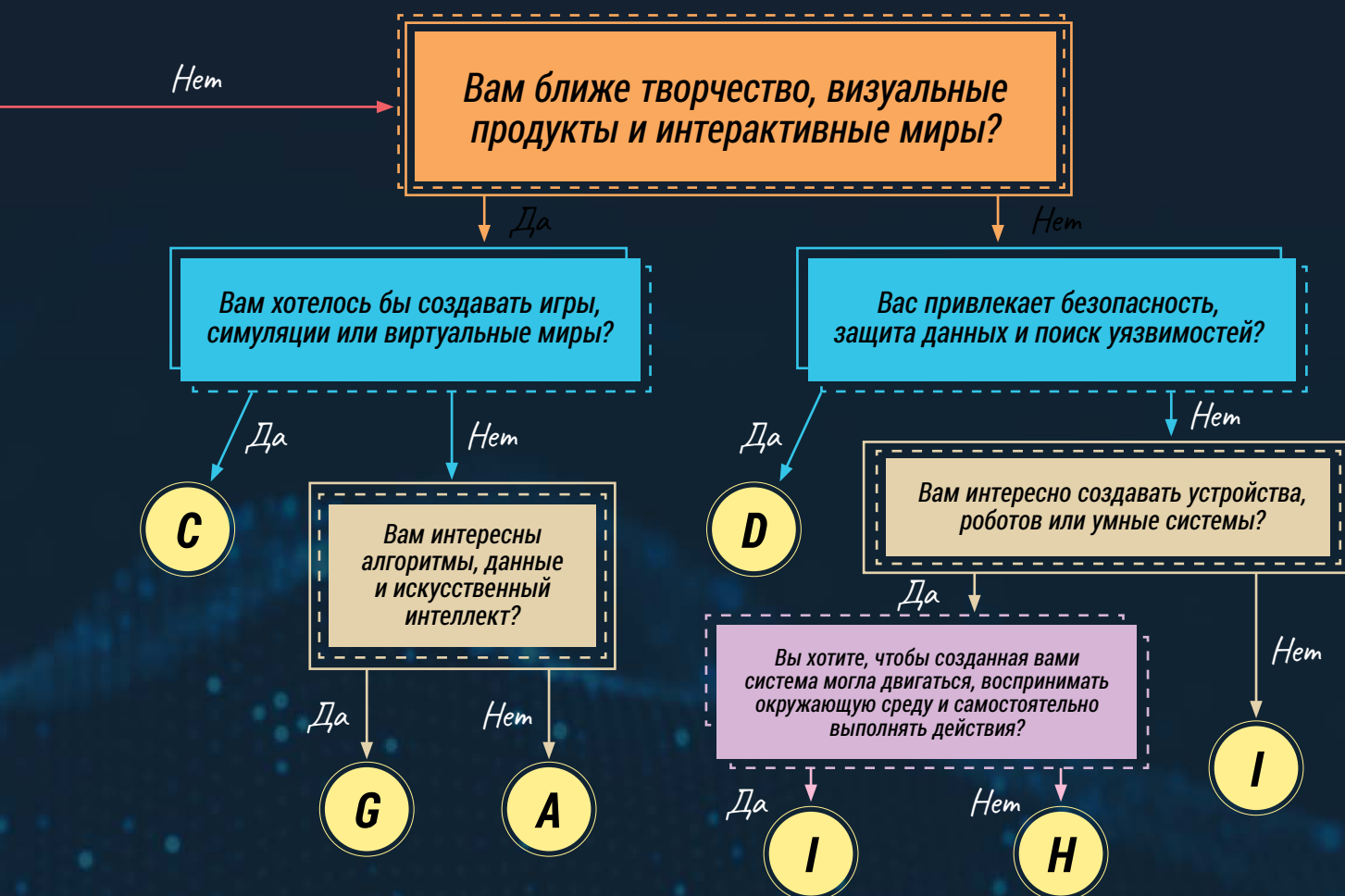
- **Плюсы:** творческая работа, наглядный результат, возможность быстро развивать собственное портфолио.
- **На что сделать упор:** Unity, Unreal Engine, C#, C++, 3D-графика, игровая физика и геймдизайн.

Д. Белый хакер

Вам подходит путь специалиста по кибербезопасности: поиск уязвимостей, моделирование атак, анализ защиты, исследование цифровых следов и предотвращение инцидентов.

Почему это может сделать вас успешнее: чем сильнее компании зависят от цифровых систем, тем выше спрос на людей, способных защитить данные, инфраструктуру и пользователей.

- **Плюсы:** высокая востребованность, разнообразные задачи, возможность работать практически в любой отрасли.
- **На что сделать упор:** Linux, компьютерные сети, веб-безопасность, Python, OSINT, криптография и этичный пентест.



Е. DevOps-инженер

Вам подходит работа на стыке разработки и эксплуатации: автоматизация, облачная инфраструктура, контейнеризация, мониторинг, CI/CD и обеспечение надёжности сервисов.

Почему это может сделать вас успешнее: бизнесу нужны специалисты, которые сокращают время выпуска продуктов, уменьшают количество сбоев и превращают сложную инфраструктуру в управляемую систему.

- **Плюсы:** высокая востребованность, сильная техническая база, влияние на весь жизненный цикл цифрового продукта.
- **На что сделать упор:** Linux, Docker, Kubernetes, Terraform, GitLab CI, мониторинг и облачные платформы.

Ф. Инженер NASA / инженер сложных научных систем

Вам подходят масштабные задачи, связанные с космосом, авиацией, промышленностью, научными вычислениями, математическим моделированием и системами высокой надёжности.

Почему это может сделать вас успешнее: такие специалисты востребованы в аэрокосмической отрасли, исследовательских центрах, робототехнике, энергетике, промышленном проектировании и разработке автономных систем.

- **Плюсы:** работа с важными инженерными задачами, интеллектуальный вызов, участие в создании технологий будущего.
- **На что сделать упор:** математика, физика, Python, C++, моделирование, теория управления и инженерный английский.

Г. Исследователь ИИ

Вам подходит искусственный интеллект: машинное обучение, нейросети, работа с данными, языковые модели, компьютерное зрение и интеллектуальная автоматизация.

Почему это может сделать вас успешнее: искусственный интеллект становится универсальным усилителем практически любой профессии и меняет разработку, аналитику, науку, медиа и бизнес-процессы.

- **Плюсы:** быстрорастущий рынок, высокий карьерный потенциал, возможность создавать новые продукты и методы работы.
- **На что сделать упор:** Python, математика, машинное обучение, нейросети, анализ данных, языковые модели и построение ИИ-агентов.

Н. Специалист по робототехнике

Вам подходит направление, в котором программный код взаимодействует с физическим миром: роботы, приводы, датчики, автономные системы, компьютерное зрение и алгоритмы управления.

Почему это может сделать вас успешнее: робототехника развивается в промышленности, логистике, медицине, строительстве, сельском хозяйстве, образовании и сфере бытовых устройств.

- **Плюсы:** практические проекты, работа с реальными механизмами, сочетание программирования, электроники и инженерии.
- **На что сделать упор:** ROS, Python, C++, электроника, механика, компьютерное зрение, датчики и системы автоматического управления.

І. Инженер встроенных систем

Вам подходит создание умных устройств: микроконтроллеров, датчиков, бытовой электроники, носимых гаджетов, IoT-систем и промышленных контроллеров.

Почему это может сделать вас успешнее: всё больше обычных предметов получают программное управление, подключение к сети и интеллектуальные функции, поэтому спрос на специалистов встроенных систем продолжает расти.

- **Плюсы:** редкая прикладная экспертиза, работа на стыке программирования и электроники, возможность создавать реальные устройства.
- **На что сделать упор:** C и C++, микроконтроллеры, RTOS, схемотехника, протоколы связи, IoT и отладка аппаратуры.

Стоимость интернета в мире

Средняя ежемесячная стоимость фиксированного широкополосного доступа в интернет в 2026 году.

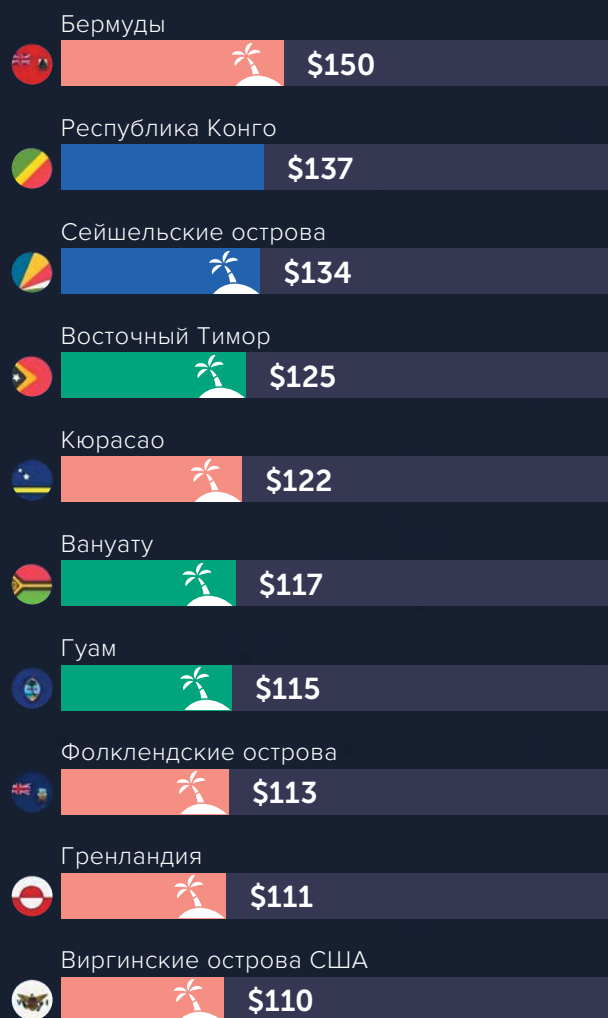


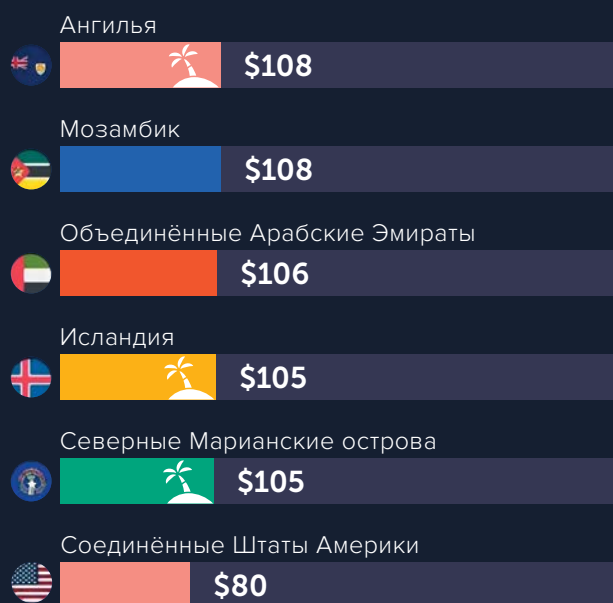
Самый дорогой

Самый дешёвый



Remote Удалённые островные территории отличаются особенно высокими ценами из-за значительных затрат на создание и обслуживание инфраструктуры.





Рост конкуренции помог снизить стоимость широкополосного интернета в США почти на две трети с 2014 года.



В Иране наблюдаются самые низкие в мире цены на интернет, что связано с обесцениванием национальной валюты и государственными субсидиями.

Данные собраны в период с 27 января по 10 февраля 2026 года на основе 2 631 тарифа широкополосного доступа в 214 странах и территориях. Все значения округлены.

Источник: visualcapitalist.com

КАК ЛЮДИ ИСПОЛЬЗУЮТ ИИ на работе

АНАЛИЗ, РАССУЖДЕНИЕ
И ПРИНЯТИЕ РЕШЕНИЙ

49%

ВЗАИМОДЕЙСТВИЕ
С ЛЮДЬМИ

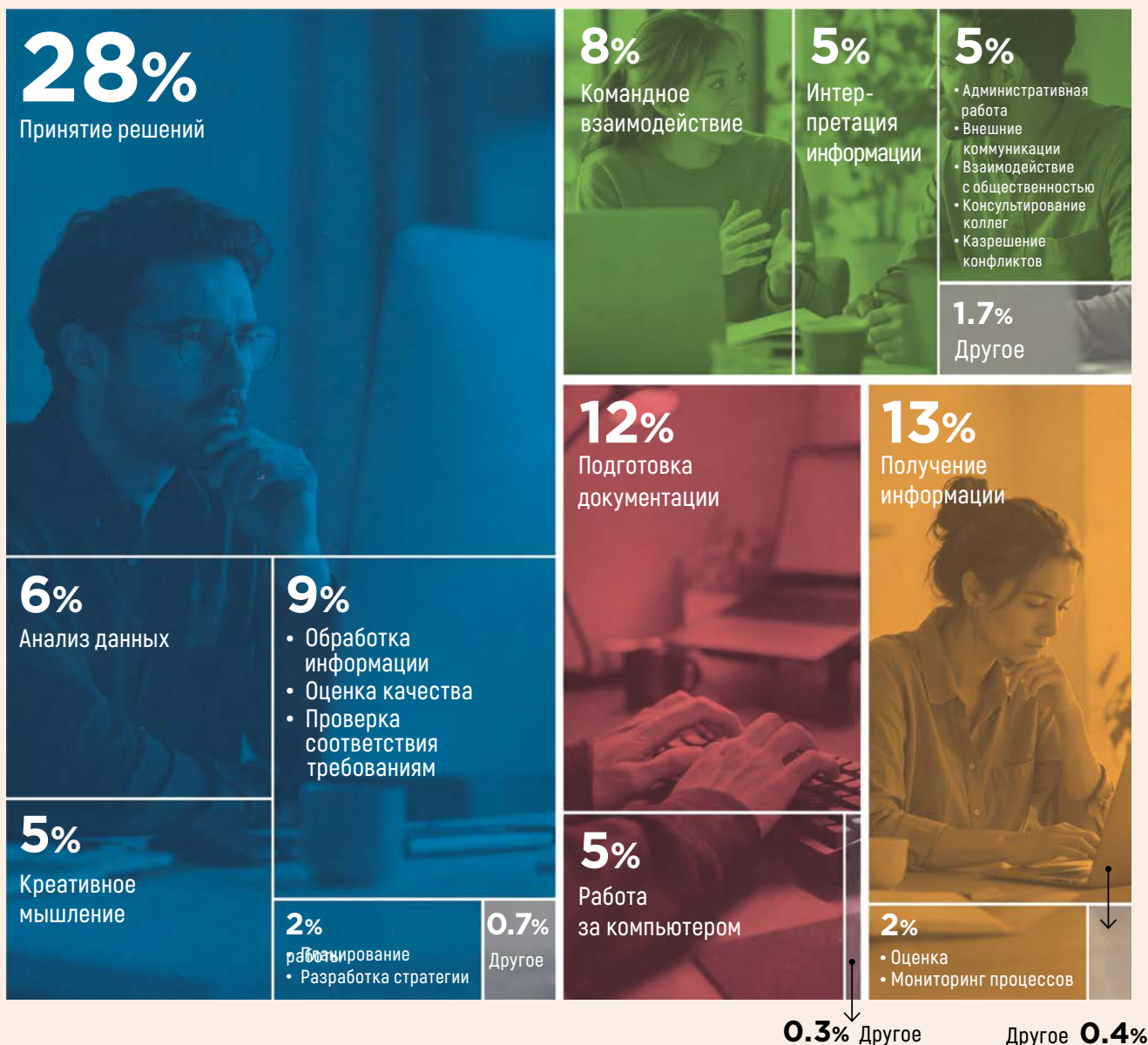
19%

СОЗДАНИЕ РАБОЧИХ
МАТЕРИАЛОВ

17%

ПОИСК И СБОР
ИНФОРМАЦИИ

15%



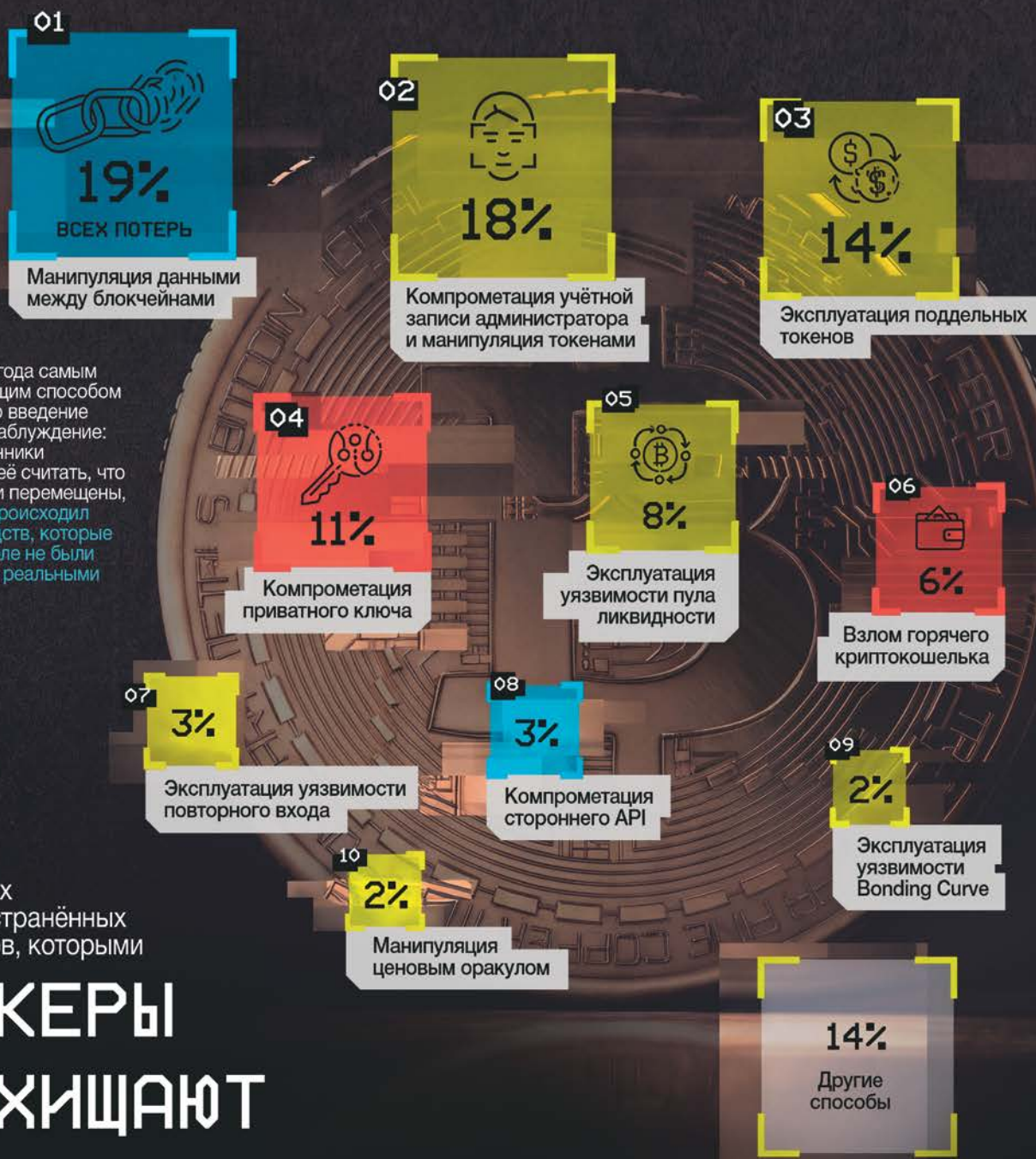
Источник: visualcapitalist.com

С мая 2025 года самым дорогостоящим способом кражи стало введение системы в заблуждение: злоумышленники заставляли её считать, что активы были перемещены, из-за чего происходил выпуск средств, которые на самом деле не были обеспечены реальными активами.

10 самых распространённых способов, которыми

ХАКЕРЫ ПОХИЩАЮТ КРИПТОВАЛЮТУ

Большинство потерь криптовалюты связано не со взломом кошельков, а с уязвимостями в программном коде и инфраструктуре.



