CIS
Современные Информационные Системы
№ 1 (19) / 2022

3 кита инфобеза

Стр. 40

Елена Нагорная

DELL и экология

Стр. 32

Борис Щербаков

Удобно или безопасно?

Стр. 36

Владимир Безмалый

ЭТИКА и искусственный интеллект

Стр. 52

Александр Чесалов

ЭКОНОМИКА

АНАЛИТИКА

ПРОДУКТЫ

РЕШЕНИЯ

ОПЫТ

ТЕХНОЛОГИИ

СОБЫТИЯ

ИТ-ГОРОСКОП

КАЛЕНДАРЬ

КРОССВОРД

От редактора

С каждым днём всё больше новых технологий проникают в нашу жизнь, и без них уже просто немыслимо представить сферу ИТ. Искусственный интеллект не стал исключением, поэтому наша редакция красной нитью вплела эту тему в выпуск, который вы сейчас читаете.

Мы расскажем, какие возникают этические аспекты, связанные с применением искусственного интеллекта, какую роль он играет в цифровой трансформации, какие полезные нагрузки несёт и как помогает человеку, заменяя его в рутинных и сложных операциях. В выпуске поднимем вопрос, как ИИ поможет построить разумную экономику.

Своим мнением с читателями поделятся уважаемые эксперты и друзья ИТ-журнала CIS. Елена Нагорная из компании «Техснабэкспорт» расскажет о «3-х китах» информационной безопасности объектов с государственным участием. Наш друг и эксперт в области ИБ – Владимир Безмалый, который, к великому сожалению, безвременно покинул нас, обратит внимание на парольную защиту, а точнее, на человеческий фактор. Об экологии, технологии и как лидеры ИТ-рынка решают сложные вопросы, связанные с изменением климата, расскажет Борис Щербаков, вице-президент и генеральный директор Dell Technologies в России.

Эти и другие интересные статьи вы найдёте в нашем новом выпуске.

А также мы объявляем о старте одного из самых красивых и ярких событий 2022 года – ИТ-конкурса красоты «Beauty&DigITal-2022». И конечно же приглашаем девушек, работающих с сфере ИТ, принять участие в конкурсе.

Редакция нашего журнала в очередной раз организовала это волшебное мероприятие, чтобы выявить самых красивых и талантливых девушек России и сделать из обладательницы короны символ информационных и цифровых технологий. Участие в конкурсе бесплатное. Заполнить анкету и ознакомиться с условиями конкурса можно на сайте www.cismiss.ru.

С уважением, редакция журнала CIS

Главный редактор: Станислав Понарин.
Директор по маркетингу: Валерия Рябинина.
Корректор: Оксана Макаренко.
Отдел рекламы и распространения: info@sovinfosystems.ru.
Сайт: www.cis.ru, интернер-блог: www.cismag.news.
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: 22-й км Киевского ш., (п. Московский), д. 4, стр. 1, кор. Б, офис 04, блок 904Б, г. Москва, 108811.
Язык: русский.
Периодичность: 4 раза в год (1 раз в квартал).

Фото на обложке: Елена Нагорная.
Тираж 5000 экз. (отпечатанный тираж).
Журнал предназначен для лиц старше 16 лет.

CIS / № 1 (19) / 2022 / www.cis.ru

Помогут ли информационные технологии, искусственный интеллект и квантовая механика построить разумную экономику?

Мы уже писали в журнале CIS о проблемах экономики и путях их преодоления с помощью современных информационных технологий (далее – ИТ), а также искусственного интеллекта (далее – ИИ). Но все попытки найти полное всеобъемлющее решение натыкаются в конечном счёте на отсутствие экономической теории, которая стала бы научной основой построения нового общества, свободного от таких проблем.

Современное общество не может смириться с расточительной, неэффективной и нестабильной экономикой, положением, когда неоправданная погоня за прибылью разрушает окружающую среду, что в результате угрожает будущему человечества.

Но предложить приемлемую модель в рамках существующей рыночной концепции оказалось сложной задачей даже с учётом широких возможностей и огромного влияния ИТ и ИИ, оказываемого на общество и экономику. Разумеется, оперирование категориями капитализм – социализм не может дать ответа, тем более обратный переход от социализма к капитализму обнажает несовершенство и все изъяны первого, а феномен возврата тому подтверждение.

Но, как оказалось, такой возврат тоже не увенчался успехом, и тут возникает вопрос: эти проблемы свойственны только капиталистической системе хозяйствования, или они присущи экономике как таковой? Нет ответа, как и просто отсутствует внятная работающая модель экономики, даже теории кризиса на настоящий момент не существует. Правда, есть экономисты, которые заявляют, что сегодняшняя макроэкономическая модель достигла совершенства, хотя по меньшей мере можно говорить о наблюдаемом расхождении теории и практики. И в этой связи уместна аналогия: если мы допускаем взаимосвязанность и взаимообусловленность всех явлений в мире – физических и социально-экономических, которые подчиняются объективным законам, то почему в экономике в отличие от физики до сих пор господствуют консерватизм и догматы XVIII века.

Если классическая физика была не способна объяснить существующий мир, то в начале XX века произошёл прорыв: появилась квантовая механика (далее – КМ). Эта революция в науке позволила не только объяснить суть происходящего в природе, но и создала предпосылки для открытий, которым сегодня обязана электроника и другие современные отрасли науки и техники.

Такой прорыв в физической теории изменил мир, и как такого прорыва на сегодня не хватает в экономической теории для правильного понимания и объяснения наблюдаемых экономических процессов. Ни идеи Смита, ни теория Маркса, основанная на детерминизме, не способны выявить существующие закономерности и дать ответ на вопросы, возникающие в этой связи. Но если так продуктивна квантовая теория, то, может, экономистам надо позаимствовать её идеи?

Естественно, могут появиться сомнения: насколько вообще это возможно, да всё в мире взаимоувязано, но совместимы ли физика и экономика и до какой степени, каковы конкретные предпосылки? Многие экономисты уже частично ответили на этот вопрос, даже появилось понятие «Квантовая экономика». Есть ряд примеров удачного объединения экономической и квантовой теории. Другие учёные более радикальны и указывают, что в настоящее время экономисты приводят многочисленные доказательства сложности, нелинейности экономических процессов.

Но традиционная методология экономического исследования не отражает данную природу положения вещей, в связи с чем существует конфликт между традиционной методологией экономической теории и предметом её исследования. Разрешить этот конфликт возможно, если построить методологию экономической теории на ином концептуальном фундаменте. В качестве такового может быть квантово-релятивистская системная картина мира и соответствующие ей представления о квантово-волновой природе поведения макросубъектов экономики.

Рассмотрим несколько примеров и попыток объяснения экономических явлений с помощью квантовой теории. Так, проявление одного из основных постулатов квантовой механики наблюдалось в плановой экономике: чем точнее и жёстче план, тем большая неопределённость его выполнения (принцип Гейзенберга запрещает строго определять одновременно, например, сроки изготовления и номенклатуру производства), что и являлось, по-видимому, главным недостатком плановой экономики. Или связь – цена товара и объём продаж: чем гибче цена, тем большая вероятность увеличения сбыта. Можно предположить, что произведение цена – объём в определённых пределах – величина постоянная.

Рассматривая такую категорию, как амортизация основных фондов, тоже можно увидеть, что, устанавливая точные нормы амортизационных отчислений, вносится неопределённость в хозяйственную деятельность предприятия, так как они влияют, с одной стороны, на инвестиционный потенциал, а с другой – на основную деятельность (текущие расходы, прибыль, налог).

Отсутствие гибкости в определении норм не позволяет добиться синхронизации двух процессов – накопления ресурсов для обновления основных фондов с появлением на рынке совре-

менного оборудования для замены действующего. Добиться оптимизации при воспроизводстве основных фондов – главная задача каждого предприятия, как и общества в целом.

Если шире смотреть, то в этом случае надо совместить несовместимое – стабильность и постоянное обновление. Для снижения остроты вопроса и возникают: ускоренная амортизация, амортизационная премия или вообще отказ от инвестирования, уход в сторону опекса от капекса, что уменьшает вероятные риски. А природа этого – неопределённость.