Компрометация учётной записи администратора и манипуляция токенами включает риски как хранения активов, так и смарт-контрактов.

Источник данных основан на анализе криптовалютных взломов, произошедших в период с 1 мая 2025 года по 30 апреля 2026 года.

Основные категории рисков

СМАРТ-КОНТРАКТЫ
Ошибки в логике программы или неверные предположения, заложенные в коде.

ХРАНЕНИЕ АКТИВОВ
Потеря контроля над криптоактивами или закрытыми ключами.

ИНФРАСТРУКТУРА
Сбои или компрометация внешних систем, сервисов и источников данных.

Атаки на веб-приложения российских компаний

В первом полугодии 2026 года атаки на веб-приложения российских компаний стали более массовыми, автоматизированными и точечными. Злоумышленники все чаще стремятся не просто нарушить доступность сервиса, а получить доступ к данным, учётным записям и критичным бизнес-процессам через уязвимости приложений и API.

Отчёт сосредоточен на динамике веб-атак, наиболее опасных техниках и отраслевых особенностях. В основу материала легли агрегированные данные компаний WMX и Servicerpipe за первое полугодие 2026 года. Данные WMX отражают веб-угрозы, зафиксированные решением ПроWAF; аналитика Servicerpipe дополняет картину наблюдениями, полученными с помощью продуктов DosGate и Cyberb, а также в рамках Лаборатории кибербезопасности компании.

Ключевые показатели

- **849,7 млн** попыток веб-атак было отражено за шесть месяцев 2026 года.
- **+27%** составил рост количества атак по сравнению с первым полугодием 2025 года.
- **+40%** составил рост попыток удалённого выполнения кода на сервере (RCE).
- **+25%** составил рост инъекционных атак, включая XSS, SQLi и SSTI.
- **Около 20%** всех зафиксированных веб-атак пришлось на XSS – этот тип угроз остаётся одним из самых распространённых.

Главная тенденция: цель атак постепенно смещается с инфраструктуры на приложения, API и бизнес-логику. Такие атаки могут выглядеть как штатные действия пользователей и поэтому сложнее обнаруживаются классическими средствами защиты.

Масштаб и динамика веб-атак

В первом квартале 2026 года межсетевой экран уровня веб-приложений WMX ПроWAF отразил 412,5 млн атак, во втором – 437,3 млн. Суммарно за полугодие было зафиксировано 849,7 млн попыток атак на онлайн-ресурсы клиентов. Наиболее заметное ускорение произошло во втором квартале: рост год к году достиг 35% (табл. 1).

Основные техники и тактики

Инъекционные атаки

Крупный блок угроз был связан с инъекционными атаками: XSS, SQLi и SSTI. Их суммарное количество выросло примерно на четверть. XSS остаётся одной из наиболее распространённых угроз: доля этого типа снизилась с 25% до примерно 21%, однако на фоне общего роста атак абсолютная нагрузка по-прежнему остаётся высокой.

RCE и Path Traversal

Попытки удалённого выполнения кода на сервере (RCE) выросли на 40% год к году. Это один из наиболее опасных сценариев: успешная эксплуатация позволяет захватить контроль над приложением и продолжить атаку на другие сегменты корпоративной сети. Высокая доля RCE и Path Traversal показывает, что злоумышленники ищут уязвимости, способные быстро дать контроль над сервером или доступ к конфиденциальной информации.

API и бизнес-логика

Отдельный тренд – рост атак на API и бизнес-логику приложений. В этом случае злоумышленник использует штатную функциональность сервиса против него самого: обходит ограничения, подбирает пользовательские сценарии или массово выполняет разрешённые операции.

Главными целями становятся авторизация и регистрация пользователей, платёжные сценарии, программы лояльности и внутренние бизнес-процессы. Основным каналом эксплуатации логических уязвимостей выступает API, через который приложения и сервисы обмениваются данными. Через API атакующие автоматизируют подбор сценариев, обход ограничений и атаки на учётные записи.

Почему это опасно: запрос может быть технически корректным и не содержать очевидного вредоносного кода.

Поэтому обычного контроля сигнатур часто недостаточно – требуется анализ поведения пользователя и последовательности операций.

Какие отрасли стали драйверами роста

Наибольшая концентрация атак сохраняется в финансах, ИТ и электронной коммерции. Одновременно меняется их характер: злоумышленники всё чаще атакуют клиентские интерфейсы, пользовательские сессии, API и серверную логику, где ущерб наступает быстрее, а обнаружение инцидента требует большего контекста.

Финансы и страхование

Финансовый сектор показал крупнейший абсолютный рост и остался главной целью атакующих. Его доля в общем объёме выросла с 38% до 42%. Основными драйверами стали Path Traversal, XSS и брутфорс. Фокус смещается с инфраструктуры на доступ, пользовательские сессии и API – здесь последствия наступают быстрее, а обнаруживать злоупотребления сложнее.

Электронная коммерция

Доля электронной коммерции выросла с 12% до 19%. Усилились атаки на клиентские интерфейсы и платёжные потоки. Массовые техники частично стабилизировались, но выросли более точечные и ресурсоёмкие векторы: SQLi, dirbust и XXE. Рост SQL-инъекций указывает на повышенный интерес к backend-логике и интеграциям, включая потенциальные атаки через цепочки поставок.

Отраслевые особенности

Государственный сектор

Доля государственных компаний и сервисов увеличилась с 4% до 6%. С учётом общего роста числа атак это означает почти двукратное увеличение их абсолютного объёма. Среди наиболее заметных техник – XSS, брутфорс, автоматизированное сканирование, RCE и Path Traversal. Динамика может быть связана с усилением политически мотивированных кампаний.

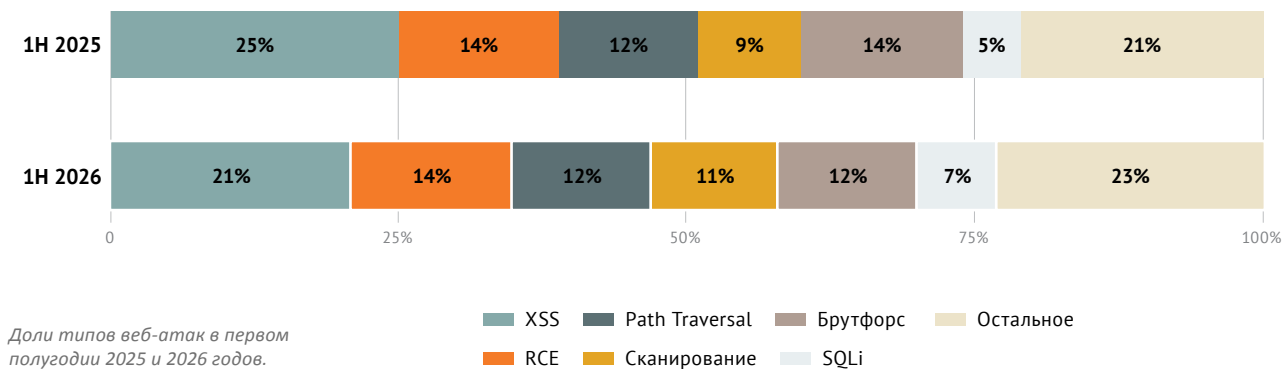
ИТ-компании и облачные провайдеры

ИТ-сектор сохранил высокую долю в общем объёме атак – около 23%.

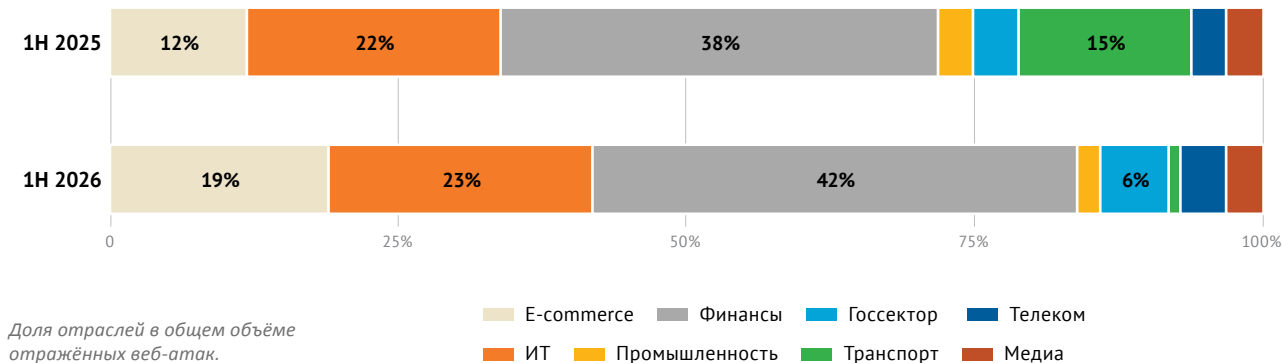
Период	2025	2026	Динамика
1 квартал	334 010 214	412 481 181	+19%
2 квартал	282 210 637	437 274 380	+35%
1 полугодие	616 220 851	849 713 611	+27%

Таблица 1. Количество отражённых веб-атак. Источник: WMX, данные ПроWAF.

Распределение атак по типам



Распределение атак по отраслям



ИТ-компании традиционно сталкиваются с SQL-инъекциями и массовым бот-сканированием. Для злоумышленников они привлекательны возможностью воздействовать на цепочки поставок, а облачные провайдеры – доступом к инфраструктуре и данным клиентов.

Общая логика атак

Во всех ключевых отраслях заметен переход от грубых массовых попыток к более адресным сценариям. Автоматизация помогает атакующим быстро проверять большое количество точек входа, а затем концентрироваться на тех, где можно получить доступ к учетным записям, данным, платёжным операциям или интеграционным механизмам.

Практический вывод: защита должна учитывать не только технические уязвимости приложения, но и допустимые пользовательские действия, которые в определенной последовательности могут превратиться в атаку на бизнес-процесс.

Выводы

Рост атак продолжается, а их качество меняется

За полугодие было отражено 849,7 млн попыток веб-атак – на 27% больше, чем годом ранее. Одновременно растёт доля сценариев, ориентированных не на массовое сканирование как конечную цель, а на получение доступа к серверу, данным и бизнес-процессам.

Приложения и API становятся основной целью

Рост RCE, атак на API и эксплуатации бизнес-логики показывает, что злоумышленники стремятся использовать штатную функциональность сервисов для финансовой выгоды, захвата учетных записей и доступа к информации.

Автоматизация затрудняет обнаружение

Боты и готовые инструменты позволяют масштабировать подбор сценариев, обход ограничений и эксплуатацию известных ошибок. При этом вредоносная активность всё чаще

имитирует нормальное поведение пользователя, что снижает эффективность простых пороговых и сигнатурных правил.

Классической защиты веб-приложений уже недостаточно

Эффективная защита требует совместной работы WAF, API Security, антибот-решений и поведенческого анализа. Средства защиты должны учитывать не только отдельный запрос, но и контекст пользовательской сессии, последовательность действий и влияние операции на бизнес-процесс.

Итог: компаниям необходимо защищать не только периметр и код приложения, но и саму логику цифровых сервисов от авторизации до платежей, программ лояльности и интеграций.

Источник: совместный отчет компаний WMX и Servicepipe «Кибератаки на онлайн-ресурсы российских компаний в 1 полугодии 2026 года».



СОВИНТЕГРА
sovintegra.ru

ДЕРЗКИЕ
ИТ-РЕШЕНИЯ





Правовое регулирование искусственного интеллекта в России

В настоящей статье расскажем о том, что такое большие фундаментальные модели (БФМ) и как они соотносятся с ИИ, какие виды таких моделей существуют, а также о том, при каких условиях их разработчики могут заручиться мерами государственной поддержки.

Чем регулируется разработка и применение ИИ

Важнейшим этапом регулирования ИИ стало подписание Президентом в июле текущего года Федерального закона от 26.07.2026 № 243-ФЗ «О поддержке развития технологий искусственного интеллекта в Российской Федерации» (далее – Закон), основные его положения раскрыты ниже.

Что Закон относит к ИИ

Критерии отнесения решений к ИИ следующие:

- 1) наличие комплекса технологических решений, включающих информационно-коммуникационную инфраструктуру, программное обеспечение, процессы и сервисы по обработке данных и поиску решений;
- 2) имитация когнитивных функций человека (включая самообучение и поиск решений без заранее заданного алгоритма);
- 3) получение результатов, сопоставимых с результатами интеллектуальной деятельности человека или превосходящие их.

Что такое БФМ

БФМ – программа для электронных вычислительных машин (ЭВМ)/составных частей ЭВМ, цель которой – выполнение большого количества интеллектуальных задач на уровне, сопоставимом с результатами интеллектуальной деятельности человека или превосходящем их (критериев оценки в Законе нет).

БФМ должна содержать не менее 1 млрд параметров, использовать алгоритмы и обучаться на составах данных для выведения (распознавания) закономерностей, предоставления информации, принятия решений или прогнозирования результатов по определённым человеком целям и одновременно являться основой для создания и доработки различных видов программного обеспечения. Функционал БФМ должен обеспечить возможность размещения предупреждения о применении технологий ИИ в порядке, предусмотренном соглашением с пользователем.

То есть БФМ является составной частью ИИ. ИИ же, кроме БФМ, включает и иную инфраструктуру.

Виды БФМ

В статье 7 Закон подробно регулирует статус суверенных и национальных БФМ и критерии отнесения к ним. Общими для этих БФМ критериями являются:

- 1) их создание российским юридическим лицом;
- 2) обеспечение подготовки ответов на запросы и хранение данных в центрах обработки данных на территории России, принадлежащих российским юридическим лицам;
- 3) подтверждение соответствия БФМ законодательству и традиционным российским духовно-нравственным ценностям (порядок подтверждения ещё не установлен).

В остальной части требования к суверенным БФМ строже: так, для них нужна полная техническая и технологическая воспроизводимость цикла разработки разработчиком БФМ, **включая её обучение**. В отношении национальных БФМ такого требования нет, более того, при разработке национальных БФМ могут использоваться зарубежные компоненты, иные БФМ, разработанные другими лицами, если они распространяются на условиях открытой лицензии.

Кому доступны меры государственной поддержки

Они доступны разработчикам национальных и суверенных БФМ. Закон не раскрывает содержание таких мер. Возможно, речь о преимуществах на государственных и муниципальных закупках, а также об ограничениях в применении в ряде социально значимых областей исключительно национальных или суверенных БФМ.

Закон также содержит послабление в части соблюдения авторских/смежных прав при работе национальных и суверенных БФМ: такие БФМ могут при обучении использовать экземпляры произведений, доведённых до всеобщего сведения и доступных для анализа без ограничения техническими средствами (фактически любую открытую в Интернете информацию).

Резюме: Многие нормы Закона отсылают к нормативным правовым актам, которые ещё предстоит разработать. Часть спорных вопросов, например по конфиденциальности и безопасности персональных данных, в Законе не урегулирована. Представляется, что Закон задаёт лишь общий вектор регулирования, за развитием которого необходимо внимательно следить.

ALTAVIA

Консалтинговая
компания «Альта Виа»
www.alta-via.ru



CISO Форум 2026

Итоги главной клубной встречи лидеров информационной безопасности

28 апреля 2026 года в Москве, в Центре международной торговли, состоялся CISO FORUM 2026 – ключевая профессиональная площадка для CISO, CIO и архитекторов ИБ, где информационная безопасность обсуждается без маркетинга на языке реальных кейсов, инцидентов и бизнес-решений.

Форум собрал более 1800 зарегистрированных участников из 1000 компаний, включая топ-менеджмент крупнейших банков, ритейлеров, промышленных холдингов, технологических корпораций и телеком-операторов.

Организатор – компания «Р-Конф»

В этом году программа форума охватила четыре параллельных трека и несколько специализирован-

ных зон: Workshop Hall по MLSecOps и сложным атакам, закрытое заседание CISO Клуб для финансового и промышленного секторов. Клубный формат с дискуссиями и разборами реальных инцидентов позволил участникам говорить правду без оглядки на вендоров и пиар.

Пленарная сессия и тренды 2026: как стать CISO и что изменилось

Форум открылся дискуссией «Лидеры ИБ в России. Как стать CISO» при модерации Георгия Руденко (CISO, Крупный банк). Участники – Дмитрий Беляев (Независимый эксперт), Виктор Бобыльков (MTS Web Services), Дмитрий Гадарь (Т-Банк), Сергей Демидов (Московская Биржа), Андрей Иванов (Wildberries & Russ), Антон Карпов (VK) и Всеслав Соленик (СберТех) – обсуждали карьерный путь CISO: от специалиста до топ-менеджера, сертификации, которые реально открывают двери в совет директоров, и личные качества, необходимые для лидерства в 2026 году.

Георгий Руденко подчеркнул, что ключевая задача CISO сегодня – объединить ожидания разных стейкхолдеров в единую стратегию и обеспечить её реализацию, при этом делая безопасность более быстрой и гибкой без потери уровня защищённости.

Андрей Иванов (Wildberries & Russ) отметил, что роль CISO находится на стыке бизнеса, ИТ, юридической функции и управления персоналом, а сами метрики и управление безопасностью должны строиться от бизнес-рисков и стратегии компании. По его словам, современный руководитель ИБ – это не только лидер команды, но и человек, который работает с угрозами, ещё не до конца сформировавшимися на рынке.

Дмитрий Беляев в ходе дискуссии отдельно подчеркнул, что современный CISO – это не только управленец, но и человек, который должен глубоко понимать техническую «землю»: без этого невозможно отличить

реальную защиту от формальной и принимать решения, которые работают в реальных инцидентах.

Ключевой вывод сессии: сегодня CISO – это стратегический партнёр, влияющий на архитектуру продуктов, инвестиционные решения и устойчивость бизнеса в целом.

Метрики ИБ и язык бизнеса: как говорить с управлением

В дискуссии «Метрики эффективной ИБ» под модерацией Дмитрия Ушакова («Гладиаторы ИБ») приняли участие Никита Гергель (Yandex B2B Tech), Георгий Руденко (CISO, Крупный банк), Виталий Медведев (ГК «Медси»), Павел Пархомец (Wildberries & Russ), Андрей Шлегель (Независимый эксперт) и Илья Борисов (Билайн). Спикеры единодушно отметили: число заблокированных атак или количество закрытых уязвимостей почти ничего не говорят совету директоров. Бизнесу нужны другие цифры – стоимость простоя, потерянная выручка, влияние на клиентский опыт.

Спикеры сошлись во мнении, что традиционные метрики ИБ перестают работать на уровне правления: бизнес не интересуется показателями вроде количества атак или закрытых уязвимостей. Гораздо важнее – влияние на выручку, простои и клиентский опыт.

Отдельно обсуждалось, что безопасность сегодня становится неотъемлемой частью бизнес-процессов и условием устойчивого развития компании.

При этом, как отмечал Виктор Бобыльков (MTS Web Services), в большинстве организаций диалог между бизнесом и безопасностью по-прежнему остаётся напряжённым: стороны часто воспринимают друг друга как ограничение или источник рисков, а не как партнёров.

Архитектура против бумажной безопасности

Одной из самых острых стала дискуссия «Архитектура vs. бумажная безопасность» при модерации Анастасии Гайнетдиновой (Whoosh). Участники – Руслан Ложкин (Абсолют Банк), Дмитрий Кузнецов (Альфа-Банк), Антон Замараев (ОТП Банк), Антон Антропов (IT TASK), Артём Гяммер (Вайлдберриз Банк) и Михаил Савельев (Ростелеком) – разобрали разрыв между докумен-



тами и реальной защитой, переход от формального комплаенса к практической архитектуре и баланс между безопасностью и удобством пользователей.

Александр Сухомлин (Ростелеком) подчеркнул, что говорить об исчезновении периметра некорректно: он не исчез, а сместился на уровень пользователей, устройств и взаимодействий. В этих условиях задача ИБ – выстраивать контроль не на границах сети, а на уровне всех точек взаимодействия.