Не менее интересны и примеры, связанные с другим принципом квантовой теории – квантовой суперпозицией, в соответствии с которым объект или система могут находиться одновременно в нескольких состояниях до того момента, как мы начинаем делать наблюдения (измерения), иначе говоря, изучать или вмешиваться и влиять на состояние системы. После этого она может перейти с разной вероятностью в одно из возможных состояний.

Надо заметить, что в экономике измерения, в отличие от физики, надо трактовать расширительно от изучения до каких-либо воздействий, также имея в виду, что наше сознание не только отображает мир, но и творит его, что особенно характерно для экономических явлений. Необходимо подчеркнуть важнейшую роль таких измерений. Нужны ли они, как их проводить, как это повлияет на конечное состояние? Представляется, что правильное понимание этого, с точки зрения КМ, на самом деле является основой управления экономикой.

В качестве примера квантовой суперпозиции может служить экономика и её состояние как суперпозиция базовых состояний. Экономика, как и квантовая система, может находиться как минимум в двух состояниях, например в состоянии с признаками, характерными для капитализма и социализма одновременно или более конкретно – рыночная и плановая экономика.

Нечто подобное мы наблюдаем сегодня в России. В зависимости от наших измерений (воздействий) она может перейти в то или другое из названных, а может – и в совершенно иное. И, надо думать, вовсе не обязательно в одно из известных. Вполне возможно, в то новое состояние, которое позволило бы освободиться от существующих проблем. Всё зависит от наших измерений, в отсутствие которых она будет продолжать оставаться и в том, и в другом одновременно.

При рассмотрении системы экономических интересов видим, что интерес человека быть здоровым может быть одновременно и личным, и общественным, или внедрение инноваций это и коллективный, и общественный интерес.

Но проводя измерения, интерес здоровья может занять одно состояние, стать только личным интересом, так как пенсионная система, например, не направлена на увеличение продолжительности жизни. Интерес к инновациям может стать только государственным при монополизации экономики и отсутствии конкуренции.

Интересы чиновника, его личные и государственные, как их носителя, в зависимости от существующих институтов могут менять приоритет, но в нём одновременно будет существовать и тот, и другой. Рассматривая принцип суперпозиции через призму интересов, нельзя не сказать об интеллектуальной собственности. Вводя законы о защите интеллектуальной собственности, патентное и авторское право, защищаются интересы авторов, что стимулирует их активность. Но одновременно существует и государственный интерес, заключающийся во внедрении новаций, и тут пример, когда одно состояние – существующие законы – тормозят использование достижений, что предопределяет необходимость перехода в иное состояние.

Попутно заметим, что пример с интеллектуальной собственностью в равной степени можно отнести и к принципу неопределённости: чем жёстче законы об охране и механизм их реализации, тем неопределённее возможности внедрения инноваций. И наконец ярким примером принципа суперпозиции является действие закона стоимости или закона цен, так как внешней формой проявления стоимости есть цена. Цена может отклоняться от стоимости, она может принимать одновременно множество состояний, но, когда мы покупаем (измеряем), занимает одно из возможных, то есть цена зависит от наблюдателя – это сильно напоминает квантовый эффект.

Укажем ещё на один принцип квантовой механики – квантовая нелокальность. Мы живём не в микромире, но отношения между людьми во многом похожи на связь между элементарными частицами (когда поведение частиц, как и людей, непредсказуемы), а коллектив не что иное, как совокупность отдельных личностей. И тут уместно говорить о коллективном сознании, напоминающем в чём-то квантовую запутанность и невидимое взаимодействие этих личностей, проявляющееся как коллективное сознание.

Наблюдая на данных примерах проявления принципов КМ в экономических процессах, мы убеждаемся в возможности и целесообразности переноса её постулатов в экономику и экономическую науку с целью построения на такой основе современной экономической теории. Данная теория должна доказать прежде всего, что объективно существует такая социально-экономическая модель, при которой можно достичь высокого уровня стабильности и эффективности, то есть избавиться от выше упомянутых проблем. Кроме того, должны быть обозначены основные контуры искомой модели. Не вдаваясь в описание возможной схемы и деталей её создания, укажем только на некоторые главные выводы, концептуально меняющие наши взгляды и под-

ходы к разработке как теории в целом, так и конкретно социально-экономической модели, вытекающей из неё.

В свете КМ необходимо отказаться от доминирования экономического детерминизма. Исходя из того, что экономическая система может находиться в различных состояниях, необходимо акцентировать многообразие и допустимость множества вариантов, в том числе непредсказуемых и случайных.

Если ранее мы мыслили в терминах или – или, то КМ диктует принцип – и то, и другое одновременно, альтернативность не обязательна. Возвращаясь к политэкономической модели нового общества, допустимо предположить, что оно может одновременно содержать черты и капитализма, и социализма, допустимо совмещение противоположностей. Ранее мы уже говорили об обществе со смешанной экономикой, где сочетается государственная и частная собственность, а планирование и рынок не взаимоисключающие явления, а дополняющие друг друга. Теперь КМ даёт теоретическое подтверждение такого подхода.

Касаясь планирования, необходимо подчеркнуть, что предполагаемое базируется не на принципах детерминизма и директивности, а планирование как поиск наилучших вариантов из большого множества вероятных, может, с применением математического аппарата КМ. В данном случае уместно говорить о роли ИТ и ИИ по обеспечению реализации предполагаемой модели, так как без них такая задача принципиально не решаемая, только сейчас это становится возможным.

Но что значит – лучшие варианты? Это когда мы нацеливаемся не только на получение максимальной прибыли, но и поставляем потребителю то, что ему наиболее полезно или производим продукцию не только высокого качества, но и по низким ценам и т. п. Может показаться, что такие подходы несовместимы, альтернативны, но фактически они могут оказаться комплементарными.

Сегодняшняя экономика может сочетать в себе высокие темпы роста и низкий уровень безработицы, высокие темпы роста и низкий уровень инфляции, рост доходов в сочетании с высокой социальной активностью и т. д.

Высказанный ранее тезис об ИИ как альтернатива рынку, по-видимому, теперь надо трактовать, как наличие двух взаимодополняющих возможностей: и та, и другая могут сосуществовать. Правда, при этом важно подчеркнуть – новая теория должна отказаться от абсолютизации рынка. Дело в том, что даже сегодняшние сторонники квантовой экономики говорят о квантово-рыночной экономической модели, акцентируя примат рыночных отношений, что, в принципе, противоречит КМ.

Кроме того, идеи КМ также подтверждают другой ранее высказанный тезис о том, что прибыль не может быть единственной целью и критерием современной и особенно будущей экономики. Главенствующая роль не должна отводиться прибыли, только в совокупности с другими критериями (сохранение природы, минимизация социального неравенства) она видится в новой теории, тем более что некоторые экономисты высказывают идею о бесприбыльной экономике вообще.

Почему господствует прибыль, почему, допустим, знания, поиск истины не рассматриваются как одна из целей современного общества? Стремясь к повышению эффективности, надо помнить, что она может быть пожертвована во имя социальной справедливости, тех же знаний, человеческого общения, что вполне естественно и будет вписываться в парадигму новой теории.

В целом данные рассуждения дают основания полагать, что имеются все предпосылки, и попытка создания новой теории должна увенчаться успехом. Это и станет прорывом в экономической мысли, а в руках учёных и практиков появится мощный рабочий инструмент для адекватного ответа на сегодняшние вызовы.

Означает ли создание новой теории отказ от классики? Да, она будет строиться на принципиально новой платформе и станет главенствующей, но некоторые постулаты классики тоже могут быть полезны.

В этой связи надо подчеркнуть, что наиболее важный урок, который можно извлечь из квантовой теории, состоит в том, что явно несовместимые позиции могут оказаться всего лишь двумя сторонами одной медали в том смысле, что мы должны воспринимать великие истины как комплементарные, даже тогда, когда они кажутся противоположностями.

Причинно-следственные связи и механистический взгляд на мир вполне могут ужиться с непредсказуемыми вероятностными моделями реальности. Это краеугольный камень новой экономической теории.

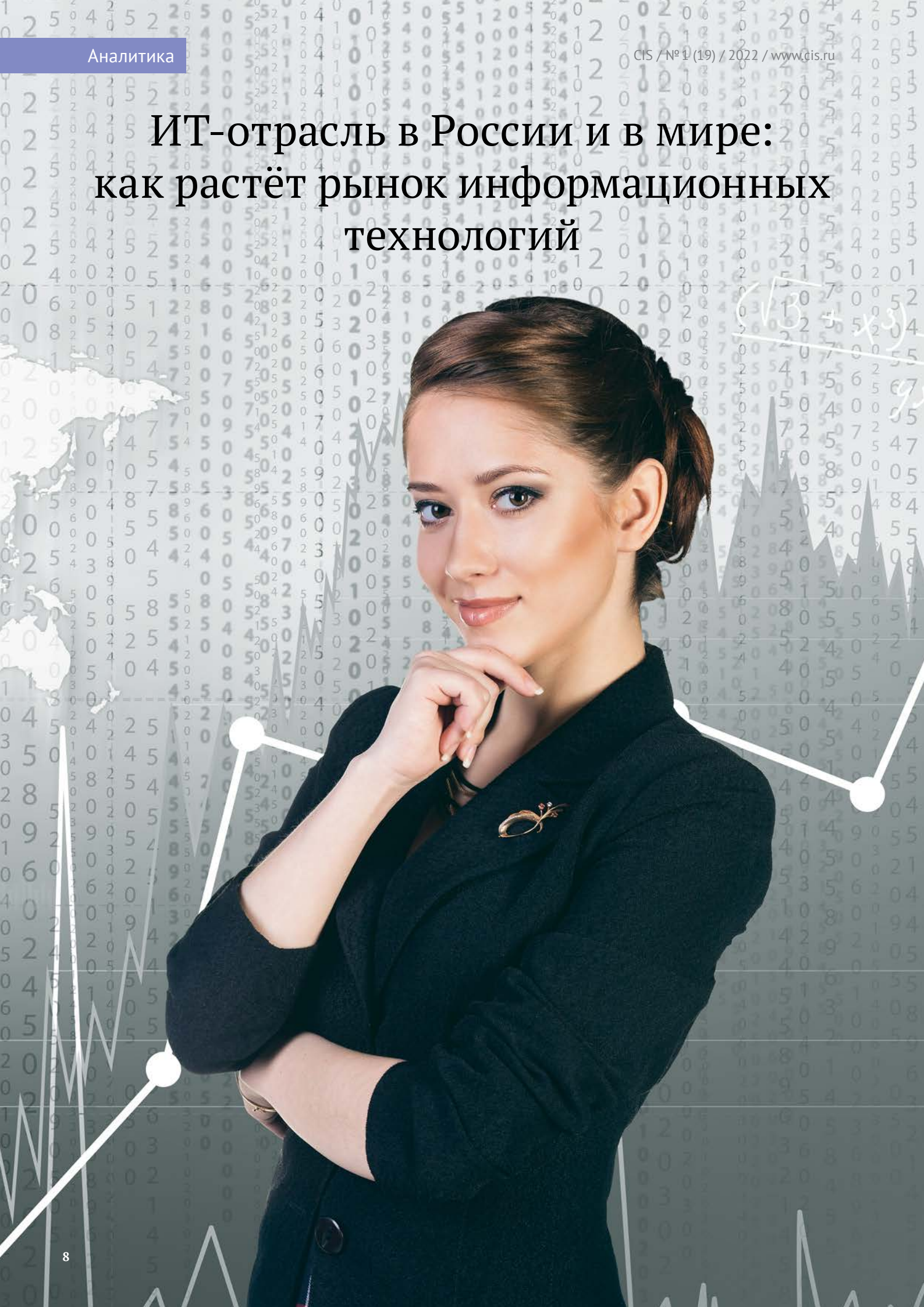
Представляется, что разработка такой теории является важнейшей задачей как учёных экономистов, так и всего научного сообщества. Без этого невозможно дальнейшее развитие, в противном случае мы обречены на постоянное непонимание сути происходящего, заблуждения, ошибочные управленческие решения и, как следствие, застой и деградацию.

Таким образом, создание новой экономической теории с учётом идей КМ станет базовым элементом конструкции, на основе которой в купе с ИТ и ИИ будет построена разумная экономика.

Анатолий Орлюк
КЭН, доцент РУТ (МИИТ)

CIS / № 1 (19) / 2022 / www.cis.ru

ИТ-отрасль в России и в мире: как растёт рынок информационных технологий



В 2020 году мировой рынок ИКТ достиг порядка 3 872,4 млрд долл., показав повышение по сравнению с предыдущим годом на 0,9 %. Доля России в этом объёме составляет не более 0,6 %. После внесения поправок в Конституцию РФ ИТ-индустрию добавили в список приоритетных видов деятельности, контролируемых государством. Согласно программе «Цифровая экономика РФ», к 2024 году планируется «оцифровать» всю экономику и социальную сферу страны. Государство активно способствует прогрессу ИТ-отрасли через налоговые послабления и законодательные инициативы. Обзор ИТ-рынка в России и в мире – в исследовании Группы «ДЕЛОВОЙ ПРОФИЛЬ».

Пандемия COVID-19 привела к прорывному переходу к цифровому формату организации процессов, многократно ускорив естественный прогресс. Уникальная ситуация 2020 года ещё больше повысила важность цифровизации и переориентировала пользователей на удалённый формат получения услуг. Люди приняли новые условия жизни, доступность технологий, что модифицировало их навыки и привычки.

По данным Salesforce, на фоне пандемии 88% клиентов ожидали, что компании активизируют свои цифровые инициативы, а 68% – заявили, что COVID-19 повысил их ожидания в отношении цифровых возможностей предоставления услуг.

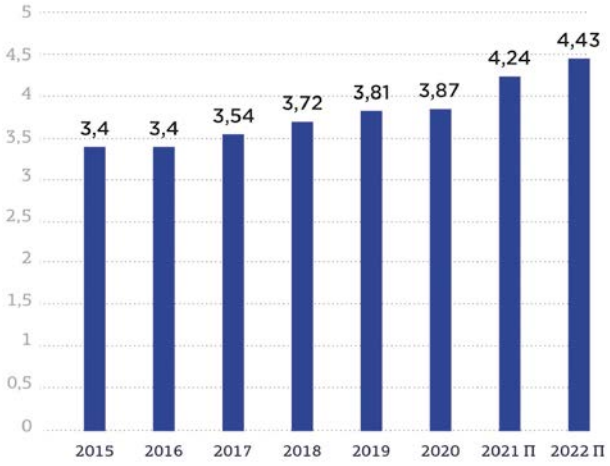


Рис. 1. Мировые расходы на ИТ-отрасль, трлн долл. Источник: Gartner.

Состояние ИТ-рынка в мире

В 2020 году мировой рынок информационно-коммуникативных технологий (ИКТ) достиг порядка 3872,4 млрд долл., показав повышение по сравнению с предыдущим годом на 0,9% (рис. 1).

По последним данным аналитиков Gartner (ноябрь 2021 года), объём мирового рынка ИКТ по итогам 2021 года составит 4,24 трлн долл., показал рост 9,5%; в 2022 году – 4,47 трлн долл., или на 5,5% к предыдущему году.

Самая большая статья расходов на мировом рынке ИКТ приходится на телекоммуникацию, на которую в 2020 году потрачено 1,39 трлн долл., а по итогам 2021 года – 1,44 трлн долл.

Второе место по расходам в структуре ИТ-рынка занимают ИТ-услуги, на которые в 2020 году потрачено порядка 1 трлн долл., а к 2022 году ожидается рост до 1,27 трлн долл.

Третье место на мировом рынке ИКТ по расходам занимают устройства и техника, на которые в 2020 году потрачено 696 млрд руб. В 2022 году ожидается, что расходы на устройства составят 820 млрд долл., а на корпоративное ПО и системы дата-центров – 700 и 207 млрд долл. соответственно.