Участники также отмечали, что классическая модель защиты трансформируется: архитектура становится распределённой, а сами средства защиты выступают скорее компенсирующими мерами, снижая риски и давая команде время на реагирование.

Эволюция атак и защита от утечек

В треке «Когда атака – вопрос времени» эксперты разобрали современные многоэтапные сценарии компрометации, использование ИИ злоумышленниками и атаки на цепочки поставок. Илья Зуев (МТС Банк) в докладе «От периметра к ядру: деконструкция современных многовекторных атак» на реальных примерах показал, как классические защитные системы дают сбой.

Илья Зуев в своём докладе показал, что современные атаки развиваются как многоэтапный процесс и обходят классические защитные модели.

Отдельное внимание уделили облачной безопасности. Михаил Захряпин (Cloud Advisor) отметил, что большин-

ство инцидентов связано не столько со взломами, сколько с ошибками конфигурации – по сути, речь идёт о «входе в открытую дверь».

Эксперты облачного трека также подчеркнули, что ключевой точкой атаки становятся учётные записи: по их словам, сегодня достаточно валидной учётной записи, чтобы получить доступ к инфраструктуре, а сама идентичность пользователя фактически становится новым периметром.

Дополнительно отмечалось, что основными причинами инцидентов остаются ошибки конфигурации и управление доступами, а не сложные технические уязвимости.

Параллельно в треке «Объект атаки» обсуждали защиту персональных данных от квантовой устойчивости до оборотных штрафов. Кристина Боровикова (RPPA. pro) модерировала дискуссию с участием Артемия Новожилова (Эксперт) и Алексея Колпакова (ОТП Банк).

Люди, стрессоустойчивость и мотивация

Заключительная дискуссия форума была посвящена теме, которая редко выносятся на публичные мероприятия, – профессиональному выгоранию в ИБ. Модератор Виктор Бобыльков (MTS Web Services) вместе с Ильёй Зуевым (МТС Банк), Кириллом Мякишевым (OZON), Виталием Медведевым (ГК «Медси»), Дмитрием Шараповым (Дом. рф) и Андреем Ивановым (Wildberries & Russ) обсуждали, как строить стрессоустойчивые команды, удерживать талантливых специалистов и сохранять себя после крупных инцидентов.



Участники отмечали, что нагрузка на специалистов растёт, а требования к скорости реагирования и уровню ответственности становятся всё выше, что делает управление командой и её состоянием критически важной задачей для CISO.

Дискуссия: взаимодействие кибербезопасности, ИТ и бизнеса

Одной из самых острых на форуме стала дискуссия о взаимодействии кибербезопасности, ИТ и бизнеса. Участники открыто обсуждали системный конфликт приоритетов: бизнесу важна скорость и рост, ИТ – стабильность, а ИБ – снижение рисков.

Эксперты отмечали, что во многих компаниях этот диалог до сих пор строится через противостояние. Как звучало в обсуждении, типична ситуация, когда бизнес воспринимает безопасность как фактор, «мешающий зарабатывать», в то время как ИБ считает, что бизнес недооценивает реальные риски.

При этом спикеры подчёркивали, что такая модель больше не работает. По их мнению, эффективное взаимодействие возможно только в случае, если безопасность становится частью бизнес-процессов и встраивается в продуктовую и ИТ-архитектуру на ранних этапах.

Отдельно обсуждалось, что задача CISO сегодня – не только защищать инфраструктуру, но и выстраивать коммуникацию между всеми сторонами. Участники отмечали, что именно отсутствие единого целеполагания чаще всего становится причиной конфликтов между командами.

Также поднималась тема практических инструментов взаимодействия: от демонстрации реальных сценариев атак до перевода рисков на язык денег и бизнес-потерь. Такой подход, по мнению участников,

помогает быстрее находить общий язык с руководством и принимать решения.

Итог дискуссии: кибербезопасность больше не может существовать как отдельная функция – она становится частью бизнес-логики и требует постоянного диалога между всеми участниками.

Workshop Hall: MLSecOps, сложные атаки и фишинг

Одним из самых востребованных форматов стала воркшоп-зона. С утра прошла сессия «MLSecOps



и безопасность ML/LLM-систем» от партнёров K2 Кибербезопасность и «Лаборатории Касперского».

Эксперты обсуждали влияние ИИ на безопасность. Евгений Сидоров (Yandex B2B Tech) отметил, что искусственный интеллект уже активно используется для повышения устойчивости облачной инфраструктуры и встроен в сервисы безопасности.

Кирилл Сорокин (Билайн) добавил, что безопасность сегодня неотрывна от бизнеса, а внедрение ИИ становится фактором повышения зрелости ИБ. По его словам, такие технологии уже позволяют снижать нагрузку на команды SOC, в том числе на уровне L1 и частично L2.

Отдельно в рамках обсуждений безопасной разработки отмечалось, что значительная часть современного кода формируется за счёт зависимостей, а в контексте ИИ-систем точкой входа в атаки всё чаще становится не уязвимость, а корректно сформулированный запрос.

CISO Клуб: закрытая дискуссия для первых лиц

В рамках форума прошли закрытый круглый стол C-level без записи и открытой аудитории.

Отдельная дискуссия CISO Клуб была посвящена теме «Безопасность цепочки поставок ПО: как закрыть риски на трёх этапах – от отбора компонентов до промышленной эксплуатации». Модератором выступил Роман Карпов (Axiom JDK).

В обсуждении приняли участие Василий Куценко (Почтатех), Антон Володченко (CodeScoring), Денис Макрушин (Yandex B2B Tech), Дмитрий Малыхин (независимый эксперт), Дмитрий Шмойлов (Лаборатория Касперского) и Алексей Захаров (Axiom JDK).

Эксперты рассматривали цепочку поставок как непрерывный процесс, в котором риски возникают на каждом этапе – от выбора зависимостей до эксплуатации приложений в продакшене.

Участники отмечали, что значительная часть современного ПО фактически собирается из сторонних компонентов: по оценке Дениса Макрушина (Yandex B2B



Tech), до 90% кода сегодня приходится на зависимости, что радикально увеличивает поверхность атаки.

В этом контексте особое внимание уделялось первому этапу – отбору и допуску компонентов. Эксперты подчёркивали необходимость более строгой проверки библиотек, контейнерных образов и источников кода ещё до их попадания в контур разработки.

Отдельно обсуждалась задача воспроизводимой и проверяемой сборки. Участники отмечали, что без прозрачности сборочного процесса невозможно гарантировать целостность продукта и доказать отсутствие компрометации на этапе разработки.

Третий блок дискуссии был посвящён эксплуатации. Спикеры сошлись во мнении, что контроль не заканчивается релизом: необходимо выстраивать процессы мониторинга уязвимостей, управления обновлениями и реагирования на инциденты уже в промышленной среде.

Дополнительно подчёркивалось, что в условиях роста использования ИИ меняется и сама модель угроз: точкой входа в атаки всё чаще становится не уязвимость в коде, а взаимодействие с системой, например через некорректно сформулированные запросы.

Общий вывод дискуссии: безопасность цепочки поставок перестаёт быть задачей отдельной команды и становится сквозным процессом, объединяющим разработку,

эксплуатацию и информационную безопасность.

Что дальше?

CISO FORUM 2026 подтвердил: отрасль находится в точке перехода. Старые подходы к защите перестают работать, роль лидера ИБ трансформируется, а бизнес требует измеримых результатов. Формат «сделано CISO для CISO» оказался востребован как никогда, потому что позволяет обсуждать реальную боль без оглядки на вендоров и согласованные сценарии.

Организаторы анонсировали, что CISO FORUM 2027 расширит программу, добавит новые отраслевые вертикали и продолжит развивать формат закрытых клубных встреч.

Благодарности партнёрам

Организаторы выражают искреннюю благодарность стратегическому партнёру Yandex B2B Tech, генеральным партнёрам CURATOR, INDEED и IT TASK, партнёру воркшопов K2 Кибербезопасность и Лаборатории Касперского, партнёру цифровых технологий Мегафон, а также всем официальным партнёрам, экспо-участникам и компаниям, поддержавшим форум: Beeline, Positive Technologies, СберТех, Selectel, RED Security / MTC, Solar, Cloud Advisor, NGR, CTRLHACK, CodeScoring / Профископ, StormWall, Security Vision, UserGate, F6 / Proway, TC Солюшн, DPA Analytics, Luntry, Itorex / Servicepipe, iTPROTECT, Rebrandy, Uniteiler, Axiom JDK, АБП24, Swordfish Security / AppSec Solutions. Без вашей поддержки это событие не состоялось бы.

Увидимся на CISO Форуме в 2027 году!



Системные программисты России беспокоятся о профильном образовании

Круглый стол «Преподавание системного программирования в вузах страны. Проблемы и решения», состоявшийся в рамках XIII Научно-практической конференции OS DAY 2026 в РЭУ им. Плеханова в июне, стал площадкой для открытого разговора экспертов российской ИТ-отрасли и преподавателей вузов о состоянии отечественной системы высшего образования.

Главный вызов, который озвучили представители индустрии: текущая модель подготовки системных программистов не поспевает за гонкой технологий в ИТ. Пожалуй, настолько

откровенного разговора о насущных кадровых проблемах отрасли на такой авторитетной площадке ещё не случилось.

Недостаточный бакалавриат

Самая острая критика на круглом столе прозвучала в адрес болонской системы: четырёхлетний бакалавриат фактически признан непригодным для подготовки специалистов необходимого уровня.

«Я был очень огорчён, когда эту систему вводили, и очень радуюсь сегодня, когда её постепенно убирают, – заявил Валерий Егоров, начальник управления разработки доверенного программного обеспечения НТЦ «Атлас». – Потому что обучить системного программиста за четыре года невозможно. Первые два года студент привыкает к тому, что ему в принципе нужно учиться,

на третьем у него появляется понимание, но ещё нет знаний, и только на четвёртом он начинает учиться, но тут бакалавриат заканчивается. Не хватает одного года».

Цифры подтверждают системный характер проблемы: по данным Минобрнауки России, только 50% поступивших на ИТ-специальности заканчивают обучение по программе бакалавриата. При этом в целом по рынку до 40% учащихся по различным специальностям не получают дипломы.

Проблема усугубляется катастрофической неравномерностью в качестве преподавания. Успешные кейсы подготовки кадров существуют, но они пока что не масштабируются за пределы топ-вузов.

«На должном уровне системное программирование преподаётся преи-

мущественно в ведущих университетах: МГУ, СПбГУ, ИТМО, – пояснил Андрей Духвалов, вице-президент «Лаборатории Касперского», директор департамента перспективных технологий. – В периферийных университетах мало преподавателей с индустриальным опытом. Разница в уровне подготовки между регионами и ведущими вузами сохраняется. Возникает потребность в широком внедрении системно-инженерного подхода».

На деле, как отметила Мария Полякова, руководитель направления по взаимодействию с вузами «Открытой мобильной платформы», в высших учебных заведениях на периферии кадровый кризис значительно глубже.

«Там в принципе острая нехватка преподавателей. Слегка утрируя, скажу, что на одного преподавателя – пятьдесят студентов. Индивидуально работать с каждым в таких условиях, скажем мягко, сложно, и это сказывается на уровне подготовки».

Кризис подготовки ИТ-кадров обусловлен не только технической отсталостью, но и методологическими ограничениями в образовательных программах. Как отметили эксперты в ходе круглого стола, для преодоления сложившейся ситуации необходимо внедрение сквозных моделей практико-ориентированного обучения и развитие исследовательской активности студентов.

Парадокс дефицита кадров

Логика подсказывала, что уход с российского рынка западных вендоров должен был бы высвободить кадры, однако этого не произошло.



Российский ИТ-сектор растёт слишком быстро, чтобы рынок труда успевал насыщаться. Однако, по мнению Алексея Новодворского, советника генерального директора «Базальт СПО», проблема лежит не столько в количестве выпускников, сколько в их ранней «деформации».

«Нельзя сказать, что высшая школа недорабатывает, – отметил он. – Проблемы начинаются на этапе опыта, поскольку рынок системного программирования узок. Многие перспективные молодые специалисты сразу уходят в аутсорс. Хорошего системного программиста приходится искать днём с огнём».

Опубликованная не так давно аналитика портала hh.ru рисует парадоксальную картину: при общем росте безработицы в ИТ на одну вакансию в среднем приходится 12–15 кандидатов. При этом дефицит высококвалифицированных кадров только усиливается. Аналити-

ки портала объясняют это тем, что работодатели активно конкурируют за специалистов с «подтверждённой экспертизой», и кадровый дефицит касается именно их, а сотрудники более низкого уровня остаются не востребованы.

Парадокс ситуации в том, что на фоне кадрового голода цены на ИТ-образование в ведущих вузах страны растут опережающими темпами. По данным CNews и «Ведомостей», стоимость обучения на программах «на стыке ИТ, математики и ИИ» выросла на 20–52%. При этом средние зарплаты в отрасли почти не растут, а крупные компании проводят масштабные сокращения, всё шире используя существующие модели искусственного интеллекта.

Такая политика может пагубным образом повлиять на кадровый конвейер. С одной стороны, нейросети идеально закрывают текущую потребность в дешёвой рабочей силе. С другой – они перекрывают кислород для вчерашних студентов, лишая их возможности проходить «школу выживания» на простых задачах.

«Искусственный интеллект очень хорошо выполняет простые, понятные задачи, которые не требуют больших умственных затрат, отлично работает на самом тривиальном уровне, на уровне джунов, – сформулировал проблему Андрей Духвалов. – Как следствие, коммерческой компании нанимать джунов становится не нужно, так как их работу гораздо быстрее и дешевле выполняет ИИ. То есть вузы будут выпускать джунов, а работы для них не будет. Но вопрос в том, откуда





в таком случае появятся более квалифицированные кадры. Кто будет их выращивать и что мы как индустрия будем с этим делать?»

ИИ как ускоритель, а не замена

Однако, по мнению экспертов отрасли, ожидания, что широкое использование ИИ приведёт к массовым увольнениям программистов, сегодня не имеют ничего общего с реальностью. Конечно, как отметила Анна Кан, руководитель центра научно-методического и экспертного сопровождения ВНИИ «Центр», к концу минувшего 2025 года объём контента, произведённого при помощи ИИ, превысил объём прочего контента. Но так называемый «цифровой голод» российской ИТ-отрасли настолько велик, что почти двадцатикратный рост объёма генерируемого кода за последние десять лет не смог его утолить даже в общих чертах.

Другое дело, что широкое использование ИИ может негативно повлиять на образование студентов. Георгий Курячий, ведущий программист «Базальт СПО» и преподаватель ВМК МГУ, в этой связи напомнил участникам круглого стола и гостям конференции о ещё одной опасной стороне использования ИИ – проблеме «памяти пальцев»: простые упражнения, которые раньше помогали нарабатывать базу, студенты теперь легко делегируют нейросетям, так и не приобретая практического опыта.

«Когда ИИ используют старшекурсники или магистранты, они делают это уже с умом, – подтверждает ход его мыслей Инна Батраева, заведующая

кафедрой технологий программирования СГУ им. Н.Г. Чернышевского. – А младшекурсники зачастую в силу того, что у них нет базовых знаний, даже не понимают, какой бредовый код написали нейросети. И опасность использования ИИ возникает именно тут, потому что не писал своими руками код – не сможешь писать его дальше».

С другой стороны, ведущие специалисты в области системного программирования беды в этом не видят.

«Если разработчик ПО понимает, как ускорить или удешевить свою работу с помощью ИИ, он будет его использовать», – считает Алексей Новодворский.

Проблема, по мнению Анны Кан, заключается в другом – в недостаточной систематичности нынешней системы образования. Использование нейросетей, составление промптов для их работы требует глубокого

понимания профессии, погружения в тему. Именно это является ключевой характеристикой даже для самого юного программиста, использующего ИИ в работе. И именно этого «метанавыка» нынешним выпускникам решительно не хватает.

Несмотря на сложные вопросы, поднятые в ходе круглого стола, конференция оставила после себя оптимистичное впечатление. Организаторы отметили возросшее количество студентов и аспирантов среди участников OS DAY 2026. Студенты-бакалавры СГУ им. Н.Г. Чернышевского, например, представили на конференции полноценную разработку – расширение Pompilius для облачной интеграции в Linux, созданную на хакатоне. Молодое поколение проявляет живой интерес к системной инженерии, что позволяет с осторожным оптимизмом смотреть в будущее.

Однако, для того чтобы этот интерес превратился в реальную конкурентоспособность отрасли, вузам придётся сломать устоявшиеся образовательные шаблоны, а бизнесу – перестать рассматривать обучение джунов как статью расходов. Как показывают исследования HR-экспертов, компании, которые инвестируют в апскиллинг и внутренние академии, получают серьёзное конкурентное преимущество на рынке труда 2026 года. Государство также расширяет образовательный контур по ИТ-специальностям, но эффект от этих инициатив проявится не скоро.

Константин Кутайгородский



25/24

2025 год

Доля крупных застройщиков, использующих ТИМ

+7 п.п.

44%

Объем рынка ТИМ, млрд Р

+5%

9,5

Введено обязательное использование ТИМ для проектирования бюджетных объектов и участия в

События

50% МКД проектируются с использованием ТИМ

~90% Положительных заключений экспертизы на проекты, разработанные с использованием ТИМ

~90 XML схем утверждено для ТИМ

Главные итоги ЦИПР-2026

Более 13 тысяч участников, 350 подписаний, полсотни стран

С 18 по 21 мая в Нижнем Новгороде прошло главное деловое событие в сфере цифровой экономики и технологий – XI международная конференция «Цифровая индустрия промышленной России».

За 4 дня мероприятие посетило более 13 тысяч участников из всех регионов России и 46 стран мира, включая Китай, Индию, Бразилию, Сербию, Аргентину, Филиппины и другие государства. На выставочной экспозиции было представлено 185 стендов с технологичными решениями от российских и международных компаний. Деловая программа включила 165 дискуссий, на которых выступило более 1 000 спикеров. За время проведения конференции было подписано более 350 соглашений, включая международные с Китаем, Лаосом, Анголой.

На ЦИПР-2026 представители бизнеса и власти традиционно обсудили ключевые вопросы цифровой трансформации различных отраслей экономики и технологического суверенитета. В конференции приняли участие Председатель Правительства РФ **Михаил Мишустин**, первый заместитель Председателя Правительства РФ **Денис Мантуров**, заместитель Председа-

теля Правительства РФ – руководитель Аппарата Правительства РФ **Дмитрий Григоренко**, министр цифрового развития, связи и массовых коммуникаций РФ **Максут Шадаев**, губернатор Нижегородской области **Глеб Никитин**, а также представители ключевых игроков рынка: президент «АвтоВАЗ» **Максим Соколов**, генеральный директор «ОАК» **Вадим Бадеха**, генеральный директор «ОДК» **Александр Грачев**, генеральный директор и председатель правления «Концерн «Калашников» **Алан Лушников**, генеральный директор холдинга «Севергрупп» **Алексей Мордашов**, президент «ГМК «Норильский никель» **Владимир Потанин**, генеральный директор «Газпром нефть» **Александр Дюков**, директор «1С» **Борис Нуралиев**, президент «Ростелекома» **Михаил Осеевский**, генеральный директор «МТС» **Инесса Галлактионова**, старший вице-президент, руководитель блока «Технологическое развитие» «Сбербанк» **Андрей Белевцев** и многие другие.

Открывая пленарную сессию «Сделано в России: цифровая трансформация промышленности», Председатель Правительства РФ **Михаил Мишустин** подчеркнул ключевую роль конференции для отрасли: «На этой площадке традиционно – уже в 11-й раз – собираются ведущие отраслевые заказчики и разработчики, эксперты и представители органов власти. Все, кто вносит весомый вклад в выполне-

ние поставленной Президентом задачи по укреплению технологического суверенитета и технологической независимости от используемого иностранного программного обеспечения».

Премьер также отметил, что за шесть лет доля ИТ-отрасли в структуре ВВП удвоилась, а объем продаж российских продуктов и сервисов вырос почти в 4,5 раза, превысив 5 трлн рублей. Впервые с 2022 года экспорт российского ПО вырос на 15%, а численность занятых в отрасли превысила миллион человек.

Заместитель Председателя Правительства – руководитель Аппарата Правительства РФ **Дмитрий Григоренко**, подводя итоги работы индустриальных центров компетенций (ИЦК), заявил: «Подход к созданию российского программного обеспечения существенно изменился. Во-первых, мы перешли к импортозамещению на основе данных: совместно с ИЦК собрали и систематизировали информацию об имеющихся на рынке российских решениях и приоритетах в ИТ-разработке. Во-вторых, разработчики не просто заместили зарубежные решения, но и доработали их с учётом новых требований и коллективных запросов отрасли». По его словам, из 175 отобранных в 2022 году особо значимых проектов 120 уже завершены, более 930 предприятий используют



разработанные решения, а российским софтом закрыто более 180 «белых пятен» – направлений, где ранее не существовало отечественного ПО.

Губернатор Нижегородской области **Глеб Никитин**, комментируя итоги форума, подчеркнул: «ЦИПР подтверждает, что наш регион – один из лидеров в индустрии ИТ в стране. Нижний Новгород сегодня ассоциируется не только с промышленностью, развитым туризмом, но и с высокими технологиями. По итогам прошлого года оборот нижегородских ИТ-компаний вырос почти в 1,5 раза и составил более 97 млрд рублей, а доля отечественного ПО в правительстве региона по итогам 2026 года достигнет, по нашим прогнозам, 75%. ЦИПР-2026 – это огромное количество гостей и участников, интересных стендов, продуктивных переговоров и подписаний. Наши ИТ-компании на конференции представили более 50 различных разработок. И самое приятное, что в «открытый день» на площадке достижения отрасли смогли увидеть все желающие».

В рамках конференции крупнейшие технологические компании представили свои **инновационные разработки**. «Группа Астра» объявила о запуске облака Astra Cloud на отечественных 48-ядерных процессорах Baikal-S – первого в России коммерческого облака с полностью российским стеком.

«Ростелеком» презентовал новую стратегию развития до 2030 года с планом выхода на выручку в 1 трлн рублей. Т-Банк провёл первую в России контролируруемую кибератаку на собственную инфраструктуру с помощью ИИ. «Росатом» показал планшет-трансформер ОКО Book 5 Yoga и платформу промышленного ИИ «АтомМайнд 2.0». «РЖД» совместно со спутниковой компанией «Бюро 1440» приступили к оснащению поездов «Сапсан» и «Ласточка» отечественной спутниковой связью. Компания «РТ-Техприёмка» (входит в Госкорпорацию «Ростех») впервые представила платформу PMC TechX 25 Про, предназначенную для централизованного управления промышленными и мобильными роботами, а также производственным оборудованием.

В рамках выставки состоялся конкурс на лучший стенд, по итогам голосования в соцсетях и приложении конференции первое место занял «Ростелеком», второе – «ИКС Холдинг», третье – «Норникель». Победители получили дипломы и фирменный мерч ЦИПР.

С международной миссией конференцию ЦИПР посетили **более 300 иностранных делегатов из 46 стран**, включая Китай, Индию, Бразилию, Сербию, Аргентину и Филиппины. Свои стенды представили 11 иностранных компаний. В этом году на площадке

ЦИПР впервые присутствовала делегация из Республики Зимбабве во главе с **первым вице-президентом Констатино Гувей Домиником Чивенгой**. Губернатор Нижегородской области Глеб Никитин встретился с первым вице-президентом африканской страны и обсудил расширение торгово-экономического и образовательного сотрудничества с Республикой Зимбабве.

На ЦИПР состоялась выставка цифрового искусства **Децентрализованное Цифровое Пространство DeCIPRaland**, которая объединила 35 художников и более 70 произведений из России, Казахстана, Беларуси, Великобритании, Узбекистана, Кипра, Сингапура и Грузии. На открытый конкурс была подана 241 заявка, а цифровой музей посетили 4 200 человек. Также при поддержке Президентской платформы «Россия – страна возможностей» состоялся **онлайн-нейромарафон проекта «Первый кубок нейроконтента»**. Ролики участников проекта были представлены на конференции и демонстрировались на протяжении всех дней мероприятия.

18 мая состоялась церемония награждения деловой премии **ЦИПР Диджитал** за выдающиеся достижения в области цифровых технологий. Среди победителей: «Газпромнефть Цифровые решения» с проектом «Отраслевая ERP-платформа для нефтегазовых и ТЭК-компаний», NtechLab с проектом



«Видеоаналитика с ИИ для поиска пропавших детей», ВТБ с проектом «Новый ВТБ Онлайн», «Газпром нефть» с проектом «Оптимизационное планирование на основе цифровых двойников цепей поставок» и многие другие. Партнёром по информационной безопасности премии и конференции выступила ГК «Солар»: компания отвечала за безопасность голосования и обеспечивала защиту информационных ресурсов ЦИПР от потенциальных кибератак.

Продолжением ЦИПР стал технологический фестиваль «Тех-Френдли Викенд» с лекциями популяризаторов ИТ и концертами, который будет проходить до 23 мая.

Организатором конференции ЦИПР и фестиваля «Тех-Френдли Викенд» является компания «ОМГ». Мероприятие проходит при поддержке Правительства Российской Федерации, Министерства цифрового развития, связи и массовых коммуникаций РФ, Правительства Москвы и Правительства Нижегородской области. Генеральными партнёрами выступили: Госкорпорация «Ростех», Госкорпорация «Росатом», «Ростелеком», Яндекс, Т-Банк, ВЭБ. РФ, ТМХ. ГигаПартнёр: Сбер. Технологический партнёр – группа компаний «ИКС Холдинг».

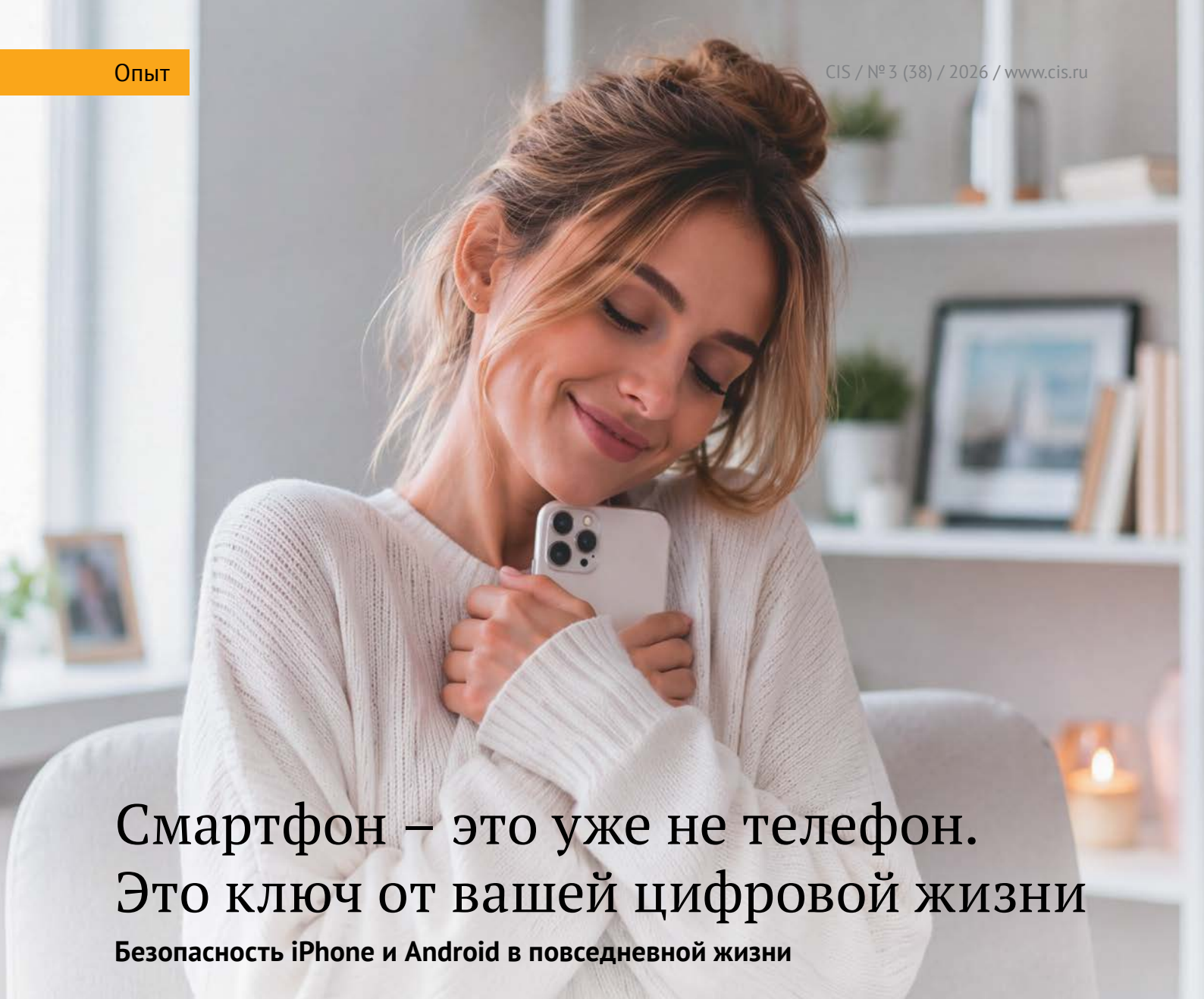
ВИП-партнёрами стали: «Группа Астра», «РЕД СОФТ», корпорация «Га-

лактика», МегаФон Пробизнес, МТС, РТК-ЦОД, ГК Softline, Центр Биометрических Технологий, «АЛМИ Партнёр», ТРАНСНЕФТЬ, компания-разработчик инфраструктурного ПО «Базис», NtechLab, Альфа-Банк, ИРТЕЯ, ГК «Солар», А7А5, «ЕвроХим», «ФосАгро», Правительство Москвы, фирма «1С», СОГАЗ, «Турбо Облако», «Билайн», «Газпром нефть», Группа «Россети», СберТех, Группа Rubytch, CSoft Development, «НАНОСОФТ», ЭР-Телеком Холдинг, Аэрофлот, Группа «Аметист». Новостным интернет-партнёром стал ДЗЕН.

Официальными партнёрами выступили: «Гравитон», «Киберпротект», «САТЕЛ», ГК «Аквариус», «Северсталь», Т8, Global ERP, «АСКОН», ГК «Урбантех», ИТ-экосистема «Лукоморье», «Агропромцифра», «Гознак», Nexign, CommuniGate Pro, «Базальт СПО», «СИБУР», НИУ ВШЭ, Postgres Professional, «СУПЕРТЕЛ», Delta Computers, OCS, ГК InfoWatch, Айтеко, МТС Web Services, Айсорс, «Норникель», Just AI, «РусГидро», Naumen, Группа компаний «Калашников», «КАМАЗ», Navio, P7, «Руцентр», международный аэропорт Шереметьево, VK, ICL Техно, ИТ-холдинг Т1, ПСБ, ГК «Катюша», «Топ Системы», Selectel, «Флант», «АльфаСтрахование», «Корпорация Робототехники», «АйСи Тех», РЖД, Группа «РОСНАНО», «Сигналтек», «Полюс». Пар-

тнёрами панельной дискуссии стали: «Лаборатория Касперского», Cloud.ru, МГТУ им. Н.Э. Баумана, «Инфосистемы Джет», «Атомдата-Интеграция», «Новые башни», Московская школа управления СКОЛКОВО, «СберМобайл», «Газпромбанк». Партнёрами – ИК «ФИНАМ», Тверская область, Эрливидео, ИТ-Элемент29, ЭКСАРА. Партнёром сайта стал «ДиаСофт». Партнёр ИИ чат-бота – Fork Tech. Партнёрами уличной зоны – SOLLERS, «Инферит Безопасность», «Самокат», «Турбо», VVP Group.

Экспонентами выступили: 1С-Парус, Cudy, WowNet, «Труконф», «Тераплан», Космическая связь, NEIMARKER, БИТ «Мастер», Frisbee, CESCO, ФОРС, Контроль ИТ, iSpring, CodeInside, «Береста ПК», Ideco, GRAMAX, «Мобиус Технологии», «Нейроинженер», DCLLogic, MORION, АРПП «Отечественный софт» («Юзергейт», «Искра Технологии», «Газинформсервис», «Аладдин», «Атомик Софт»), СТМ Лабс, Content AI, AXENIX, AggreGate, «Петровайзер Софт», «ГЕРС Технолоджи», «Инвентив ДЛМ», «Ринго», ГК «Юзтех», «Айкон», «КАДАИТЕК», «Вангард софт», Фонд «Сколково», Ижевский радиозавод, Эльбрус-2000, ITKey, MFASOFT, СберСервис, «Экспертика», SIGNAL, МГТУ «СТАНКИН», Meril. Бизнес-партнёрами стали: FishStat, Lamoda, MasterSCADA.



Смартфон – это уже не телефон. Это ключ от вашей цифровой жизни

Безопасность iPhone и Android в повседневной жизни

Ещё десять-пятнадцать лет назад потеря мобильного телефона означала лишь необходимость купить новый аппарат, восстановить SIM-карту и заново сохранить контакты. Конечно, было неприятно лишиться дорогого устройства, но последствия редко выходили за рамки финансовых потерь. Сегодня ситуация изменилась настолько радикально, что сам смартфон зачастую представляет для преступников значительно меньшую ценность, чем информация, которая в нём хранится.

Современный телефон давно перестал быть средством связи. Фактически это цифровой паспорт человека. Через него подтверждаются банковские операции, оплачиваются покупки, подписываются документы, ведётся деловая переписка, хранятся личные фотографии, медицинские документы, корпоративные данные, электронные ключи, криптовалютные кошельки и доступ к десяткам сервисов. Одно устройство объединяет практически всю цифровую жизнь владельца.

Именно поэтому в последние годы произошла серьёзная трансформация киберпреступности. Если раньше злоумышленники старались украсть сам телефон, то сегодня главной целью становится получение доступа к аккаунтам пользователя. Стоимость украденного смартфона может составлять несколько десятков тысяч рублей, а успешный захват цифровой

личности иногда приносит преступникам суммы в сотни раз больше.

Особенно тревожит тот факт, что многие владельцы дорогих смартфонов по-прежнему считают себя защищёнными только потому, что пользуются известным брендом. Владельцы iPhone уверены, что их устройство невозможно взломать благодаря закрытой экосистеме Apple. Пользователи Android нередко полагаются на антивирусные программы и считают, что этого достаточно. На практике ошибаются обе стороны.

Наибольшую опасность сегодня представляет вовсе не технический взлом устройства. Большинство успешных атак строится вокруг человеческой психологии. Злоумышленники убеждают человека самостоятельно сообщить код подтверждения, перейти по поддельной ссылке, установить вредоносное приложение или открыть доступ к своим данным. Такой

подход значительно дешевле, проще и эффективнее, чем поиск сложных уязвимостей в современных операционных системах.

Представьте обычную ситуацию. Человек получает сообщение якобы от службы доставки. В нём говорится, что курьер не смог вручить посылку и необходимо подтвердить адрес. Ссылка открывает страницу, внешне практически не отличающуюся от официального сайта известной компании. Пользователь вводит номер телефона, затем приходит код подтверждения, который также предлагается указать для проверки личности. Через несколько минут этот же код используется уже не для доставки, а для входа в аккаунт владельца.

Похожим образом работают звонки от имени банка, государственных служб, операторов связи и даже технической поддержки известных компаний. Современные технологии позволяют злоумышленникам подменять номера телефонов, использовать ИИ для создания убедительной речи и получать из открытых источников достаточно информации о потенциальной жертве, чтобы разговор выглядел абсолютно правдоподобным.

Особенно активно преступники используют утечки персональных данных. За последние годы в открытом доступе оказались миллионы записей с номерами телефонов, адресами электронной почты и другой информацией пользователей. Обладая такими сведениями, мошенник начинает разговор уже не с общих фраз, а обращается по имени, знает город проживания, иногда место работы и даже последние покупки. У человека возникает ложное ощущение, что звонит действительно представитель знакомой организации.

Сами смартфоны за это время стали значительно безопаснее. И Apple, и Google ежегодно усиливают механизмы защиты своих операционных систем. Современные процессоры содержат отдельные защищённые области памяти для хранения криптографических ключей, данные автоматически шифруются, а биометрическая аутентификация стала значительно надёжнее. Однако все эти технологии бессильны, если пользователь добровольно передаёт злоумышленнику необходимую информацию.

Почему преступникам нужны именно аккаунты

Если раньше украденный телефон можно было быстро продать на вторичном рынке, то сегодня всё чаще встречаются устройства, защищённые настолько хорошо, что использовать их после кражи практически невозможно.

Например, iPhone уже много лет привязан к учётной записи Apple ID. Даже после полного стирания памяти устройство требует данные прежнего владельца для повторной активации. Аналогичный механизм Factory Reset Protection существует и в Android. После сброса настроек система просит войти в тот Google-аккаунт, который был привязан к устройству до удаления данных.

В результате цена украденного смартфона для преступников значительно снизилась. Разобрать его на запчасти можно, но заработать на этом намного сложнее, чем раньше.

Зато доступ к аккаунтам открывает совершенно другие возможности.

Через учётную запись электронной почты можно восстановить пароли большинства интернет-сервисов. Получив контроль над почтой, злоумышленник постепенно получает доступ к социальным сетям, облачным хранилищам, интернет-магазинам, рабочим сервисам и мессенджерам. Если к телефону привязаны банковские приложения, последствия могут стать ещё серьёзнее.

Отдельную ценность представляют облачные хранилища. Многие пользователи автоматически сохраняют в них копии документов, фотографии паспортов, свидетельств, договоров, налоговой отчётности и других конфиденциальных материалов. Иногда именно облачный архив содержит больше информации о владельце, чем сам телефон.

Не менее привлекательны корпоративные данные. Один потерянный смартфон сотрудника способен открыть доступ к внутренней переписке компании, рабочим чатам, VPN-подключениям, системам электронного документооборота и коммерческой информации. Именно поэтому современные требования информационной безопасности всё чаще распространяются не только на компьютеры, но и на мобильные устройства сотрудников.

Телефон могут украсть, даже если он всегда находится у вас в руках

Существует распространённое заблуждение, что опасность возникает только после физической кражи устройства. На самом деле смартфон можно «потерять», не выпуская его из рук.

Достаточно установить приложение из неофициального источника, предоставить ему избыточные разрешения или войти в поддельный сайт под своим Apple ID либо Google-аккаунтом. Формально телефон останется у владельца, но значительная часть информации уже окажется в распоряжении злоумышленников.

Особую угрозу представляют публичные сети Wi-Fi, особенно если пользователь отключает предупреждения системы безопасности или самостоятельно соглашается установить неизвестный сертификат. Несмотря на то что современные сайты используют защищённое соединение HTTPS, некоторые схемы атак до сих пор строятся именно на доверчивости пользователя, а не на недостатках самой технологии.

Не стоит забывать и о так называемом «плечевом сёрфинге». В людных местах злоумышленники могут подсмотреть код разблокировки устройства через плечо владельца, а затем украсть смартфон буквально через несколько минут. Именно поэтому производители начали внедрять специальные режимы защиты украденного устройства, которые мы подробно рассмотрим далее.

Безопасность сегодня начинается не с антивируса

Многие до сих пор считают, что защита смартфона сводится к установке антивирусного приложения. Это наследие эпохи персональных компьютеров, когда большая часть угроз действительно была связана с вредоносными программами.

Современная мобильная безопасность устроена иначе. Основную роль играют встроенные механизмы операционной системы, шифрование данных, защищённое хранение криптографических ключей, двухфакторная аутентификация, биометрия, облачные сервисы поиска устройств и грамотная настройка учётных записей.

Именно поэтому два одинаковых смартфона могут иметь совершенно разный уровень защищённости. Один окажется практически бесполезным для преступников даже после кражи, а другой позволит получить доступ практически ко всей цифровой жизни владельца всего за несколько минут.