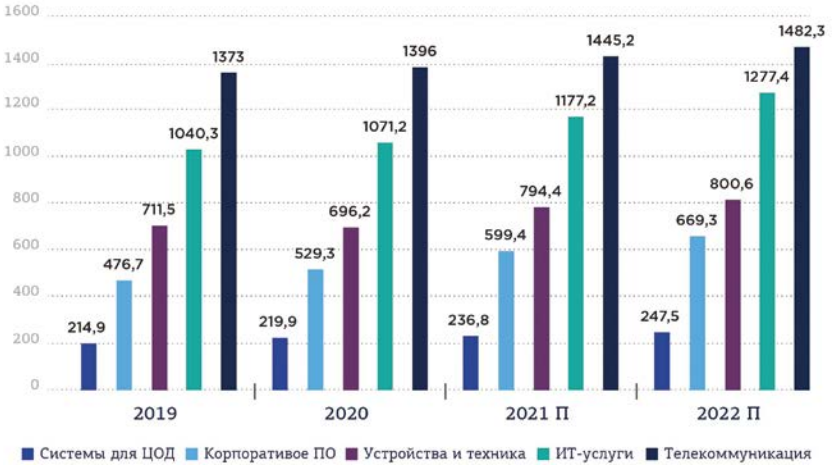


Рис. 2. Мировые расходы на ИТ-отрасль по сферам в 2019–2022 П, млрд долл. Источник: Gartner.

Наибольший рост расходов ожидается в секторе корпоративного ПО. По оценкам Gartner, рост на 11,5%, прогнозируемый на 2022 год, обусловлен тем, что «расходы на инфраструктурное ПО продолжат опережать расходы на прикладное ПО» (рис. 2).

Динамика мирового рынка ИКТ за период 2007–2018 годы достаточно хорошо коррелирована с динамикой темпов роста ВВП. Однако в последние годы рынок ИКТ растёт примерно в 2 раза быстрее ВВП (рис. 3).

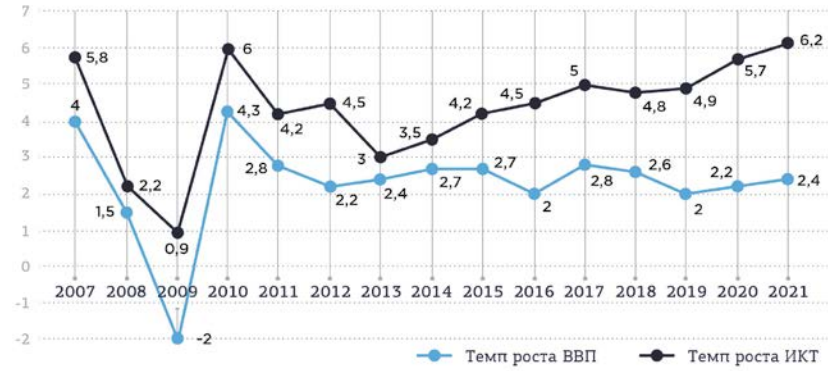


Рис. 3. Динамика мирового рынка ИКТ и ВВП, %. Источник: Tadviser www.tadviser.ru.

Рис. 4. Динамика российского ИТ-рынка, трлн руб. Источник: Руссофт, IDC.

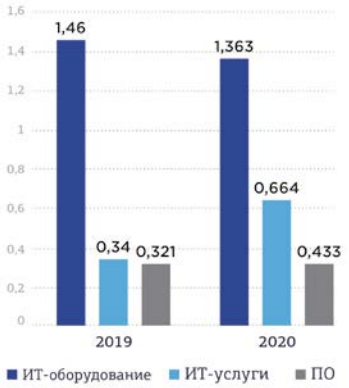


Рис. 5. Структура российского ИТ-рынка в 2019–2020 гг., трлн руб. Источник: Руссофт

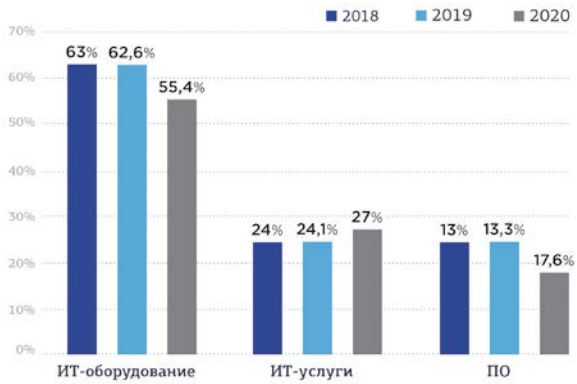


Рис. 6. Структура российского ИТ-рынка в 2019–2021 гг., %. Источник: Руссофт, ITResearch.

Рис. 7. Деятельность российских организаций сектора ИКТ по видам экономической деятельности, тыс. ед. Источник: ВШЭ, Минцифра.

Состояние ИТ-отрасли в России

Доля России на мировом рынке ИКТ составляет не более 0,6% по итогам 2020 года. По оценке ассоциации РУССОФТ, размер ИТ-рынка России в 2020 году достиг 2,46 трлн руб., увеличившись за год на 16–20%, или $ 34,1 млрд с ростом на 7,9%. Однако, по данным компании IDC, эти показатели оказались значительно ниже – 1,83 трлн руб., или $ 25,35 млрд с увеличением на 14% и 2% соответственно (рис. 4).

Российский ИТ-рынок считался незрелым из-за слишком высокой доли продаваемого на нём оборудования. Отчасти он таковым остаётся, если применять указанный критерий зрелости, но после долгих лет медленного увеличения доли ИТ-услуг и ПО, в 2014–2015 годы произошёл резкий скачок по ИТ-услугам – их доля выросла с 20% до 25%. В 2016 году доля услуг почти не изменилась, а по итогам 2017 года увеличилась ещё на один процентный пункт – до 26% (рис. 5).

Такое изменение в 2014–2015 годы было вызвано в первую очередь существенным удорожанием импортного оборудования в результате девальвации рубля из-за кризиса на Украине при очень малом количестве российских аналогов, что привело к сокращению его продаж. Однако фактор девальвации рубля в 2017 году на увеличение доли ИТ-услуг уже не мог работать, поскольку в этом году произошло существенное укрепление рубля.

В 2018 году компания IDC определила существенное увеличение продаж в России именно ИТ-оборудования (в долларовом выражении – на 15%), а вот ИТ-услуги и ПО почти не изменились. Следовательно, произошло некоторое отступление и возврат к структуре, которая была до 2014 года, хотя доля ИТ-услуг (24%) по-прежнему оставалась выше, чем была в 2014 году (20%). В 2019 году структура рынка существенно не изменилась, но доля ИТ-услуг и ПО немного возросла. По итогам 2020 года доля ИТ-услуг и ПО показала рост на 3% и 4% соответственно, а доля ИТ-оборудования сократилась на 7% (рис. 6).

Таблица 1. Топ-20 ИТ-компаний в России. Источник: CNews www.cnews.ru.

Рейтинг 2020	Рейтинг 2019	Компания	Сфера деятельности	Выручка 2020 г., тыс. р.	Выручка 2019 г., тыс. р.	Рост выручки 2020/2019, %
1	2	Ланит (Москва)	Группа компаний	216810014	173767327	24,8%
2	-	OCS Distribution (СПб)	Дистрибуция АО и ПО	214991706	н/д	н/д
3	3	EPAM Systems	ИТ-услуги	191322847	148477545	28,9%
4	5	Марвел-Дистрибуция (Москва)	Дистрибуция АО и ПО	156139390	97517347	60,1%
5	4	Softline (Москва)	Группа компаний	131953000	108834000	21,2%
6	6	ИКС Холдинг (Москва)	Группа компаний	88563000	82231000	7,7%
7	8	Ростелеком (Москва)	ИТ-услуги	77230000	48600000	58,9%
8	7	1С (Москва)	Разработка и дистрибуция ПО	65010000	54300000	19,7%
9	15	Группа Т1 (ранее Техносерв) (Москва)	ИТ-услуги	59168070	26518197	123,1%
10	-	Лаборатория Касперского (Москва)	Разработка и дистрибуция ПО	50638566	44320631	14,3%
11	-	IBS (Москва)	ИТ-услуги	41791973	40441694	3,3%
12	13	Крок (Москва)	ИТ-услуги	38534454	30669720	25,6%
13	10	Ай-Теко (Москва)	ИТ-услуги	32226998	36340434	-11,3%
14	12	Инфосистемы Джет (Москва)	ИТ-услуги	31342561	31114511	0,7%
15	-	Новый Ай-Ти Проект (3Logic Group) (Москва)	Дистрибуция АО и ПО	30083835	21530503	39,7%
16	-	Ситроникс (Москва)	ИТ-услуги	29522555	10388864	184,2%
17	14	Центр Финансовых Технологий (Москва)	ИТ-услуги	27442921	27854902	-1,5%
18	9	Газпром Автоматизация (Москва)	ИТ-услуги	27000000	46407903	-41,8%
19	-	Рубитех (Москва)	ИТ-услуги	25000000	339000	7274,6%
20	-	Аквариус (Москва)	Производство АО	22800698	10	-

Деятельность ИТ-компаний в России

В России на начало 2021 года функционировало порядка 108 тыс. организаций, в секторе ИКТ это на 2,8% меньше по сравнению с 2019 годом (116 тыс. организаций). 52,7 тыс. организаций осуществляют свою деятельность в отрасли именно информационных технологий (рис. 7).