И здесь начинается самое интересное. И Apple, и Google за последние годы внедрили десятки функций безопасности, о существовании которых многие пользователи даже не подозревают. Некоторые из них способны полностью сорвать попытку захвата устройства, другие позволяют восстановить данные даже после полной потери телефона, а третьи делают украденный смартфон практически бесполезным для злоумышленников.

Как превратить iPhone в бесполезную добычу для злоумышленника

Если попросить специалистов по информационной безопасности назвать устройство, которое сегодня сложнее всего использовать после кражи, большинство без раздумий ответит – современный iPhone. Причина вовсе не в том, что продукция Apple обладает какой-то «магической» защитой или не подвержена атакам. Просто компания на протяжении многих лет строит экосистему, в которой ценность украденного устройства постепенно стремится к нулю.

Интересно, что многие владельцы iPhone пользуются этой защитой лишь частично. Они знают о Face ID, иногда включают функцию поиска устройства, но при этом оставляют отключёнными несколько механизмов, которые способны полностью изменить развитие событий в случае потери телефона.

Самая распространённая ошибка пользователей заключается в уверенности, что преступник обязательно попытается взломать сам смартфон. На практике всё происходит иначе. Получив устройство, злоумышленник прежде всего анализирует, можно ли заставить владельца самостоятельно сообщить необходимые данные.

За последние годы правоохранительные органы разных стран неоднократно сталкивались с похожей схемой. После кражи телефона вла-

дельцу начинают приходить сообщения якобы от службы поддержки Apple. В письме говорится, что устройство найдено и для его возврата необходимо подтвердить личность. Пользователь переходит по ссылке, вводит данные Apple ID, после чего преступник получает именно то, что ему было нужно. Сам телефон зачастую интересовал его значительно меньше.

Именно поэтому современные механизмы защиты Apple рассчитаны не только на технические атаки, но и на противодействие социальной инженерии.

Face ID – это не просто удобство

Многие воспринимают Face ID исключительно как замену цифровому паролю. На самом деле система выполняет гораздо более серьёзную задачу.

При первом сканировании лица создаётся математическая модель, которая хранится исключительно внутри защищённого сопроцессора Secure Enclave. Ни фотография лица, ни его трёхмерная модель не передаются в облако Apple и не покидают пределы устройства.

Каждый раз при разблокировке смартфона Face ID сравнивает текущее изображение с локально сохранённой моделью. Даже если злоумышленник каким-либо образом получит доступ к резервной копии iPhone, извлечь эти биометрические данные он не сможет.

Современные версии Face ID умеют учитывать возрастные изменения лица, бороду, очки, причёску и многие другие факторы. При этом система остаётся крайне устойчивой к попыткам обмана с помощью фотографий, видео и масок.

Однако существует одна особенность, о которой знают далеко не все владельцы iPhone.

Если устройство оказалось в руках преступника, а ситуация вызывает угрозу вашей безопасности, достаточно одновременно удерживать боковую кнопку и любую кнопку регулировки громкости. После появления экрана выключения питания Face ID автоматически отключается. Следующая разблокировка станет возможна только после ввода цифрового пароля.

Эта функция создавалась именно для ситуаций, когда человека могут попытаться заставить разблокировать устройство при помощи лица.

Почему шестизначного кода уже недостаточно

Когда Apple несколько лет назад перешла с четырёхзначного PIN-кода на шестизначный, уровень защиты значительно вырос. Однако сегодня специалисты рекомендуют идти дальше.

Лучшим решением остаётся полноценный буквенно-цифровой пароль.

Да, вводить его приходится крайне редко благодаря Face ID, зато именно этот пароль становится последним рубежом защиты при невозможности использовать биометрию.

Любопытно, что многие пользователи придумывают сложный пароль для Apple ID, но оставляют максимально простой код разблокировки самого телефона. Между тем именно этот код используется для изменения большинства настроек безопасности устройства.

Украденный iPhone должен перестать доверять своему владельцу

Одним из самых интересных нововведений последних лет стала функция «Защита украденного устройства» (Stolen Device Protection).

Она появилась после того, как преступники начали использовать довольно необычный сценарий. Сначала они наблюдали за человеком в кафе, метро или торговом центре и подсматривали код разблокировки телефона. Затем устройство незаметно похищали.

Казалось бы, пароль известен – значит, защита преодолена. Но Apple решила иначе. Если функция защиты украденного устройства включена, одного знания PIN-кода становится недостаточно. При попытке изменить пароль Apple ID, отключить функцию поиска устройства, просмотреть сохранённые пароли, изменить доверенные номера телефона или выполнить ряд других критически важных действий система потребует обязательную биометрическую аутентификацию.

Если же iPhone находится вне привычных для владельца мест, например не дома и не на работе, перед

выполнением особо важных операций дополнительно запускается таймер безопасности примерно на один час. Этот час может показаться мелочью, однако именно он часто становится решающим. Пока злоумышленник ожидает окончания задержки, настоящий владелец устройством, войдя в свою учётную запись, включить режим пропажи, изменить пароль Apple ID и фактически лишить преступника всех преимуществ.

Поиск устройства работает даже тогда, когда телефон выключен

Для многих пользователей становится неожиданностью, что современные iPhone способны передавать своё местоположение даже после выключения. Конечно, это не означает, что полностью обесточенный телефон продолжает работать. Всё устроено значительно интереснее.

В устройстве остаётся небольшой резерв энергии, достаточный для работы сверхэкономичного беспроводного модуля. Он периодически передаёт специальные зашифрованные идентификаторы. Любой проходящий рядом iPhone, iPad или Mac анонимно принимает этот сигнал и отправляет его в сеть Apple, не зная, кому именно помогает.

Таким образом создаётся огромная распределённая сеть поиска устройств по всему миру. В результате владелец может увидеть примерное местоположение своего телефона даже спустя некоторое время после выключения.

Это одна из самых необычных технологий последних лет, поскольку она использует миллионы чужих устройств без раскрытия личности владельца потерянного телефона, людей, через которых проходит информация.

Что необходимо сделать сразу после покупки iPhone

На практике большинство пользователей начинают задумываться о безопасности только после возникновения проблемы. Между тем правильная настройка занимает меньше получаса.

Первое, что необходимо проверить, – активирована ли функция **«Локатор» (Find My)**. Именно она позволяет определить местоположение

устройства, включить режим пропажи, дистанционно вывести сообщение на экран, заблокировать смартфон или полностью удалить данные, если вернуть его уже невозможно.

Как включить

1. Откройте **Настройки**.
2. Нажмите на **своё имя** вверху экрана.
3. Выберите **Локатор**.
4. Зайдите в **Найти iPhone**.
5. Включите **Найти iPhone**; при желании также включите **Сеть Локатора** и **Последняя геопозиция**.

Как дать доступ близким

1. В приложении **Локатор** откройте вкладку **Люди**.
2. Нажмите **«Поделиться геопозицией»** и выберите контакт.
3. Либо добавьте человека в **Семью** через Apple ID, если хотите постоянный доступ.

Где искать, если телефон потерян

После настройки можно искать iPhone через приложение **«Локатор»** на другом устройстве Apple или через сайт **iCloud Find Devices**.

Следующий шаг – убедиться, что для Apple ID включена двухфакторная аутентификация. Сегодня она активируется автоматически для большинства новых учётных записей, однако владельцам старых аккаунтов стоит проверить её наличие. Благодаря этой функции одного знания пароля недостаточно для входа: потребуется ещё и подтверждение с доверенного устройства или через доверенный номер телефона.

Не менее важно заранее указать несколько способов восстановления доступа к учётной записи. Многие вспоминают об этом только после потери телефона, когда выясняется, что единственный доверенный номер был привязан именно к исчезнувшему устройству. В результате процесс восстановления превращается в длительную процедуру проверки личности.

Apple предлагает добавить резервный доверенный номер телефона и при желании назначить доверенный контакт для восстановления доступа. Если владелец по каким-либо причинам не сможет войти в свою учётную запись, этот человек сможет

помочь подтвердить её восстановление без получения доступа к личным данным.

Резервная копия – страховка, о которой вспоминают слишком поздно

Самый драматичный момент после потери телефона наступает тогда, когда человек понимает: устройство можно купить новое, а фотографии последних десяти лет, рабочие документы, переписка и заметки исчезли навсегда.

Именно поэтому автоматическое резервное копирование в iCloud – не роскошь, а элемент информационной безопасности. Многие ошибочно считают, что резервная копия нужна только на случай поломки телефона. На практике она становится основным способом быстрого восстановления после кражи.

Как проверить

1. Откройте **Настройки**.
2. Нажмите **своё имя**.
3. Зайдите в **iCloud**.
4. Выберите **Резервное копирование в iCloud**.
5. Включите переключатель **Резервное копирование iPhone**.

Если места не хватает

Если iCloud ругается на нехватку места, нужно либо освободить место, либо купить дополнительный объём хранилища iCloud.

Ручная копия

Если нужно сделать бэкап прямо сейчас, в том же разделе нажмите **«Создать резервную копию»**.

Представьте ситуацию: вечером вы потеряли iPhone, а утром приобрели новый. Достаточно войти в свой Apple ID, и спустя некоторое время устройство восстановит приложения, контакты, фотографии, настройки, сообщения, большинство паролей и даже расположение значков на рабочих столах. Для пользователя это выглядит почти как продолжение работы на прежнем телефоне.

Конечно, существуют ограничения. Не все приложения восстанавливают своё содержимое автоматически, а некоторые банковские программы специально требуют повторной авторизации. Это сделано в целях безопасности и является нормальной практикой.

Если телефон всё-таки украл

Главное правило – не пытаться самостоятельно договариваться с преступниками.

В интернете регулярно появляются истории о том, как владельцу предлагают вернуть телефон за вознаграждение, но предварительно просят отключить функцию поиска устройства или удалить его из своей учётной записи. Как только это происходит, смартфон перестаёт быть защищённым Activation Lock и превращается в обычный товар, который можно перепродать.

Именно поэтому удалять устройство из Apple ID следует только тогда, когда вы абсолютно уверены, что больше никогда его не увидите и уже дистанционно стёрли все данные.

Если же телефон действительно потерян, первым делом необходимо воспользоваться сервисом «Локатор» с другого устройства, перевести iPhone в режим пропажи, изменить пароль Apple ID и связаться с оператором связи для блокировки SIM-карты. После этого желательно уведомить банк, если на устройстве были установлены платёжные приложения или использовались электронные кошельки.

Практика показывает, что в большинстве случаев ущерб удаётся свести к минимуму именно тем пользователям, которые заранее настроили все механизмы защиты. Для них потеря телефона превращается скорее в неприятность, чем в катастрофу.

Однако мир Android устроен иначе. Здесь существует огромное количество производителей, различных оболочек и собственных систем безопасности. И вопреки распространённому мнению, современные Android-смартфоны способны обеспечить уровень защиты не ниже iPhone – при условии, что пользователь знает, какие функции необходимо включить.

Android: безопасность, о которой многие до сих пор судят по мифам десятилетней давности

Стоит произнести слова «безопасность Android», как практически всегда находятся люди, которые с уверенностью заявляют: «Настоящая защита есть только у iPhone».

Этот миф оказался удивительно живучим. Он появился ещё в начале 2010-х годов, когда экосистема Android действительно страдала от фрагментации, а некоторые производители месяцами не выпускали обновления безопасности. За прошедшие годы ситуация изменилась настолько сильно, что сравнивать современные версии Android с теми устройствами десятилетней давности уже просто некорректно.

Сегодня флагманские смартфоны на Android используют аппаратное шифрование памяти, защищённые криптографические модули, биометрическую аутентификацию, дистанционную блокировку, облачное резервное копирование и механизмы защиты от сброса настроек. Более того, Google постепенно переносит всё больше компонентов безопасности из прошивки в собственные сервисы, благодаря чему многие защитные функции обновляются независимо от версии операционной системы.

Но есть одно важное отличие от мира Apple. Если экосистема iPhone относительно однородна, то Android представлен десятками производителей, каждый из которых добавляет собственные инструменты защиты. Поэтому уровень безопасности зависит не только от Google, но и от компании, выпустившей устройство.

Самая важная защита Android работает ещё до загрузки системы

Многие пользователи считают, что смартфон начинает защищать данные только после ввода пароля. На самом деле всё начинается значительно раньше.

При первом включении современного Android-устройства автоматически создаются криптографические ключи шифрования, которые хранятся в специальном аппаратном модуле безопасности. У Google он называется Titan M (или Titan M2 на более новых устройствах Pixel), у Samsung используется защищённая среда Knox Vault, а другие производители применяют аналогичные решения.

Это означает, что даже если злоумышленник физически извлечёт микросхему памяти из телефона и подключит её к специализированному оборудованию, он увидит

лишь набор зашифрованных данных. Без аппаратных ключей, которые никогда не покидают защищённый модуль, эта информация бесполезна. Подобные технологии раньше использовались только в корпоративных системах хранения информации. Сегодня они стали стандартом для миллионов обычных пользователей.

Почему сброс телефона уже давно не помогает преступникам

Когда-то украденный Android-смартфон можно было легко вернуть к заводским настройкам и использовать как новый. Именно поэтому старые модели пользовались спросом на чёрном рынке.

Ситуацию изменила технология Factory Reset Protection (FRP), которая стала обязательной частью Android. Её принцип достаточно прост. Если устройство было сброшено без предварительного удаления Google-аккаунта владельцем, при следующем запуске система попросит войти именно под той учётной записью, которая использовалась до сброса. Без этих данных пользоваться устройством не получится.

На практике это резко снизило привлекательность краж современных Android-смартфонов. Да, существуют специализированные способы обхода защиты для отдельных моделей, но они становятся всё менее эффективными, а производители регулярно закрывают подобные уязвимости обновлениями безопасности.

Искусственный интеллект начинает защищать владельца

Одной из самых интересных функций последних поколений Android стала Theft Detection Lock – интеллектуальная защита от кражи.

Представьте обычную ситуацию. Человек идёт по улице, держит телефон в руке, и внезапно злоумышленник выхватывает устройство и убегает. Раньше у преступника появлялось несколько минут, чтобы отключить связь, изменить настройки безопасности или перевести смартфон в авиарежим.

Теперь система анализирует движения устройства с помощью встроенных датчиков и алгоритмов машинного обучения. Если она распознаёт

характерный сценарий резкого выхватывания телефона и последующего быстрого перемещения, экран автоматически блокируется практически мгновенно.

Конечно, технология не гарантирует стопроцентную защиту, однако она значительно сокращает время, которое преступник может использовать для получения доступа к данным. Интересно, что пользователь обычно даже не замечает работу этой функции. Она активируется только при обнаружении характерного поведения, похожего на кражу.

Find My Device стал значительно умнее

Долгое время сервис поиска устройств Google воспринимался как упрощённая версия аналогичного решения Apple. Однако последние обновления заметно изменили ситуацию.

Современная сеть Find My Device использует принцип коллективного поиска, похожий на тот, что применяется в экосистеме Apple. Если потерянный смартфон находится рядом с другими Android-устройствами, они помогают определить его местоположение, передавая анонимные зашифрованные сигналы через инфраструктуру Google. При этом владельцы этих устройств не знают, что помогают искать чужой телефон, а сама компания не получает информации о личности участников процесса. В результате вероятность обнаружить потерянный смартфон существенно возрастает даже в том случае, если он уже не подключён к мобильной сети.

Через сервис поиска можно удалённо заблокировать устройство, вывести сообщение с просьбой вернуть телефон, воспроизвести звуковой сигнал или полностью стереть данные. Именно поэтому функцию поиска рекомендуется включать сразу после первого запуска смартфона.

Samsung Knox – защита, пришедшая из корпоративного мира

Если говорить о безопасности Android, невозможно обойти стороной Samsung Knox. Первоначально эта технология создавалась для государственных организаций, банков и крупных корпораций. Позже многие её элементы стали доступны обычным пользователям.

Knox представляет собой не одно приложение, а целый комплекс защитных механизмов. Во время каждой загрузки устройства система проверяет целостность программного обеспечения. Если обнаруживаются признаки вмешательства в прошивку, пользователь получает предупреждение.

Отдельно защищаются криптографические ключи, биометрические данные и платёжная информация. На некоторых моделях реализована защищённая папка Secure Folder, позволяющая хранить документы, фотографии и приложения в полностью изолированной среде с отдельной аутентификацией. Фактически внутри одного телефона создаётся ещё один защищённый смартфон.

Для многих пользователей это оказывается гораздо полезнее, чем кажется на первый взгляд. Например, рабочие документы можно полностью отделить от личных данных, а доступ к ним защитить дополнительным паролем.

Нужно ли устанавливать антивирус?

Это один из самых частых вопросов, который задают специалисты по информационной безопасности. Ответ не столь однозначен, как несколько лет назад.

Если смартфон используется в обычном режиме, приложения устанавливаются исключительно из официального магазина Google Play, а система регулярно получает обновления безопасности, необходимость в отдельном антивирусе значительно ниже, чем во времена Android 4 или Android 5.

Google уже встроила в систему сервис Play Protect. Он автоматически проверяет приложения до установки, периодически повторно анализирует уже установленные программы и способен удалённо отключать известное вредоносное программное обеспечение.

Конечно, специализированные антивирусные решения по-прежнему востребованы в корпоративной среде или при использовании нестандартных сценариев работы. Но для большинства пользователей куда важнее соблюдать цифровую гигиену, чем устанавливать сразу несколько программ защиты.

Практика показывает, что подавляющее большинство успешных атак начинается вовсе не с вируса. Пользователь сам выдаёт приложению опасные разрешения, переходит по мошеннической ссылке или устанавливает программу из сомнительного источника.

Самая опасная кнопка в Android

Парадоксально, но одной из наиболее рискованных функций остаётся разрешение устанавливать приложения из неизвестных источников. Изначально эта возможность создавалась для разработчиков и корпоративных пользователей, которым необходимо устанавливать внутреннее программное обеспечение без публикации в магазине приложений. Однако именно через такие программы распространяется значительная часть мобильного вредоносного кода.

Современные версии Android требуют отдельного подтверждения для каждой программы, которая пытается установить стороннее приложение. Это серьёзно повысило безопасность по сравнению с прошлым, но полностью проблему не устранило.

Если вам присылают APK-файл в мессенджере с предложением «обновить банковское приложение», «получить бесплатную подписку» или «ускорить телефон», практически всегда речь идёт о попытке мошенничества. Ни один крупный банк не распространяет свои мобильные приложения подобным способом без предварительного информирования клиентов.

Безопасность – это не только настройки

Даже идеально настроенный Android не сможет защитить владельца, если тот добровольно передаст преступникам одноразовый код подтверждения или разрешит удалённый доступ к своему устройству.

Именно поэтому Google постепенно развивает не только технические механизмы защиты, но и системы обнаружения мошеннических действий. Современные версии Android предупреждают пользователя о подозрительных звонках, потенциально опасных ссылках и необычных запросах на предоставление разрешений. Однако никакая технология не заменит внимательности самого владельца.

Практически каждая крупная атака последних лет строилась вокруг доверия человека. Злоумышленники убеждали установить «обновление безопасности», подтвердить личность, пройти проверку или срочно отменить несуществующую операцию. Телефон оставался технически защищённым, но пользователь собственноручно открывал дверь злоумышленнику.

К счастью, даже если устройство потеряно, украдено или пароль оказался забыт, это ещё не означает потерю всей цифровой жизни. Современные облачные сервисы позволяют восстановить доступ практически ко всем данным при условии, что необходимые меры были приняты заранее.

Потеря телефона – ещё не потеря данных

Есть одна фраза, которую специалисты по информационной безопасности любят повторять начинающим системным администраторам: «Компьютер можно заменить за один день, данные иногда невозможно восстановить никогда». Сегодня то же самое можно сказать и о смартфонах. Их стоимость продолжает расти, но ценность самого устройства всё чаще оказывается несопоставимой со стоимостью информации, которую оно хранит.