Слияния и поглощения на рынке ИТ

Следует сказать, что сокращение количества организаций сектора ИКТ за последние два года связано, прежде всего, с процессом слияния и поглощения (M&A).

- Так, в 2021 году «Ростелеком» приобрёл за 500 млн руб. 51% акций компании «Войслинк» (разработчик решения для проектов «Умный город» и «Безопасные дороги»); 50,01% – в «БФТ-холдинге», который владеет ИТ-компанией «Бюджетные и финансовые технологии» за 1,65 млрд руб.; в декабре 2021 года осуществил покупку профильной ИТ-компании провайдера MVNE-платформы «ТВЕ-Телеком» за 1,7 млрд руб.
- МТС приобрёл компанию VisionLabs B. V по предварительной оценке за 7 млрд руб.; 100% акций МТТ за 5 млрд руб., тем самым вложившись в развитие искусственного интеллекта.
- «Вымпелком» приобрёл лидера среди провайдеров облачных сервисов IBS DataFort (около 3 млрд руб.).
- «ЭР-Телеком Холдинг» купил группу компаний «Лартех» и «Авантел».
- Epam Systems совершил сделку по приобретению PolSource, занимающейся внедрением CRM-системы Salesforce за 111,8 млн долл.
- В ближайшее время должна быть завершена сделка по продаже «ИКС Холдинга», основатель которой намеревается выкупить у группы USM Алишера Усманова.

В целом аналитики предполагают дальнейшую активность на рынке M&A в ИТ-секторе с ростом 5–8% в год.

ТОП крупнейших ИТ-компаний в России

По результатам исследования CNews, выручка участников рейтинга крупнейших ИТ-компаний России в 2020 году увеличилась на 28,6% и впервые превысила 2 трлн руб. Первое место в рейтинге занял «Ланит» с показателем 216,8 млрд руб. На втором – OCS Distribution – 215 млрд руб. На третьем, как и в 2019 году, Epam – 191,3 млрд руб. (табл. 1).

Таблица 2. Российские компании в магическом квадранте Gartner

Наименование магического квадранта Gartner	Год публикации	Наименование компании
Endpoint Protection Platforms	2021	Kaspersky
Enterprise Data Loss Prevention	2017	InfoWatch Zecurion Searchinform
Enterprise Backup and Recovery Software Solutions	2021	Veeam Acronis
Treat Intelligence	2014	Kaspersky Lab Group IB
Application Security Testing	2018	Positive Technologies (лидер)
Operational Technology Security	2016	Positive Technologies
Data Center Backup and Recovery Software/Solutions	2020	Veeam Acronis
Integrated Revenue and Customer Management for CSPs	2019	Nexign
Sales Force Automation	2021	bpm»online (Terrasoft)
CRM Lead Management	2020	bpm»online (Terrasoft)
CRM Customer Engagement Center	2021	bpm»online (Terrasoft)
Meeting Solutions	2020	TrueConf
Insight Engines	2021	EPAM

** компания продвигает свои решения bpm'online на зарубежных рынках под брендом Creatio. Источник: Руссофт.*

Одними из наиболее престижных рейтингов для продуктовых компаний (производителей программных продуктов) являются рейтинги аналитического агентства Gartner Group, которое ежегодно составляет так называемые «магические квадранты Gartner» (Gartner Magic Quadrants). В них указываются продукты и компании, входящие в число лидеров в определённых сегментах ПО (табл. 2).

Внедрение ИТ-продуктов в отрасли

Самый большой вклад ИТ-сектора в развитие российской экономики был сделан в добычу полезных ископаемых, торговлю и операции с недвижимостью (рис. 8).

Стимулирование развития ИТ-отрасли в России: цифровая экономика

После внесения поправок в Конституцию РФ в 2020 году ИТ-индустрию добавили в список приоритетных видов деятельности, контролируемых государством. Внесение ИТ-индустрии в Конституцию говорит о том, что ИТ-сфера и связанная с ней система информационной безопасности имеет большое значение и требует регулирования федеральным законодательством.

В силу этого 9 мая 2017 года Указом Президента Российской Федерации была утверждена стратегия развития информационного общества на 2017–2030 годы. На основании данной стратегии Правительством РФ была разработана и утверждена программа «Цифровая экономика Российской Федерации» (Распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р), куда включены 6 федеральных проектов (рис. 9).

Суть программы в том, чтобы к 2024 году оцифровать экономику и социальную сферу России. Для этого власти совершенствуют законодательство, развивают инфраструктуру, внедряют новые технологии в ключевых сферах экономики и готовят кадры для работы в цифровой среде. Власти рассчитывают довести долю ИТ-сектора в ВВП страны до 2%. Для сравнения: сейчас этот показатель составляет менее 1%, хотя в странах Западной Европы он достигает 3%.

Налоговый манёвр для ИТ-отрасли

Первый пакет мер поддержки ИТ-отрасли в России был разработан летом 2020 года так называемый «налоговый манёвр» для ИТ-отрасли. Благодаря подписанному Президентом РФ **Федеральному закону «О внесении изменений в часть вторую Налогового кодекса Российской Федерации» от 31.07.2020 № 265-ФЗ** летом 2020 года был снижен налог на прибыль для ИТ-компаний с 20 до 3% и уменьшены тарифы страховых взносов с 14 до 7,6%. Также российских разработчиков софта освободили от уплаты НДС. Льготы будут бессрочными, получить их может любая российская компания, у которой не менее 90% доходов приходится на продажу софта и услуги по его разработке, внедрению и поддержке. Чтобы получить льготы, необходимо зарегистрироваться в реестре российских разработчиков ПО.

Кроме того, власти хотят снизить налог на прибыль для любых компаний, использующих российское оборудование и программное обеспечение. Авторы инициативы рассчитывают, что это позволит дополнительно поддержать ИТ-отрасль.

Чтобы получить налоговые льготы, необходимо зарегистрироваться на сайте Минцифры, заполнив два документа: заявление и справку деятельности в сфере ИТ.

Этими льготами решили воспользоваться и крупные компании: в апреле 2021 года они начали создавать отдельные юрлица для своих ИТ-подразделений, чтобы подпасть под требования закона. Такой манёвр совершили «ВымпелКом», МТС, «Почта России», «Росатом» и «Сбер». В первоначальной редакции закона «Яндекс», «Сбер» и прочие крупные компании не подпадали под требования и не могли претендовать на применение этих налоговых режимов, потому что они получают основной доход не от ПО, а от рекламы и маркетплейсов. Однако бизнес подстраивается под нюансы законодательства. В результате ИТ-гиганты начали выделять в отдельные самостоятельные

Рис. 8. Вклад сектора ИКТ в развитие российской экономики по итогам 2020 г., % от ВВП. Источник: Минцифра

структуры юрлица, которые генерируют выручку от продаж ПО.

Регуляторные песочницы для ИТ-компаний

Принят **Федеральный закон «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации»** от 31.07.2020 № 258-ФЗ, который вступил в силу 28 января 2021 года. Данным законом были введены «регуляторные песочницы», которые позволяют компаниям тестировать инновационные предложения на рынке с реальными потребителями. Песочница предназначена для авторизованных фирм, несанкционированных фирм, которым требуется авторизация, и технологических компаний, которые стремятся внедрять инновации на рынке финансовых услуг.

Российская практика внедрения «песочниц» предполагает реализацию опыта Великобритании, которая первую «песочницу» создала в 2016 году. К слову, позже их внедрили в США, Австралии, Сингапуре, ОАЭ, Малайзии, Таиланде, Индонезии, Бахрейне, Швейцарии и Канаде.

На опыте Великобритании «песочница» стремится предоставить фирмам

- возможность тестирования продуктов и услуг в контролируемой среде,
- сокращение времени вывода на рынок при потенциально более низких затратах,
- поддержка в определении надлежащих гарантий защиты прав потребителей для включения в новые продукты и услуги,
- более широкий доступ к финансированию.

Тесты в песочнице должны иметь чёткую цель (например, снижение затрат для потребителей) и проводиться в небольших масштабах. Фирмы тестируют свои инновации в течение ограниченного периода времени с ограниченным числом клиентов.

С момента своего запуска нормативная «песочница» работала на когортной основе, что означает, что фирмы могли подавать заявки только в течение определённого периода календарного года. В то время как когортный подход подходил для среды тестирования, которая служила основой для регулирующих органов во всём мире, песочница требовала изменений, отражающих её зрелость и уроки, извлечённые с момента её создания в 2016 году.

В обзоре Kalifa по финтеху Великобритании было рекомендовано расширить «песочницу», чтобы обеспечить большую ценность для фирм. Это включало конкретную рекомен-

Рис. 9. Национальная программа «Цифровая экономика». Источник: ВШЭ

дацию о том, чтобы «песочница» предоставлялась на постоянной основе, а не через ограниченные по времени окна.

В августе 2021 года нормативная «песочница» перешла на режим «всегда открыто», что позволило фирмам подавать свои заявки в течение всего года. Внеся это изменение, фирмы теперь могут получить доступ к сервисам тестирования в «песочнице» в нужный момент жизненного цикла своей разработки, чтобы максимально использовать преимущества тестирования на реальном рынке для продвижения своих инновационных моделей.

В России по аналогии с Великобританией смысл внедрения «песочницы» в том, чтобы компании могли применять новые технологии, а государство могло выработать соответствующие регуляторные нормы для них. Речь идёт об апробации таких инноваций, как искусственный интеллект, блокчейн, Big Data, нейротехнологии, квантовые технологии, виртуальная и дополненная реальность.

В России регуляторные «песочницы» функционируют для компаний в сфере медицины, транспорта, промышленности и других секторов экономики. Специальное регулирование не коснётся сферы электронных и дистанционных образовательных технологий: этот пункт изъяли из финальной редакции документа.

Дорожная карта по развитию ИТ-рынка

В сентябре 2021 года Правительство РФ утвердило «План мероприятий («дорожная карта») «Создание дополнительных условий для развития отрасли информационных технологий» (утв. Правительством РФ 09.09.2021) в качестве *второго пакета мер поддержки ИТ-отрасли.я*

«Дорожная карта» включает 62 мероприятия, 20 из которых носят общесистемный характер:

- выравнивание условий ведения бизнеса в России для международных интернет-корпораций и российских ИТ-компаний (а именно «цифровой налог» для иностранных компаний);
- стимулирование внедрения российских решений в деятельность отечественных предприятий;
- поддержка экспорта и продвижения российских ИТ-решений на зарубежных рынках.

Ещё 42 мероприятия плана направлены на стимулирование развития и внедрения российских разработок: решения для бизнеса, электронные образовательные сервисы, цифровые медицинские сервисы, офисное программное обеспечение и операционные системы, обработка данных и облачные сервисы, решения в сфере искусственного интеллекта, больших данных и Интернета вещей, производство компьютерных игр и профессионального видеоконтента, решения в сфере информационной безопасности.

Эффект от внедрения двух пакетов мер составляет порядка 49 млрд руб.

Третий пакет мер поддержки ИТ-отрасли: искусственный интеллект

В 2022 году планируется разработка третьего пакета мер поддержки ИТ-компаний, который, прежде всего, коснётся разработок в сфере искусственного интеллекта.

В декабре 2021 года стало известно, что в России будет разработана дорожная карта поэтапного внедрения технологий искусственного интеллекта, предусматривающая разработку и реализацию комплекса законодательных инициатив. Эти мероприятия предусмотрены в рамках федерального проекта «Искусственный интеллект».

На разработку и внедрение технологий искусственного интеллекта в 2021 году выделено более 6 млрд руб., а до 2024 года – 31,5 млрд руб. При этом предполагается внедрение новых налоговых льгот для ИТ-компаний. Суть одной из льгот заключается в использовании повышающего коэффициента 1,5 к расходам на приобретение российских решений в сфере искусственного интеллекта. При их внедрении компании будут платить меньше налога на прибыль.

Приземление ИТ-гигантов

Вместе со стимулированием отечественных разработчиков государство вводит ограничения для иностранных платформ.

Федеральным законом от 01.07.2021 № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации» обязывает иностранных лиц (в том числе граждан) открыть филиал/представительство/юридическое лицо на территории России и обеспечить его функционирование. Закон коснётся иностранных лиц, которые владеют иностранным ресурсом (сайтом, страницей, мобильным приложением и т. п.) с числом российских пользователей более 500000 в сутки.

Роскомнадзор будет вести перечень иностранных лиц, осуществляющих деятельность в сети Интернет на территории России. Иностранное лицо должно подать заявление о включении информации о нём и его информационном ресурсе в перечень Роскомнадзора в течение суток после регистрации личного кабинета на сайте Роскомнадзора. Роскомнадзор будет определять иностранных провайдеров хостинга, операторов рекламной системы и организаторов распространения информации в сети Интернет, обязанных соблюдать новый закон по методике, которая будет утверждена Правительством РФ. Для осуществления контроля со стороны Роскомнадзора иностранное лицо обязано установить предложенную Роскомнадзором программу для ЭВМ, которая позволит определить количество пользователей информационного ресурса в сети Интернет.

В случае неисполнения указанных в законе требований Роскомнадзор вправе применить следующие меры:

- информирование пользователей ресурса о нарушениях;
- запрет распространения рекламы об информационном ресурсе и на информационном ресурсе;
- ограничение проведения платежей в адрес информационного ресурса;
- запрет на появление информационного ресурса в поисковой выдаче поисковых систем;
- запрет на сбор и трансграничную передачу персональных данных;
- частичное или полное ограничение доступа к информационному ресурсу.

Новые меры, установленные за нарушение закона, могут быть применены по решению Роскомнадзора так же и в случае нарушения иностранным лицом иных положений законодательства, например:

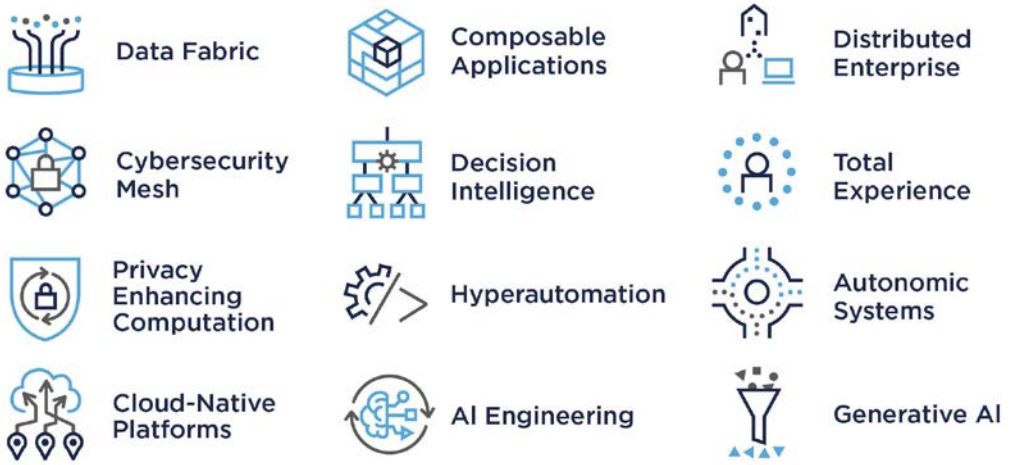


Рис. 10. Основные технологических тенденций в 2022–2025 гг. Источник: Gartner.

- за нарушение обязанности по ограничению доступа к информационным ресурсам;
- за нарушение законодательства о персональных данных;
- в случае признания лица нежелательной организацией;
- за нарушение законодательства о рекламе, в том числе за неисполнение обязанности по предоставлению информации об интернет-рекламе.