Парадоксально, но именно в первые минуты после потери телефона большинство пользователей совершают ошибки, которые затем уже невозможно исправить. Одни пытаются часами дозваниваться на пропавший аппарат, надеясь, что его поднимет добросовестный человек. Другие начинают переписываться с теми, кто якобы нашёл устройство. Третьи просто впадают в панику и не предпринимают никаких действий. Между тем современный смартфон предоставляет владельцу достаточно инструментов, чтобы даже в такой неприятной ситуации сохранить контроль над своей цифровой жизнью.

Главное правило звучит просто: считать потерянный смартфон потенциально скомпрометированным с того момента, как он исчез из поля зрения. Даже если позже окажется, что устройство спокойно лежало между подушками дивана, лучше выполнить лишние проверки, чем упустить момент, когда злоумышленник уже получил доступ к вашим аккаунтам.

Первые тридцать минут после потери

Представим ситуацию. Вы вышли из такси, зашли домой и через несколько минут обнаружили, что телефона нет. Возможно, он выпал в машине или остался на кассе магазина, а возможно, его уже держит в руках человек, который вовсе не собирается возвращать находку.

Самая большая ошибка – начинать менять пароли всех сервисов подряд, не понимая, что происходит с самим устройством. Сначала необходимо определить его статус.

Если это iPhone, следует воспользоваться сервисом «Локатор» с другого устройства Apple или через браузер. Владельцы Android могут открыть сервис поиска устройств Google. Если телефон отображается на карте и продолжает передавать координаты, это уже хорошая новость. Значит, устройство ещё находится в сети и может принимать команды.

Следующий шаг – перевод смартфона в режим пропажи. Многие недооценивают эту функцию, считая её обычной блокировкой экрана. На самом деле режим пропажи запускает сразу несколько механизмов защиты. Телефон блокируется, платёжные сервисы перестают работать, на экране появляется сообщение владельца с контактным номером, а информация о перемещениях устройства продолжает передаваться владельцу.

Иногда именно эта функция помогает вернуть смартфон. Бывает, что человек действительно нашёл устройство и готов его отдать, но не знает, кому оно принадлежит. Сообщение на заблокированном экране становится единственным способом связаться с владельцем.

Если же становится понятно, что телефон не удастся вернуть, наступает следующий этап – дистанционное удаление данных. Многие боятся использовать эту функцию, опасаясь потерять фотографии или документы. На самом деле при наличии актуальной резервной копии это решение значительно безопаснее, чем оставлять информацию в руках неизвестного человека.

Почему нельзя сразу удалять устройство из Apple ID или Google-аккаунта

Это ещё одна распространённая ошибка. Некоторые пользователи считают, что раз телефон украден,

его необходимо немедленно удалить из своей учётной записи. На первый взгляд это кажется логичным, однако последствия могут оказаться противоположными ожидаемым.

Пока устройство связано с Apple ID или Google-аккаунтом, оно остаётся защищённым механизмами Activation Lock или Factory Reset Protection. Даже после полного сброса настроек новый пользователь не сможет активировать смартфон без данных прежнего владельца.

Если же удалить устройство из своей учётной записи слишком рано, эта защита исчезнет. Телефон превратится в обычный аппарат, который можно подготовить к продаже.

Именно поэтому специалисты рекомендуют сначала включить режим пропажи, затем при необходимости удалить данные, и только после окончательного понимания, что устройство вернуть невозможно, отвязать его от своей учётной записи.

Не забывайте про SIM-карту

На протяжении многих лет основным способом подтверждения личности оставались SMS-сообщения. Хотя сегодня большинство сервисов постепенно переходит на более безопасные методы двухфакторной аутентификации, мобильный номер по-прежнему играет важную роль.

Если преступник получил доступ к SIM-карте, он может попытаться воспользоваться восстановлением паролей через SMS, зарегистрировать мессенджеры на другом устройстве или подтвердить операции в сервисах, которые ещё используют этот механизм.

Поэтому после потери телефона стоит как можно быстрее связаться с оператором связи и заблокировать SIM-карту. Современные операторы позволяют сделать это через личный кабинет, мобильное приложение, службу поддержки или ближайший офис. Получение новой SIM-карты с сохранением номера обычно занимает считанные минуты, а вот последствия промедления могут оказаться значительно серьёзнее.

Банковские приложения: паника не нужна

Пожалуй, чаще всего после кражи телефона люди переживают именно за деньги. На практике

современные банковские приложения защищены значительно лучше, чем принято считать. Большинство из них требует повторной биометрической проверки или ввода отдельного кода при выполнении важных операций. Даже если преступник разблокировал телефон, это ещё не означает автоматического доступа к банковскому счёту. Тем не менее уведомить банк всё же необходимо.

Практически все крупные банки имеют круглосуточные службы поддержки, которые способны временно ограничить доступ к мобильному приложению, отключить цифровые карты или усилить контроль подозрительных операций. Особенно важно сделать это, если телефон был разблокирован в момент исчезновения или злоумышленник мог видеть пароль разблокировки.

А если забыт пароль?

Иногда устройство не украдено, не потеряно, а просто перестало пускать владельца внутрь. Причиной может стать забытый пароль, неудачная смена кода или длительный перерыв в использовании телефона. Именно здесь становится понятно, насколько важно заранее подготовиться к подобной ситуации.

В случае с Apple основным инструментом восстановления остаётся Apple ID. Если учётная запись настроена правильно, владелец может инициировать процедуру восстановления доступа. В некоторых случаях потребуется подтвердить личность через доверенное устройство или доверенный номер телефона. Если такой возможности нет, запускается процесс проверки личности, который может занять некоторое время. Это неудобно, но именно так система защищает пользователя от попыток захвата аккаунта посторонними.

Google использует похожий подход. Для восстановления доступа могут использоваться резервный адрес электронной почты, доверенное устройство, подтверждение через другое ранее авторизованное оборудование или дополнительные сведения о владельце.

Многие пользователи воспринимают эти вопросы как лишнюю формальность. На самом деле именно они нередко становятся

единственным способом доказать, что аккаунт действительно принадлежит вам.

Кто действительно может помочь

После кражи телефона некоторые начинают искать «волшебные программы», обещающие удалённо взломать устройство, определить его точное местоположение или самостоятельно вернуть доступ к данным. Подобные предложения регулярно появляются в интернете и почти всегда оказываются мошенничеством. В действительности круг организаций, которые действительно способны помочь, довольно ограничен.

Производитель устройства помогает восстановить доступ к учётной записи и объясняет, как воспользоваться встроенными средствами защиты. Оператор связи блокирует SIM-карту и выпускает новую. Банк контролирует безопасность финансовых сервисов.

Правоохранительные органы принимают заявление о краже и могут использовать серийный номер или IMEI в рамках расследования. Если устройство принадлежало работодателю, необходимо как можно быстрее уведомить ИТ-службу компании. Во многих организациях корпоративные смартфоны подключены к системам централизованного управления, позволяющим удалённо заблокировать или полностью очистить устройство.

Во всех остальных случаях обещания «разблокировать украденный iPhone за пять минут» или «обойти защиту любого Android» чаще всего заканчиваются потерей денег.

Безопасность – это привычка

За годы работы с инцидентами информационной безопасности всё чаще прослеживается одна закономерность. Люди редко становятся жертвами из-за недостатков современных технологий. Значительно чаще причиной оказывается уверенность, что неприятности происходят с кем угодно, только не с ними.

Кто-то годами откладывает включение резервного копирования. Кто-то использует один и тот же пароль для десятков сервисов. Кто-то хранит фотографию паспорта в открытой галерее, а код от банковской карты –

в записках телефона без какой-либо защиты. До первого серьёзного инцидента всё это кажется мелочами.

Современные iPhone и Android-смартфоны умеют защищать данные значительно лучше, чем большинство пользователей предполагает. Они автоматически шифруют память, используют защищённые аппаратные модули, умеют искать потерянные устройства, восстанавливать информацию из облака, блокировать подозрительные действия и противостоять попыткам несанкционированного доступа. Но даже самая совершенная технология не способна заменить здравый смысл владельца.

Информационная безопасность давно перестала быть делом исключительно системных администраторов и специалистов по кибербезопасности. Сегодня она касается каждого человека, который хотя бы раз входил в интернет-банк, фотографировал паспорт для оформления документов, переписывался с коллегами в корпоративном мессенджере или хранил семейные фотографии в облаке.

Смартфон стал главным ключом к нашей цифровой личности. И задача владельца заключается не только в том, чтобы купить современное устройство, но и в том, чтобы научиться пользоваться всеми возможностями его защиты. Потратить на настройку безопасности полчаса значительно проще, чем затем месяцами восстанавливать доступ к аккаунтам, менять документы, перевыпускать банковские карты и объяснять друзьям, почему от вашего имени кто-то просит срочно перевести деньги.

Технологии продолжают развиваться, и вместе с ними совершенствуются методы злоумышленников. Однако в этом противостоянии у обычного пользователя есть серьёзное преимущество. Производители смартфонов уже создали большинство инструментов, необходимых для защиты данных. Осталось лишь не забыть ими воспользоваться до того момента, когда они действительно понадобятся.

Когда однажды нас спросят, чего достигло наше поколение



История обладает удивительной особенностью: она почти никогда не предупреждает современников о том, что именно в этот момент они становятся свидетелями рождения новой эпохи.

Великие перемены редко входят в жизнь с торжественными фанфарами. Чаще они появляются как очередное инженерное решение, удачная научная гипотеза, новая машина, странный прибор или программа, возможности которой сначала кажутся полезными, но ещё не судьбоносными.

Только спустя десятилетия становится ясно, что за внешне технической новинкой скрывался перелом, после которого человечество уже не могло жить по-старому. Жители Европы XV века видели в печатном станке Иоганна Гутенберга прежде всего ремесленное изобретение, а не начало новой информационной цивилизации. Первые паровые машины создавались для вполне практических задач и не сразу воспринимались как начало промышленной революции. Опыты Майкла Фарадея с электромагнетизмом были частью науки своего времени, но именно из них вырос мир, пронизанный электричеством. Даже космическая эра, ставшая главным символом XX века, начиналась не как красивый исторический миф, а как тяжёлая инженерная работа, полная расчётов, испытаний, неудач и решений, каждое из которых по отдельности казалось всего лишь очередной технической задачей.

Так устроена история: она почти никогда не запоминает подробности в том виде, в каком они волновали современников. Через столетия редко кто будет обсуждать характеристики конкретных устройств, версии программного обеспечения, скорость процессоров или названия сервисов, которые сегодня кажутся нам важнейшими признаками прогресса. История выбирает другое. Она оставляет в памяти те моменты, когда менялась сама траектория цивилизации. Поэтому, если попытаться мысленно перенестись на несколько столетий вперёд и открыть учебник о начале XXI века, возникает вопрос: что именно будущие историки назовут главным достижением нашего времени? Смартфоны? Социальные сети? Облачные платформы? Электронную коммерцию? Всё это, безусловно, изменило повседневную жизнь, но едва ли станет главной темой эпохи. Гораздо вероятнее, что они напишут о другом: именно в начале XXI века человечество впервые создало искусственный интеллект, который перестал быть лабораторной гипотезой и стал повседневным инструментом миллионов людей.

Вопрос, который однажды неизбежно прозвучит, будет не о том, какими телефонами мы пользовались и какие операционные системы устанавливали. Он будет гораздо проще и од-

новременно гораздо строже: какую невозможную задачу решало наше поколение? Каждое великое поколение получает такую задачу. Одним пришлось научиться пересекать океаны, другим – построить промышленный мир, третьим – подняться в небо, поколению середины XX века – вывести человека за пределы Земли. Нашему поколению достался иной вызов. Ему выпало приблизиться к вопросу, который тысячелетиями принадлежал философии, религии, математике и фантастике: можно ли создать систему, способную участвовать в интеллектуальной работе человека? Не просто считать быстрее, хранить больше информации или выполнять заранее заданные команды, а понимать человеческий язык, анализировать знания, помогать искать решения и становиться собеседником в сложной мыслительной деятельности.

Путь к этому моменту был гораздо длиннее, чем кажется при взгляде на последние технологические новости. Сегодня появление новых моделей ИИ воспринимается как стремительная гонка компаний и исследовательских лабораторий, но на самом деле эта история началась задолго до современных дата-центров. Она уходит корнями в первые попытки человека понять природу собственного мышления.

Аристотель, создавая основы формальной логики, не мог знать, что спустя более двух тысяч лет его идеи о правилах рассуждения станут частью интеллектуального фундамента информатики. Лейбниц, мечтавший об универсальном языке рассуждений, при помощи которого споры можно было бы превращать в вычисления, выглядел для своего времени почти фантастом. Гегель рассуждал о развитии разума в истории, не предполагая, что однажды человечество будет обсуждать уже не только разум человека, но и искусственные системы, способные обучаться на накопленном опыте цивилизации. Позже Алан Тьюринг поставил вопрос, который до сих пор остаётся одним из центральных в информатике: может ли машина мыслить? Он предложил смотреть на эту проблему не как на мистическую загадку, а как на научную и инженерную задачу. С этого момента древний философский спор начал постепенно переходить в область математики, кибернетики и программирования.

Писатели-фантасты оказались в этой истории не менее важными участниками, чем учёные. Они редко угадывали конкретные технические решения, но удивительно точно чувствовали направление движения цивилизации. Айзек Азимов понял, что появление разумной машины поставит перед человеком не только инженерные, но и нравственные вопросы. Артур Кларк писал о технологиях, которые при достаточном развитии становятся неотличимы от магии, и сегодня эта мысль звучит почти буквально для человека, впервые разговаривающего с ИИ. Станислав Лем

предупреждал, что искусственный разум вовсе не обязан быть похожим на человеческий, и именно поэтому его природу будет особенно трудно понять. Фантасты не строили нейронные сети, но они подготовили культурное воображение человечества к миру, где машина может быть не только инструментом, но и участником диалога.

Однако между идеей и её воплощением всегда лежит огромная инженерная дистанция. Чтобы искусственный интеллект стал реальностью, человечеству нужно было пройти через всю историю современной вычислительной техники. И здесь особенность нашего поколения становится особенно заметной. Одному поколению довелось прожить путь, который в прежние века занял бы несколько столетий. Многие из тех, кто сегодня работает с интеллектуальными системами, ещё помнят компьютеры, которые не были привычными бытовыми устройствами. Они стояли в машинных залах, требовали особых условий, шумели вентиляторами, мигали индикаторами и запускались не красивой кнопкой на тонком корпусе, а тяжёлым, почти промышленным действием. Кто-то действительно включал вычислительную машину рубильником, слышал характерный металлический звук, ждал, пока оживут блоки питания и раскрутятся накопители. Для молодых специалистов это уже почти музейная сцена, но для части нынешнего поколения это личная профессиональная память.

Не менее символичны рассказы о жёстких дисках объёмом 20 Мб, которые по размерам напоминали небольшую стиральную машину. Сегодня эта цифра кажется смешной: современная фотография со смартфона может занимать больше места. Но тогда 20 Мб были серьёзным ресурсом, а каждый байт имел значение. Программы писались в условиях жёстких ограничений, и эти ограничения формировали особую инженерную культуру. Код начинался не с набора строк, а с размышления. Ошибка в программе на перфокартах могла означать необходимость переделывать физический носитель. Память приходилось экономить, алгоритмы – продумывать, структуру данных – выстраивать заранее. Машина не подстраивалась под человека. Напротив, человек учился говорить с ней на её языке и принимать её суровые правила.

Затем всё начало меняться с такой скоростью, что сами участники процесса не сразу понимали масштаб происходящего. Персональный компьютер вывел вычислительную технику из машинных залов в офисы и дома. Интернет соединил отдельные машины и людей в единое информационное пространство. Электронная почта, поисковые системы, первые сайты, цифровые библиотеки, мобильная связь, смартфоны и облачные вычисления последовательно меняли не только технологии, но и привычки мышления. Каждое из этих достижений воспринималось как самостоятель-

ная революция. Казалось, что персональный компьютер – это и есть вершина цифровой эпохи. Потом казалось, что вершиной стал интернет. Затем таким символом оказался смартфон.

Сегодня, оглядываясь назад, легче увидеть, что все эти революции были ступенями одной лестницы. Персональный компьютер сделал вычисления массовыми, интернет собрал знания в глобальную сеть, смартфон обеспечил постоянный доступ к этой сети, облачные платформы дали вычислительные мощности, без которых обучение современных моделей было бы невозможно. Человечество строило инфраструктуру для технологии, которую ещё не умело создавать.

В этом смысле появление ИИ не было внезапным чудом. Оно стало результатом множества линий развития, которые долго шли параллельно, а затем сошлись в одной точке. Математика дала язык описания, физика и микроэлектроника – аппаратную базу, информатика – алгоритмы, интернет – данные, облачные вычисления – масштаб, а общество – миллиарды людей, готовых взаимодействовать с цифровой средой ежедневно. Никто специально не проектировал всю эту траекторию от рубильника до нейросети. Но история часто развивается именно так: миллионы людей решают локальные задачи, а спустя годы выясняется, что вместе они построили фундамент для события цивилизационного масштаба.

И всё же ИИ отличается от предыдущих технологических революций. Паровая машина усилила физическую силу человека. Автомобиль увеличил скорость передвижения. Самолёт позволил преодолеть расстояния и силу земного притяжения. Телескоп расширил зрение, микроскоп открыл невидимый глазу мир, компьютер ускорил вычисления. ИИ впервые начал усиливать сам процесс мышления. Он не заменяет человека, как иногда опасаются, и не превращает его в пассивного наблюдателя. В лучшем своём проявлении он становится тем же, чем когда-то стали научные приборы: инструментом, который позволяет увидеть больше, рассмотреть сложнее, сопоставить шире и быстрее проверить гипотезу. Он помогает программисту писать и проверять код, врачу – анализировать публикации и снимки, инженеру – проектировать системы, учёному – искать закономерности в данных, журналисту – работать с массивами информации. Это пока первые шаги, и они сопровождаются ошибками, ограничениями и новыми рисками. Но историческое значение технологии определяется не только её первым состоянием, а тем направлением, которое она открывает.

Первый автомобиль уступал лошади по надёжности и скорости на плохой дороге. Первый самолёт находился в воздухе меньше минуты. Первые компьютеры занимали залы и обладали вычислительной мощностью, которую сегодня

превосходят карманные устройства. История не оценивает великие изобретения по их первым образцам. Она оценивает их по тому, куда они привели. Поэтому разговор об искусственном интеллекте не должен сводиться к тому, насколько совершенны сегодняшние модели, как часто они ошибаются и какие ограничения имеют. Эти вопросы важны для практики, но они не отменяют главного: впервые за всю историю человечества интеллект перестал быть исключительно биологической способностью и стал инженерной задачей.

Именно здесь начинается самая сложная часть разговора. Создав ИИ, поколение начала XXI века не просто добавило ещё одну технологию к длинному списку человеческих изобретений – оно изменило механизм появления будущих технологий. До сих пор каждое открытие зависело только от человеческого разума, вооружённого инструментами. Теперь у человека появился инструмент, который сам участвует в интеллектуальной работе. Это не означает, что исследователь, инженер или автор становятся ненужными. Наоборот, роль человека становится ещё ответственнее: нужно формулировать задачи, проверять результаты, понимать контекст, принимать решения, отвечать за последствия. Но сам процесс поиска решений уже меняется. Человечество получило не просто новый инструмент, а новый способ ускорять собственное развитие.

Поэтому вопрос о достижении нашего поколения неизбежно превращается в вопрос о следующем поколении. Если нам выпало превратить многовековую мечту об искусственном разуме в повседневную инженерную реальность, то какую невозможную задачу история поставит перед теми, кто придёт после нас? Достаточно ли им будет создать более совершенный искусственный интеллект? Вероятно, нет. История редко запоминает очередное улучшение уже родившейся идеи. Она запоминает момент, когда невозможное впервые стало возможным. Значит, следующему поколению предстоит искать вершину, которая сегодня кажется столь же далёкой, как когда-то казалась мыслящая машина. Это может быть управляемый термоядерный синтез, радикальное продление человеческой жизни, первые постоянные города за пределами Земли, принципиально новые формы взаимодействия человека и машины, открытия в фундаментальной физике или нечто такое, для чего у нас пока нет даже словаря. Настоящие революции часто приходят не оттуда, откуда их ждут.