Закон вступил в силу 01.07.2021, однако отдельные положения закона об обязанности иностранного лица создать филиал/открыть представительство/юридическое лицо и обеспечить его функционирование на территории России вступают в силу с 01.01.2022, а положения о применении Роскомнадзором мер понуждения, в случае неисполнения иностранным лицом обязанностей по предоставлению информации о рекламе, вступают в силу с 01.09.2022.

Кроме того, Правительство РФ собирается ввести новый налог для зарубежных ИТ-компаний, который получил название «Цифровой налог» (налог зарубежных ИТ-компаний с прибыли в России). Власти хотят взимать дополнительную плату с тех, кто использует данные россиян для демонстрации таргетированной рекламы. Предположительно, размер нового налога для организаций составит 3%. Полученные средства направят на поддержку отечественной ИТ-отрасли. В декабре 2021 года в Совете Федерации предложено ввести прогрессивную ставку налога в зависимости от прибыли зарубежных ИТ-компаний на территории России.

На этом фоне все зарубежные ИТ-гиганты подняли цены на ПО, заложив в стоимость НДС. Российские разработчики воспользовались трендом и также провели индексацию. Кроме того, некоторые иностранные разработчики, ранее планировавшие выйти на отечественный рынок, отложили своё решение из-за возросших задержек.

В целом, по данным Минцифры, порядка 13 млрд руб. предусмотрено в федеральном бюджете на 2022 год для поддержки разработки и внедрения российских цифровых решений.

Перспективы развития ИТ-отрасли

Отечественные и зарубежные специалисты прогнозируют дальнейший рост ИТ-рынка и повсеместного распространения и внедрения ИКТ.

По мнению специалистов, в ближайшие 2–3 года ИТ-рынок будет развиваться согласно 12 технологическим тенденциям, выступающих в качестве мультипликаторов цифрового бизнеса и инноваций. В число основных трендов аналитики включили, в том числе:

- ткань данных (Data Fabric) – гибкая интеграция различных источников данных на платформах и среди бизнес-пользователей;
- сеть кибербезопасности (Cybersecurity Mesh) – гибкая архитектура, которая объединяет распределённые и разрозненные службы безопасности;
- вычисления, повышающие конфиденциальность (Privacy-Enhancing Computation), обеспечивают обработку персональных данных (рис. 10).

За последние десятилетия ИТ-сектор превращается в один из наиболее динамично развивающихся сегментов мирового хозяйства, сохраняя за собой репутацию отрасли, подверженной динамичным, непрерывным и кардинальным изменениям. С учётом того, что политика РФ в сфере ИКТ складывается на качественно новом экономическом, политическом и социальном уровнях, в условиях научно-технологических изменений, наше государство обладает всеми шансами на высокие позиции в рейтингах стран-лидеров мировой инновационной системы.

Однако в результате рыночных преобразований в России сложились особые черты развития, отличающиеся как от старой советской системы, так и от новой, заимствованной у западных стран. Это нашло проявление прежде всего в возрастающем тренде импортозамещения. Активная интеграция в глобализационные процессы требует от России наличия собственных передовых технологий как весомого фактора обеспечения преимуществ в конкурентной борьбе.

DELOVOY PROFIL
A member of mgiworldwide

По вопросам проведения аналитических исследований
Александра Шнипова
Заместитель руководителя практики Управленческого консалтинга Группы «ДЕЛОВОЙ ПРОФИЛЬ» | MGI Worldwide
+7 (495) 7401601
Contact@delprof.ru

По вопросам подготовки экспертных комментариев и статей
Александра Пашкевич
Ведущий маркетолог Группы «ДЕЛОВОЙ ПРОФИЛЬ» | MGI Worldwide
+7 (495) 7401601 (вн. 1048)
Pashkevich@delprof.ru4

CIS / № 1 (19) / 2022 / www.cis.ru

Результаты отраслевого исследования зрелости команд и процессов разработки программного обеспечения: ожидания и реальность

Весной 2021 года компания Logrocon при информационной поддержке itSMF провела некоммерческое исследование и оценила состояние ИТ-рынка РФ в части зрелости команд и процессов разработки/эксплуатации ПО.

Организаторы дали возможность респондентам проанализировать уровень зрелости команд и цикла разработки/эксплуатации в своей компании, а также сопоставить его с показателями по отрасли. **Консолидированный отчёт** с результатами есть в свободном доступе. В данной статье хотим поделиться некоторыми наблюдениями, которые появились в процессе подготовки и проведения исследования.

Сначала немного исходной информации. К участию в опросе приглашались сотрудники ИТ-компаний и ИТ-департаментов компаний разных отраслевых сегментов. При выборе респондентов приоритет отдавался сотрудникам, обладающим полномочиями принятия решения по вопросам организации ИТ-процессов либо оказывающим значительное влияние на их принятие. Анкета содержала вопросы, разбитые на несколько тематических модулей. Мнение отвечающего отражалось на шкалах.

С какими сложностями столкнулась рабочая группа при организации исследования?

Во-первых, привлечение партнёров. Мы искали единомышленников среди консалтинговых компаний, специализированных СМИ и т.п. – всего 23 компании. По факту поддержки исследования партнёры могли получить:

- права на публикацию и использование результатов;
- определённое конкурентное преимущество, основанное на обладании уникальной информацией;
- качественный контент, интересный их аудитории и повышающий её вовлечённость в дальнейшее сотрудничество.

От партнёров мы ждали поддержки при распространении опросников в целевой аудитории и её вовлечении в исследование, открытого продвижения результатов по окончании работ.

Оказалось, что практически нет организаций, готовых сегодня работать на свою аудиторию и участвовать в подобных исследованиях. Если коротко, то желание «заработать здесь и сейчас» значительно превышало стремление к получению маркетингового результата, который мог принести отложенный экономический эффект. Почти все, с кем велись переговоры, пытались в одностороннем порядке предлагать или коммерческие условия, или выдвигать сложно реализуемые требования. «Тактика» победила «стратегию».

Мы пришли к следующим выводам:

1. При организации исследовательских проектов и привлечении к ним партнёров необходимо опираться, в основном, на собственную сеть контактов, для чего требуется постоянное её формирование и развитие.
2. Необходим более агрессивный PR при продвижении подобных проектов.
3. В случае проведения исследований как системного вида деятельности необходим непрерывный, а не ситуативный поиск партнёров.
4. Ориентированность отраслевых СМИ на исключительно коммерческое донесение информации показывает нехватку на рынке независимых некоммерческих исследований. Следовательно, их ценность и важность будет расти на фоне растущей коммерциализации СМИ и соцсетей.

Теперь несколько слов о подборе респондентов и их поведенческих особенностях.

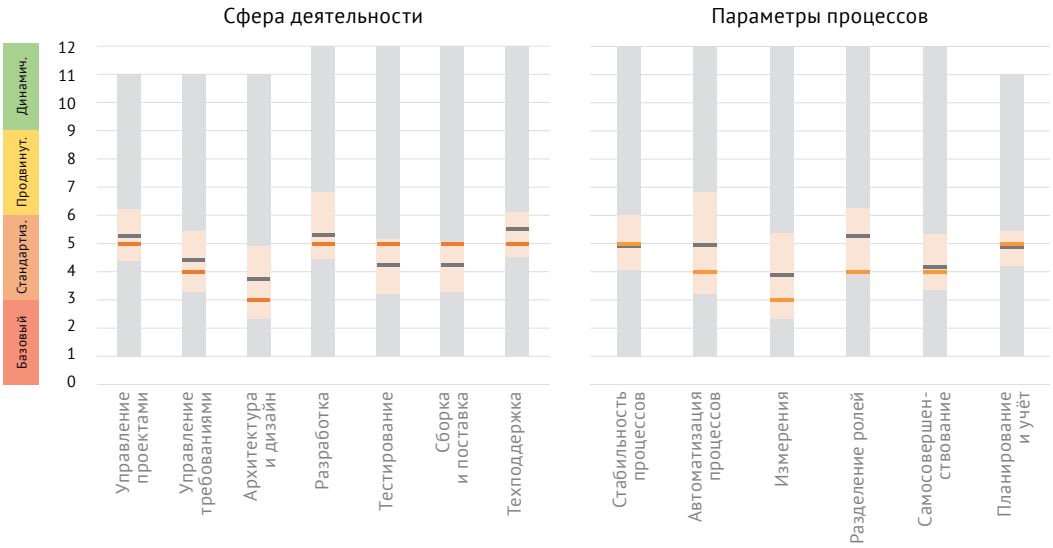
Проект был некоммерческим, мы надеялись, что многим он будет интересен, поскольку, кроме возможности получить обобщённые результаты, предоставлялись и персональные бесплатные консультации, содержащие ключевые рекомендации по оптимизации ИТ-процессов.