Но одно уже ясно: планка поднята очень высоко. Поколение покорителей космоса передало миру доказательство того, что человек способен выйти за пределы своей планеты. Поколение цифровой эпохи передаёт другой рубеж: человек сумел создать систему, которая участвует в работе с его знаниями. Это не соревнование с прошлым и не повод для самодовольства. История не устроена как пьедестал, где одно

поколение занимает место выше другого. Она больше похожа на эстафету. Одни передали нам электричество, радио, вычислительную технику, космос и микроэлектронику. Нашему поколению выпало передать дальше ИИ не как завершение истории, а как новую стартовую линию.

Через несколько десятилетий ИИ, вероятно, перестанет удивлять. Для будущих инженеров, врачей, учёных, преподавателей и школьников он будет таким же естественным элементом среды, каким для нас стали интернет и мобильная связь. Они будут удивляться не тому, что машина умеет анализировать информацию, а тому, что когда-то люди обходились без подобных помощников. Им будет трудно представить программиста, который часами искал ошибку без интеллектуального ассистента, врача, вручную просматривавшего десятки исследований, инженера, работавшего с огромными объёмами документации без системы, способной объяснить, сопоставить и подсказать. Так же сегодня трудно представить работу с перфокартами человеку, выросшему в эпоху облачных сервисов.

И всё же привычность будущего не отменит исторического значения его рождения. Когда через столетия будут писать о начале XXI века, спорить, вероятно, будут о деталях: какие модели стали первыми по-настоящему массовыми, какие компании сыграли ключевую роль, какие ошибки сопровождали раннее развитие технологии, какие социальные и правовые последствия оказались самыми важными. Но едва ли будет спор о главном. Именно этому поколению выпало превратить одну из древнейших философских идей человечества в инженерную реальность. Оно не начало разговор о разуме и не закончило его. Но оно впервые сделало так, что этот разговор перестал быть только человеческим монологом.

Возможно, главным достижением нашего поколения было не только то, что оно научило машину понимать человека. Не менее важно другое: создавая ИИ, человек начал иначе понимать самого себя. Он заново увидел ценность вопроса, ответственности, воображения, сомнения, проверки и смысла. Машина может помочь обработать знания, но именно человек решает, зачем эти знания нужны. Машина может предложить вариант, но именно человек отвечает за выбор. Машина может имитировать рассуждение, но именно человек задаёт направление истории. И если однажды будущие поколения спросят, что оставило после себя наше время, ответ, возможно, уместится в одной фразе: это было поколение, которое изменило представление человечества о собственном разуме.

Невидимые технологии: почему будущее цифровых платежей зависит не только от банков

Как российские инженеры ищут способы сделать оплату быстрее, безопаснее и удобнее для малого бизнеса



Пока покупатель видит QR-код, продавец видит совсем другую картину

Для большинства из нас оплата по QR-коду давно стала привычным действием. Достать смартфон, открыть банковское приложение, навести камеру, подтвердить перевод – весь процесс занимает считанные секунды. Настолько привычные секунды, что мы практически перестали обращать на них внимание.

Так происходит с любой зрелой технологией. Когда она становится удобной для пользователя, её перестают замечать. Именно поэтому многим кажется, что цифровая трансформация платежей уже завершена. Банковские карты работают, Система быстрых платежей развивается, смартфоны есть практически у каждого. Что ещё можно улучшить?

Ответ на этот вопрос редко можно найти в банковских офисах или конференц-залах. Его гораздо проще увидеть ранним утром на городском рынке, в небольшой кофейне у станции метро или в фермерской лавке, где

продавец одновременно взвешивает овощи, отвечает на вопросы покупателей, считает стоимость нескольких товаров и принимает оплату.

Именно здесь цифровые технологии сталкиваются с реальной жизнью.

Со стороны процесс выглядит элементарным. Покупатель выбрал товар, продавец назвал сумму, деньги переведены, покупка завершена. Но, если внимательно посмотреть на действия продавца, становится заметно, что за несколькими секундами оплаты скрывается целая цепочка мелких операций. Нужно быстро подсчитать итоговую стоимость покупки, сформировать QR-код, показать его покупателю, дождаться подтверждения перевода, проверить поступление денег и сразу же переключиться на следующего клиента.

Каждое из этих действий занимает совсем немного времени. Однако в течение рабочего дня они повторяются сотни раз. Именно поэтому даже небольшое неудобство постепенно превращается в фактор, влияющий на ско-

рость обслуживания, комфорт работы продавца и впечатление покупателя.

История инженерии показывает любопытную закономерность. Крупные технологические прорывы далеко не всегда происходят благодаря созданию принципиально новых устройств. Гораздо чаще изменения начинаются с поиска ответа на простой вопрос: **какое действие человек вынужден повторять снова и снова, хотя оно не приносит никакой дополнительной ценности?**

Когда инженеры находят ответ на этот вопрос, появляются решения, которые сначала кажутся незначительными, а спустя несколько лет становятся новой нормой.

Именно таким путём развивались банкоматы, бесконтактные карты, мобильный банкинг и бесконтактная оплата. Пользователи не мечтали о новой технологии как таковой. Они хотели тратить меньше времени на выполнение привычных операций.

Сегодня аналогичный этап переживают и QR-платежи.

QR-код оказался лишь первым шагом

Когда Система быстрых платежей начала активно использовать QR-коды для оплаты товаров и услуг, многие восприняли это как завершённое решение. Действительно, технология позволила отказаться от дорогостоящих терминалов в ряде сценариев, упростила подключение торговых точек и дала предпринимателям дополнительный способ принимать безналичную оплату. Для многих категорий бизнеса этого оказалось вполне достаточно. Однако очень быстро выяснилось, что между возможностью принять платёж и удобством повседневной работы существует заметная разница.

Если стоимость товара фиксирована, задача действительно решается достаточно просто. Покупатель сканирует заранее подготовленный QR-код, подтверждает перевод, продавец получает оплату. Совсем иначе выглядит ситуация там, где цена формируется непосредственно в момент покупки.

Представим обычный рынок. Покупатель просит двести граммов орехов, килограмм огурцов, два килограмма картофеля и пучок зелени. Пока продавец взвешивает товары, итоговая стоимость постепенно меняется. Использовать заранее распечатанный QR-код уже невозможно: требуется сформировать новый, соответствующий конкретной сумме покупки.

Именно такой сценарий описывается в материалах компании «СОВИНТЕГРА» как одна из практических задач малого бизнеса.

На первый взгляд проблема кажется незначительной. Но именно она демонстрирует разницу между технологией, которая **работает**, и технологией, с которой **действительно удобно работать**.

И здесь начинается область, которой долгое время уделяли значительно меньше внимания, чем самим платёжным сервисам. Речь идёт об эргономике цифровой торговли – о том, насколько естественно современные технологии вписываются в привычные действия продавца и покупателя.

Когда смартфон становится лишним звеном

На протяжении последних десяти лет смартфон постепенно превратился в универсальный инструмент предпринимателя. Он заменил фотоаппарат, ежедневник, калькулятор, банковский терминал, средство связи

и даже рабочее место. Логично было предположить, что и приём QR-платежей полностью останется его задачей. На практике оказалось, что универсальность имеет свою цену.

Инженеры давно знают простой принцип: устройство, которое должно выполнять десятки разных функций одновременно, редко оказывается идеальным хотя бы в одной из них. Смартфон прекрасно подходит для формирования QR-кода, но далеко не всегда удобен в роли устройства, которое продавец вынужден постоянно демонстрировать покупателю. Этот нюанс становится очевидным только при наблюдении за реальной работой торговой точки.

Представим небольшую кофейню. Бариста одной рукой готовит напиток, другой принимает заказ, отвечает на вопросы посетителей и следит за очередью. После ввода суммы оплаты он разворачивает экран смартфона к покупателю, ожидает, пока тот считывает QR-код, затем снова берёт телефон в руки и проверяет поступление платежа. Подобная последовательность повторяется десятки, а иногда и сотни раз за смену.

В продуктовом магазине возникает другая ситуация. Продавец работает в ограниченном пространстве за кассой, где каждый предмет имеет своё место. Смартфон приходится постоянно брать в руки, поворачивать экран к покупателю, следить, чтобы устройство не оказалось слишком далеко или слишком близко. В часы пик эти движения становятся частью непрерывного потока действий.

Ещё сложнее обстоят дела на рынках и ярмарках. Здесь продавец одновременно работает с весами, упаковкой, продуктами и деньгами. Смартфон в такой среде превращается в предмет, который приходится постоянно перекладывать, очищать от загрязнений и беречь от случайных повреждений.

Возникает интересный парадокс. Само формирование QR-кода занимает доли секунды. Основное время уходит вовсе не на вычисления, а на организацию взаимодействия между продавцом и покупателем. Именно этот участок процесса редко попадает в поле зрения разработчиков банковских приложений.

Эргономика важнее скорости процессора

Когда говорят о цифровых платежах, чаще всего обсуждают скорость об-

работки транзакций, безопасность передачи данных или банковские комиссии. Между тем в повседневной работе предпринимателя гораздо большее значение имеет эргономика.

- Насколько естественно устройство вписывается в привычный рабочий процесс?
- Нужно ли менять последовательность действий?
- Требуется ли технология дополнительных движений?
- Можно ли пользоваться ею одной рукой?

Эти вопросы могут показаться второстепенными, однако именно они определяют, станет ли новая технология частью ежедневной практики или останется функцией, которой пользуются только при необходимости.

История промышленного дизайна знает множество примеров, когда небольшое изменение конструкции позволяло радикально повысить удобство работы. Иногда достаточно было изменить расположение кнопки, форму ручки или угол наклона дисплея, чтобы устройство стало восприниматься совершенно иначе. Цифровые платежи постепенно приходят тот же путь. Сегодня внимание инженеров смещается с самой транзакции на окружающий её процесс.

Инженерия начинается с наблюдения

Любопытно, что многие удачные инженерные решения рождаются не в лабораториях, а во время наблюдения за пользователями. Разработчик может создать технически безупречное устройство, но только работа в реальных условиях показывает, какие действия человек выполняет автоматически, а какие вызывают раздражение.

В случае QR-платежей таким наблюдением стало понимание простой вещи: покупателю вовсе не нужен смартфон продавца. Ему нужен только QR-код. Это кажется очевидным. Но именно эта мысль позволяет полностью переосмыслить процесс оплаты.

Если отделить отображение QR-кода от смартфона, продавцу больше не придётся разворачивать устройство к покупателю, рисковать его сохранностью или менять привычный порядок работы. Фактически смартфон остаётся инструментом формирования платежа, а взаимодействие с покупателем берёт на себя отдельное устройство.

Именно вокруг этой идеи компания «СОВИНТЕГРА» построила один из своих продуктов – **QR Display**. Это отдельный дисплей с экраном E-Ink, который подключается к смартфону или смарт-кассе по Bluetooth, а для Android также может использовать проводное подключение. После формирования платежа QR-код автоматически выводится на внешний экран, установленный в удобном для покупателя месте. Для интеграции используется библиотека с открытым API, входящая в комплект поставки.

Однако было бы ошибкой воспринимать QR Display только как ещё один аксессуар для смартфона. По сути, перед нами пример инженерского подхода, при котором сложная задача решается не усложнением программного обеспечения, а перераспределением функций между устройствами. Смартфон продолжает выполнять то, для чего подходит лучше всего, – взаимодействовать с банковским приложением. Отдельный дисплей берёт на себя другую задачу – сделать процесс оплаты удобным и для продавца, и для покупателя.

На первый взгляд такое разделение выглядит незначительным. Но именно подобные решения часто становятся основой новой пользовательской привычки. И если QR Display отвечает на вопрос, **как удобнее показать покупателю QR-код**, то следующая разработка компании пытается решить более сложную задачу: **можно ли вообще отказаться от использования смартфона как основного рабочего инструмента продавца при расчёте стоимости покупки?**

Когда калькулятор оказывается умнее смартфона

В мире потребительской электроники давно существует негласное правило: чем больше функций удаётся объединить в одном устройстве, тем успешнее оно выглядит на рынке. Именно поэтому современные смартфоны умеют практически всё – от навигации и видеосъёмки до банковских операций и управления умным домом.

Но профессиональное оборудование развивается по другому принципу.

В медицине врач не заменяет хирургический инструмент смартфоном. На производстве инженер не использует телефон вместо измерительного прибора. В торговле тоже существу-

ют задачи, для которых специализированное устройство оказывается удобнее универсального.

На первый взгляд идея использовать отдельный калькулятор в эпоху смартфонов может показаться неожиданной. Однако, если посмотреть на рабочий день продавца, становится понятно, что калькулятор никуда не исчезал. Во многих небольших магазинах, павильонах и на рынках он по-прежнему остаётся привычным инструментом, позволяющим быстро складывать стоимость нескольких товаров.

Причина проста: во время обслуживания важна не только точность вычислений. Не менее важно, чтобы все действия выполнялись автоматически, без необходимости переключаться между приложениями, экранами и режимами работы.

Именно эту особенность разработчики «СОВИНТЕГРА» положили в основу устройства **QR Calc**.

Не гаджет, а рабочий инструмент

Название QR Calc может создать впечатление, что речь идёт всего лишь о калькуляторе с дополнительной функцией генерации QR-кодов. На самом деле концепция устройства значительно шире.

Разработчики попытались объединить несколько привычных для продавца действий в одну непрерывную последовательность. Сначала рассчитывается стоимость покупки. Затем одним действием формируется запрос на оплату. После этого QR-код автоматически появляется на отдельном дисплее, обращённом к покупателю. Сам продавец при этом продолжает работать так же, как работал раньше.

Это важный момент, который часто остаётся за рамками обсуждения цифровых технологий. Большинство людей привыкает к определённому порядку действий. Чем меньше новая система заставляет менять этот порядок, тем быстрее она становится частью повседневной работы.

QR Calc объединяет функции калькулятора, Bluetooth-модуля и генерации QR-кода, а также работает с выносным дисплеем для покупателей. После расчёта стоимости устройство взаимодействует с мобильным банковским приложением через библиотеку с открытым API и получает QR-код, который выводится на экран.

С инженерной точки зрения здесь интересно не количество функций, а логика их объединения. Фактически QR Calc становится связующим звеном между привычным способом расчёта стоимости и современной инфраструктурой Системы быстрых платежей.

Почему это важно именно для малого бизнеса

Крупные торговые сети могут позволить себе сложные кассовые системы, интеграцию с товароучётным программным обеспечением и дорогостоящие POS-терминалы. Для небольшого бизнеса ситуация выглядит иначе.

Фермерские хозяйства, сезонные ярмарки, торговые островки, небольшие магазины у дома или палатки на рынке часто работают в условиях, где главным требованием становится простота. Чем меньше оборудования необходимо установить и обслуживать, тем легче предпринимателю сосредоточиться на продаже товара. Поэтому развитие платёжных технологий постепенно идёт не только по пути усложнения функциональности, но и по пути уменьшения количества лишних действий.

QR Calc интересен именно этим подходом. Он не предлагает продавцу полностью изменить привычный процесс обслуживания. Наоборот, он старается встроиться в него максимально естественно. Это принцип, который хорошо знаком специалистам по промышленному дизайну: лучшая технология не требует обучения. Она позволяет человеку продолжать работать почти так же, как раньше, лишь избавляя его от повторяющихся операций.

Инженерия повседневности

Существует устойчивое заблуждение, что инновации обязательно должны выглядеть впечатляюще. Огромные сенсорные панели, искусственный интеллект, роботы, дополненная реальность – всё это действительно привлекает внимание. Однако в повседневной жизни гораздо чаще оказываются востребованы решения другого типа. Они не стремятся произвести эффект. Их задача – сделать привычный процесс немного проще.

Именно поэтому многие самые успешные инженерные разработки последних десятилетий кажутся удивительно скромными. Они не меняют профессию человека. Они меняют несколько движений, которые тот выполняет сотни раз в день. В случае QR Calc речь идёт именно об этом.

Устройство не пытается заменить кассовую систему, банковское приложение или смартфон. Оно берёт на себя небольшой, но регулярно повторяющийся участок работы – переход от расчёта стоимости к формированию платежа.

Подобный подход особенно интересен тем, что ориентирован не на абстрактные технологические возможности, а на реальные привычки пользователей.

От устройства – к экосистеме

Если рассматривать QR Display и QR Calc по отдельности, они выглядят как специализированные устройства для приёма платежей. Но, если посмотреть шире, становится заметно другое.

Оба продукта решают одну и ту же задачу – сокращают количество лишних действий между моментом, когда продавец называет сумму покупки, и моментом, когда покупатель подтверждает оплату.

Это уже не разговор о конкретном оборудовании. Это разговор о новой философии проектирования цифровой торговли, в которой внимание уделяется не только банковской инфраструктуре, но и человеку, ежедневно работающему за прилавком.

Именно здесь начинается следующий этап развития технологий. Не там, где появляются новые способы оплаты, а там, где привычные способы становятся настолько удобными, что перестают требовать дополнительных усилий со стороны пользователя.

От удобства к экономике: почему несколько лишних движений имеют значение

Когда говорят о цифровой торговле, чаще всего сравнивают технологии, обсуждают скорость обработки платежей, банковские комиссии, способы интеграции с кассовыми системами или возможности мобильных приложений. Но для предпринимателя, который ежедневно стоит за прилавком, всё это нередко оказывается вторичным. Гораздо важнее другое – насколько естественно технология вписывается в привычный рабочий процесс.

Владелец небольшой торговой точки редко оценивает эффективность своей работы в миллисекундах или количестве обработанных транзакций. Его день складывается из совершенно других вещей: успел ли он обслужить всех покупателей в часы пик, возникла ли очередь, приходилось ли отвлекаться на действия, не связанные с продажей,

были ли ошибки при расчётах или задержки во время оплаты. Именно эти, на первый взгляд, незначительные детали формируют общее впечатление от работы торговой точки.

Цифровые технологии нередко воспринимаются как самостоятельная ценность. Однако в реальной жизни они лишь инструмент. Продавец приходит на работу не для того, чтобы демонстрировать экран смартфона, кассир – не для того, чтобы запускать банковское приложение, а бариста – не ради формирования QR-кодов. Их задача остаётся прежней: быстро, удобно и без лишних усилий обслужить покупателя. Всё остальное должно происходить почти незаметно.

Поэтому сегодня разговор о цифровых платежах постепенно выходит за рамки банковских сервисов. Всё чаще предметом обсуждения становится эргономика – насколько удобно человеку взаимодействовать с технологией в течение всего рабочего дня. Именно здесь проявляется простая закономерность: чем меньше действий требует система, тем легче она становится частью повседневной работы.

Инженеры давно знают, что пользователи редко замечают удачные решения. Они обращают внимание только на неудобства. Если продавцу приходится каждый раз брать смартфон в руки, разворачивать его к покупателю, ждать, пока тот считывает QR-код, а затем снова возвращаться к работе, эти несколько секунд постепенно превращаются в сотни одинаковых повторений за смену. Каждое отдельное действие кажется незначительным, но вместе они формируют тот самый опыт взаимодействия с технологией, который определяет, будет ли она восприниматься как помощник или как источник постоянных мелких раздражителей.

Не случайно многие самые успешные инженерные решения последних десятилетий были направлены вовсе не на создание новых возможностей, а на устранение лишних действий. Компьютерная мышь не сделала вычислительную технику мощнее, сенсорный экран не ускорил работу процессора, а бесконтактная банковская карта не изменила саму природу платёжной системы. Все эти решения сделали взаимодействие человека с технологией более естественным. Пользователю стало проще выполнять привычные операции, и именно поэтому они быстро превратились в повседневную норму.

Малый бизнес – самая сложная среда для инженера

Когда речь заходит о цифровизации торговли, воображение чаще всего рисует современные супермаркеты с автоматизированными кассами, электронными ценниками и сложными информационными системами. Однако повседневная торговля значительно разнообразнее. Она состоит из небольших магазинов у дома, фермерских лавок, сезонных ярмарок, рыночных павильонов, кофеен, островных торговых точек, мастерских и множества других предприятий, каждое из которых живёт по собственным правилам.

В таких условиях невозможно создать одно универсальное устройство, одинаково удобное для всех. Где-то особенно важна автономность, где-то – компактность, в одном случае решающее значение имеет простота настройки, в другом – возможность начать работу практически сразу после включения. Именно поэтому развитие оборудования для малого бизнеса идёт по пути специализации. Производители всё чаще стараются не заменить привычные инструменты предпринимателя, а дополнить их, избавив человека от повторяющихся операций, которые не создают дополнительной ценности.

Такой подход прослеживается и в разработках компании «СОВИНТЕГРА». QR Display и QR Calc не требуют перестраивать существующую инфраструктуру Системы быстрых платежей и не предлагают отказаться от банковских приложений. Напротив, они используют уже существующие механизмы взаимодействия через открытый API, стремясь встроиться в привычный рабочий процесс максимально естественно.

На первый взгляд подобные изменения могут показаться небольшими, но именно из таких деталей обычно и складывается повседневное удобство работы. Хорошая инженерия редко начинается с желания создать ещё одно устройство. Чаще всего она начинается с внимательного наблюдения за тем, как человек выполняет свою работу, и с попытки сделать её хотя бы немного проще.

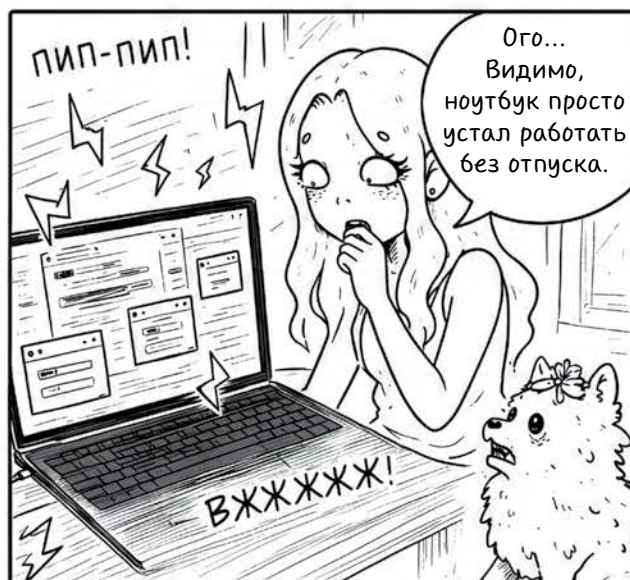


СОВИНТЕГРА

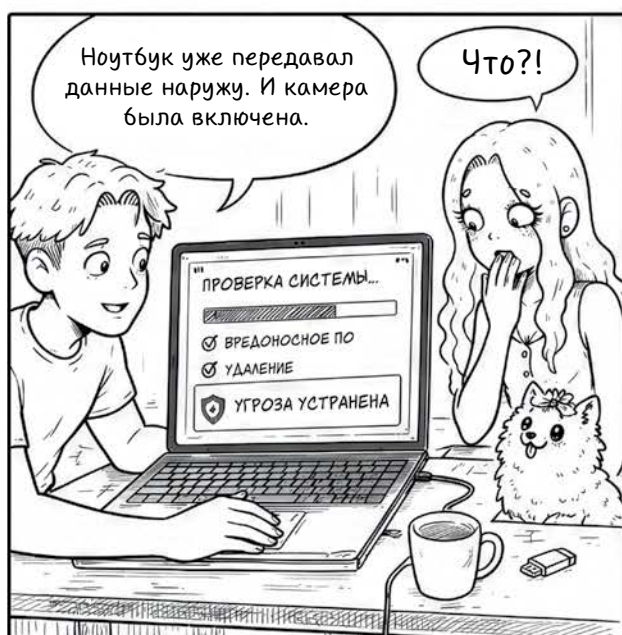
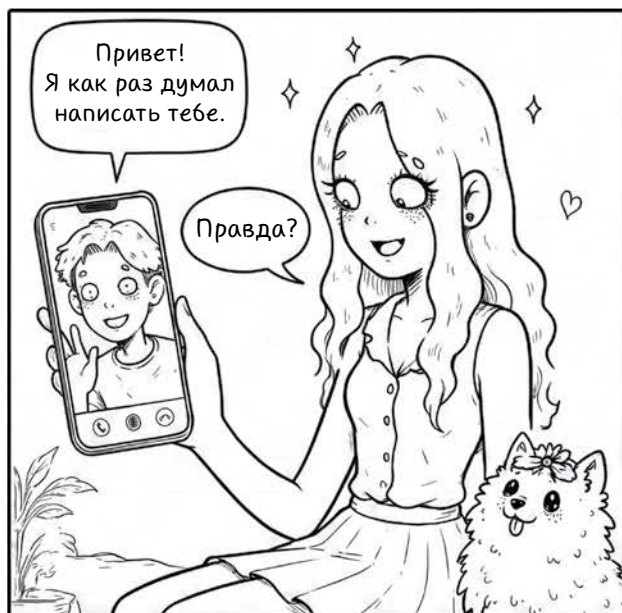
Поставщик и правообладатель решения компания «СОВИНТЕГРА».

sovintegra.ru

Флешка с «сюрпризом»...



...и любопытная Бринти



Осенний бизнес-гороскоп – 2026 для ИТ-компаний

Осень традиционно считается самым насыщенным и ответственным периодом для большинства компаний ИТ-отрасли. После летнего сезона рынок возвращается к высокой деловой активности: возобновляются крупные проекты, увеличиваются корпоративные бюджеты, проходят отраслевые конференции, запускаются новые продукты и начинается подготовка к завершению финансового года. Именно осенью многие организации подводят промежуточные итоги, корректируют стратегию развития и принимают решения, которые будут определять их успех в 2027 году.

Осень 2026 года обещает быть особенно динамичной. Искусственный интеллект продолжит проникать практически во все направления бизнеса, возрастет роль информационной безопасности, цифровой трансформации и автоматизации процессов. Компании будут активнее конкурировать за квалифицированных специалистов, а заказчики станут ещё более требовательными к качеству, скорости внедрения и экономической эффективности ИТ-решений.

Этот гороскоп создан специально для компаний ИТ-сферы, основанных под разными знаками зодиака. Он носит развлекательный характер, однако многие рекомендации вполне могут оказаться полезными для стратегического планирования бизнеса.

♈ Овен

21 марта – 20 апреля

Состояние компании

Осень станет для компании периодом высокой деловой активности. Руководство почувствует желание ускорить развитие, вывести на рынок новые продукты и опередить конкурентов. В коллективе возрастет мотивация, однако вместе с ней увеличится нагрузка на сотрудников. Некоторые подразделения могут работать практически на пределе возможностей, особенно если летом были начаты масштабные проекты.

Компания будет привлекать внимание потенциальных клиентов своей энергией, смелыми решениями и готовностью быстро реагировать на изменения рынка. Главное – не позволить скорости снизить качество конечного продукта.

Состояние бизнеса и рынка

Рынок ИТ продолжит активно развиваться, но конкуренция заметно усилится. Особенно востребованными окажутся решения в сфере ИИ, кибербезопасности, автоматизации бизнес-процессов и корпоративного программного обеспечения. Осенью возможны крупные тендеры и долгосрочные контракты, в которых преимущество получают компании с хорошей репутацией и готовыми кейсами.

Рекомендации для руководства

Используйте осенний период для уверенного роста, но не принимайте стратегические решения исключительно на эмоциональном подъёме. Перед запуском новых направлений проведите дополнительный анализ рынка и оцените реальные возможности команды. Осенью особенно важно соблюдать баланс между амбициями и ресурсами компании.

Рекомендации для команды

Проявляйте инициативу, но не забывайте о дисциплине. Это хорошее время для освоения новых технологий, участия в корпоративном обучении и обмена опытом между подразделениями. Высокая организованность позволит успешно справиться даже с самыми сложными задачами.

♉ Телец

21 апреля – 20 мая

Состояние компании

Осенью компания будет чувствовать себя уверенно благодаря накопленному опыту и стабильной клиентской базе. Организация сможет избежать резких потрясений даже в условиях меняющейся рыночной конъюнктуры. Особенно хорошо проявят себя компании, которые заранее подготовились к осеннему деловому сезону.

Состояние бизнеса и рынка

Заказчики будут более внимательно относиться к выбору подрядчиков. На первый план выйдут надёжность, качество исполнения проектов и долгосрочные гарантии. Компании, сумевшие заслужить доверие клиентов, получают значительное преимущество.

Рекомендации для руководства

Осень идеально подходит для укрепления финансовой устойчивости бизнеса. Стоит уделить внимание оптимизации расходов, развитию постоянных клиентов и совершенствованию внутренних процессов. Не следует рисковать инвестициями без детальной оценки потенциальной отдачи.

Рекомендации для команды

Ваша внимательность и профессионализм станут важнейшим ресурсом компании. Не бойтесь брать ответственность за сложные проекты – именно они помогут раскрыть ваш потенциал.

II Близнецы

21 мая – 21 июня**Состояние компании**

Осень окажется чрезвычайно насыщенной переговорами, конференциями, деловыми встречами и новыми знакомствами. Компания может получить сразу несколько интересных предложений о сотрудничестве, однако далеко не каждое из них окажется одинаково выгодным.

Состояние бизнеса и рынка

На рынке возрастёт спрос на интеграционные проекты, аналитические платформы, цифровые сервисы и решения, основанные на обработке больших данных. Компании, умеющие быстро адаптироваться, смогут значительно увеличить свою долю рынка.

Рекомендации для руководства

Не стремитесь участвовать одновременно во всех возможных проектах. Лучше сосредоточиться на наиболее перспективных направлениях, где компания действительно обладает сильной экспертизой.

Рекомендации для команды

Общайтесь, учитесь друг у друга и активно делитесь знаниями. Осенью коллективная экспертиза станет значительно ценнее индивидуальных достижений.



Рак

22 июня – 22 июля**Состояние компании**

Осень станет временем укрепления внутренней стабильности. Компания будет уделять больше внимания корпоративной культуре, удержанию сотрудников и развитию управленческой команды. Благодаря этому повысится эффективность взаимодействия между подразделениями.

Состояние бизнеса и рынка

Рынок сохранит высокий уровень активности, однако заказчики будут отдавать предпочтение компаниям, способным обеспечить долгосрочную поддержку проектов и высокий уровень сервиса.

Рекомендации для руководства

Инвестируйте в людей. Осенью именно сильная команда станет главным конкурентным преимуществом компании. Полезными окажутся программы наставничества, обучение и развитие кадрового резерва.

Рекомендации для команды

Будьте готовы помогать коллегам и делиться опытом. Совместная работа позволит успешно завершить даже самые масштабные проекты.



Лев

23 июля – 23 августа**Состояние компании**

Осенью компания окажется в центре внимания профессионального сообщества. Высока вероятность успешного участия в конкурсах, отраслевых премиях, крупных выставках и конференциях. Организация сможет значительно укрепить свой бренд.

Состояние бизнеса и рынка

Клиенты будут всё чаще выбирать компании с сильной публичной репутацией и подтверждённой экспертизой. Повысится значение личного бренда руководителей и технических специалистов.

Рекомендации для руководства

Активнее выступайте на конференциях, публикуйте исследования, рассказывайте об успешных проектах. Осень благоприятствует развитию бренда работодателя и укреплению доверия со стороны рынка.

Рекомендации для команды

Не бойтесь публичности. Участие в профессиональных мероприятиях поможет не только компании, но и вашему карьерному развитию.

**Дева**

24 августа – 23 сентября

Состояние компании

Компания сосредоточится на совершенствовании процессов, повышении качества продуктов и минимизации рисков. Осенью особенно заметными станут результаты работы, выполненной в течение всего года.

Состояние бизнеса и рынка

Клиенты будут ожидать высокой надёжности и безупречного качества. Компании, уделяющие внимание тестированию, безопасности и сопровождению решений, окажутся в наиболее выгодном положении.

Рекомендации для руководства

Настало время провести внутренний аудит процессов, оценить эффективность подразделений и устранить накопившиеся организационные проблемы. Эти действия создадут прочную основу для следующего года.

Рекомендации для команды

Не торопитесь завершать задачи любой ценой. Именно внимательность к деталям поможет избежать серьёзных ошибок и повысить доверие клиентов.

**Весы**

24 сентября – 23 октября

Состояние компании

Осенью компания будет стремиться найти оптимальный баланс между развитием новых направлений и сохранением стабильности существующего бизнеса. Многие решения будут приниматься после длительного анализа и обсуждений.

Состояние бизнеса и рынка

Возрастёт значение стратегических альянсов, совместных разработок и долгосрочных партнёрств. Компании всё чаще будут объединять компетенции для реализации крупных проектов.

Рекомендации для руководства

Уделите максимум внимания переговорам. Осенью могут появиться партнёры, сотрудничество с которыми определит развитие бизнеса на многие годы вперёд.

Рекомендации для команды

Развивайте навыки коммуникации и проектного взаимодействия. Чем лучше вы умеете работать в команде, тем выше будут результаты всей организации.

**Скорпион**

24 октября – 21 ноября

Состояние компании

Осенью возможны серьёзные изменения внутри компании: реструктуризация, запуск новых направлений, изменение продуктовой стратегии или обновление управленческой команды. Несмотря на масштаб преобразований, они откроют новые возможности для роста.

Состояние бизнеса и рынка

Конкуренция станет особенно жёсткой в высокотехнологичных сегментах. Побеждать будут компании, способные быстро адаптироваться и принимать непростые решения.

Рекомендации для руководства

Не бойтесь отказаться от проектов, которые перестали приносить ожидаемый результат. Иногда своевременная оптимизация становится лучшей инвестицией в будущее компании.

Рекомендации для команды

Относитесь к изменениям как к возможности профессионального роста. Осенью гибкость мышления окажется одним из самых ценных качеств сотрудников.

**Стрелец**

23 ноября – 21 декабря

Состояние компании

Осень откроет перед компанией новые перспективы развития. Возможны выходы на новые регионы, расширение линейки продуктов или заключение крупных контрактов. В коллективе будет ощущаться стремление двигаться вперёд и ставить амбициозные цели.

Состояние бизнеса и рынка

Особенно благоприятными окажутся направления, связанные с международным сотрудничеством, облачными технологиями, образовательными платформами и цифровыми сервисами.

Рекомендации для руководства

Сейчас удачный момент для разработки стратегии развития на несколько лет вперёд. Не ограничивайтесь краткосрочными задачами – смотрите шире.

Рекомендации для команды

Не прекращайте обучение. Осенью новые знания и навыки начнут приносить практическую пользу значительно быстрее, чем вы ожидаете.

**Козерог**

22 декабря – 20 января

Состояние компании

Компания продолжит уверенно двигаться к поставленным целям благодаря грамотному планированию и дисциплине. Осенью будут особенно заметны результаты последовательной работы, выполненной в течение года.

Состояние бизнеса и рынка

Даже при высокой конкуренции организация сможет сохранить стабильное положение благодаря профессиональной команде, устойчивым бизнес-процессам и внимательному отношению к клиентам.

Рекомендации для руководства

Не стремитесь к быстрым победам любой ценой. Осень благоприятствует постепенному укреплению бизнеса, развитию компетенций и формированию долгосрочных конкурентных преимуществ.

Рекомендации для команды

Продолжайте соблюдать высокие стандарты качества. Ваш профессионализм станет одним из главных факторов успеха компании.

**Водолей**

21 января – 19 февраля

Состояние компании

Осенью компания станет одним из генераторов инноваций. Новые идеи будут появляться практически постоянно, а некоторые разработки смогут привлечь внимание рынка и потенциальных инвесторов.

Состояние бизнеса и рынка

Высокий спрос сохранится на решения, связанные с ИИ, машинным обучением, цифровыми платформами, автоматизацией и интеллектуальной аналитикой.

Рекомендации для руководства

Поддерживайте культуру экспериментов, но не забывайте оценивать экономическую эффективность каждого нового проекта. Лучшие результаты принесут инновации, решающие реальные задачи клиентов.

Рекомендации для команды

Осваивайте современные технологии, участвуйте в исследовательских проектах и предлагайте собственные идеи. Осенью руководство будет особенно внимательно прислушиваться к инициативным сотрудникам.

**Рыбы**

20 февраля – 20 марта

Состояние компании

Осенью компания сможет лучше понимать потребности своих клиентов и быстрее реагировать на изменения рынка. Усилится внимание к пользовательскому опыту, качеству сервисов и развитию долгосрочных отношений с заказчиками.

Состояние бизнеса и рынка

Наиболее востребованными станут цифровые продукты, которые помогают бизнесу работать быстрее, безопаснее и удобнее. Всё больше клиентов будут выбирать поставщиков, ориентированных не только на технологии, но и на высокий уровень сопровождения.

Рекомендации для руководства

Регулярно собирайте обратную связь от клиентов, анализируйте пожелания пользователей и совершенствуйте продукты. Осенью именно понимание реальных потребностей рынка станет источником новых возможностей.

Рекомендации для команды

Развивайте навыки общения с заказчиками, проектного управления и междокомандного взаимодействия. Ваша способность понимать бизнес клиента станет не менее важной, чем техническая экспертиза.

Учебный Центр

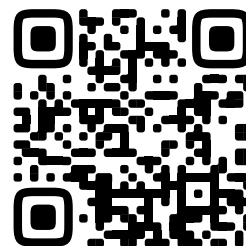
Курсы в сфере
информационных
технологий



Образование в ИТ-сфере

Курсы предназначены для специалистов и компаний, служб безопасности, работающих в сфере защиты информации.

В процессе обучения Вы получите не только теоретические знания, но и комплексные практические навыки по созданию надёжного центра информационной безопасности в своей компании.



cis.ru/courses

Сканворд



Пришлите разгаданный сканворд и ключевое слово
на почту magazine@sovinfosystems.ru до 15-го декабря и получите приз
от редакции ИТ-журнала CIS.



1	1	Актёр... Депардье	3	«И» из кириллицы	Укротитель домомучи- тельниц	Драз- нит быка на арене	Основа- ние, смысл, довод
Восседает на троне		Компью- терный вредитель	Святос- лав, ри- совавший Гималаи	Каждое из 20 тысяч в романе Верна	Золочё- ный оклад иконы	Тот же атом, но с иной массой	Ходок в театр без билета
8	Родной город Аркадия Райкина	Место состатками костра	Небольшой трактир на Кавказе	Группа повозок	Актриса... Зеленая	В матема- тике еди- ничный вектор	
7	Проходная лососевая рыба	Апарта- менты на шести сотках			Роспись по ткани	Единица количества информа- ции	Засасываю- щее прост- ранство
2	«Братья Ка- рамазовы», персонаж	Представ- ление, зрелище		2	Спел арию мистера Икс		
	Брат Гека из рассказа Гайдара	Глава этой се- мьи-крёс- тный отец	Промежудо- чный блок хра- нения данных у компьютера	Лохматый трофей Чингачгука	Обращение к королю Франции	Аукцион- ный товар с молотка	Печатник на поводу у компью- тера
	«Чистый» день Страстной недели	«Вольно- му – воля, спасённому – ...»	Линейное алгебраи- ческое уравнение	4	Выражение, «затёртое до дыр»		
6	Цветок- «звезда»		Угощение на презен- тации				
	Людвиг... Бетховен	И день недели, и место обитания	Бобовое растение	Один из братьев ветров			
	Масло для хри- стианских обрядов	Двухпу- довка для атлета	9	3		3	
			10				

Ключевое слово

NEXTLOT
nextlot.ru

АУКЦИОН ОТ 1 РУБЛЯ!

Площадка NEXTLOT приглашает в эксклюзивный клуб B&D, где участники получают доступ к торгам с минимальным стартом и особыми условиями участия.



Хотите стать участником?

Напишите нам

magazine@sovinfosystems.ru

— откроем доступ
и расскажем подробности.



ТОВАРЫ



УСЛУГИ



ГАДЖЕТЫ



РАЗВЛЕЧЕНИЯ

И МНОГОЕ
ДРУГОЕ