Были организованы массовые активности по вовлечению участников: публикации, рассылки, посты… Мы отправили только по тёплым и холодным контактам более 250 приглашений.

Реальность вновь оказалась неожиданной: направленные в корпоративную электронную почту приглашения практически всегда оставались без внимания, а вот прямой контакт, в том числе и в соцсетях, давал живой отклик. Это стало основным каналом коммуникаций. Организаторами был пройден весь путь формирования доверия к исследованию и команде, мы работали с сопротивлениями на всех этапах: от категоричных отказов до заинтересованности и принятия. Сложный и небыстрый путь! В итоге удалось вывить некоторую статистическую закономерность: расчётное количество респондентов составляет не более 25% от общего числа людей, получивших приглашения. Основными причинами отказа от участия заявлялись: нехватка времени, загруженность приоритетными задачами, недостаточность информации для ответа на вопросы, боязнь за распространение служебной информации, непонимание значимости результатов.

Кого исследования заинтересовали больше всего?

Здесь просматривалась прямая закономерность: чем выше статус респондента, чем больше у него возможностей влиять на процессы через изменения, тем выше была заинтересованность и активность. Но и тут команда столкнулась с проблемой: выше должность – меньше времени на подобные задачи. Сняли напряжённость за счёт предоставления возможности отвечать



на вопросы за несколько итераций с сохранением ответов на уже отвеченные вопросы.

При обработке результатов исследовательская группа столкнулась ещё с одним интересным эффектом – неравномерность оценок, то есть при ответах на вопросы одного из модулей баллы значительно увеличивались. Индивидуальная работа с респондентами позволила понять причину этого. Такой эффект наблюдался только в опросниках руководителей какого-то конкретного функционального направления. Например, руководитель тестирования, оценивая свои процессы, ставил оценки выше, нежели при оценке процессов разработки ПО.

Кроме того, результаты показали, что у ИТ-директоров взгляд на процессы был более критическим, чем у руководителей команд и подразделений, что отразилось при выставлении баллов.

Что же в итоге получили респонденты в практическом плане?

1. Индивидуальные результаты независимого исследования зрелости ИТ-процессов и готовности команд в виде аналитического отчёта в графической форме с пояснительными записками.
2. Возможность без затрат проанализировать уровень зрелости своих команд и процессов в области разработки/эксплуатации ПО, сравнить корпоративные результаты с отраслевыми показателями, получить индивидуальные консультации по результатам исследования и рекомендации по оптимизации процессов. Средняя стоимость подобных исследований колеблется в пределах одного миллиона рублей.
3. Оценку перспектив необходимых или возможных изменений в корпоративных ИТ-процессах, сравнение с результатами своей управленческой аналитики.
4. Возможность определить причины отклонений от оптимального состояния процессов, выработать стратегию поэтапного внедрения изменений.
5. Получить аргументы для обоснования перед руководством компании необходимости этих изменений.

Прежде чем переходить к выводам о качестве отдельных компонентов процесса разработки и эксплуатации ПО, следует подвести общий итог исследования. Они показали, что ключевыми проблемами формирования зрелости команд являются:

1. Сложность определения критериев результативности деятельности. Проблема связана с большой вариативностью решаемых задач, а также с различием групповых и индивидуальных подходов к созданию продукта.
2. Размытость системы материального стимулирования по результатам проектной деятельности.
3. Балансировка внепроектных и проектных коммуникаций.
4. Трансформация культуры среды разработки ПО в условиях автоматизации и цифровизации процессов.

Зрелость ИТ-процессов

Центральным направлением исследования была выбрана оценка зрелости процессов жизненного цикла ПО: управление требованиями, управление проектами, архитектура и дизайн, разработка, тестирование, сборка и поставка (управление релизами), техническая поддержка.

Напомним, что зрелость процессов не коррелирует с качеством продукции: даже организации с очень низким уровнем зрелости процессов могут производить высококачественную продукцию, но это достигается обычно за счёт экстраординарных усилий отдельных уникальных работников и менеджеров, которые интуитивно чувствуют текущее состояние дел. Поэтому организации с низким уровнем зрелости очень чувствительны к кадровым изменениям, не могут планировать своё развитие и не могут гарантировать повторение успешных результатов, в то время как организации с высоким уровнем зрелости нацелены как раз на гарантированное повторение результата с таким же

уровнем качества, и его менеджмент имеет необходимые инструменты для контроля и управляющих воздействий, не зависящие от интуиции, смены кадров и технологий.

По каждому процессу изучались: стабильность, уровень автоматизации, наличие планирования и учёта, наличие измерений (метрик, показателей эффективности), разделение ролей, выполнение мероприятий по самосовершенствованию.

Результаты опросов показывают, что на рынке имеются как организации с очень высокими уровнями зрелости (по крайней мере, в части нескольких процессов), так и с «нулевым». На столбчатой диаграмме видно, что значения колеблются от 1 до 12. Такой разброс также частично может объясняться субъективностью мнений опрашиваемых или их недостаточной осведомлённостью. Но такие отклонения нивелируются при усреднении значений.

Зрелость отдельных процессов

Исследования показали, что:

1) в организациях наиболее высокий уровень зрелости наблюдается в управлении проектами, разработке и технической поддержке. Это ожидаемый результат, поскольку обычно наиболее эффективными становятся те процессы, в которых напрямую задействован заказчик (управление проектом, техподдержка) или он использует их результаты (разработка);

2) процессы тестирования, сборки, поставки и управления требованиями бизнес обычно рассматривает как обеспечивающие, второстепенные, поэтому показатели их зрелости меньше;

3) абсолютным аутсайдером является процесс архитектуры и дизайна. Ему уделяют так мало внимания, что как минимум в половине исследуемых организаций он находится на базовом уровне или ниже (значение моды равно 3). Этот результат подтверждается также нашей консалтинговой практикой. При проведении обследований ИТ-процессов мы часто сталкиваемся с проблемами незрелой архитектуры, когда организации в течение многих лет и даже десятилетий экономят на решении архитектурных проблем и постепенно загоняют свой ИТ-ландшафт в ситуацию, когда его дальнейшее развитие невозможно. Сопровождение в текущем виде становится рискованно и дорого, а модернизация потребует полной переделки всего ИТ-ландшафта и масштабных инвестиций;

4) в части процессов тестирования и сборки/поставки выделяется значимое количество аутсайдеров – компаний, у которых зрелость данных процессов «нулевая», то есть существенно ниже среднеотраслевого уровня. К сожалению, наше исследование не позволяет выяснить, является ли данное отставание объективным (нет потребности в таких процессах) или системной проблемой (ошибка менеджмента).

Отдельные аспекты зрелости процессов

1. При рассмотрении отдельных аспектов зрелости процессов, мы также видим явного аутсайдера – измерение и контроль процессов. Это действительно характерная проблема для российского рынка: ИТ-менеджеры предпочитают управлять подразделениями, ориентируясь на своё чутьё и субъективные мнения исполнителей, а не на численные показатели и метрики.
   Данный подход полностью противоречит одному из ключевых принципов менеджмента: если что-то не измеряется, то им нельзя управлять.
   В большинстве производств – строительство, машиностроение, обрабатывающая, химическая и пищевая промышленность – использование измерений для контроля процесса и качества продукции является неотъемлемой частью производства и зачастую закреплено даже на законодательном уровне.
   В производстве программного обеспечения законодательных требований по контролю и измерению процессов нет, но они предписываются такими добровольными стандартами как ISO 9001 (системы менеджмента качества), ISO 27001 (системы менеджмента информационной безопасности), ГОСТ Р 59194 (управление требованиями). В мире в целом предпочитают следовать таким стандартам. Даже компании, прибегающие к аутсорсинговым услугам из развивающихся стран, выполняют соответствующие контроль и измерения на своей стороне.
   В России данный подход пока не распространён, вызывает отторжение как у работников, которым не хочется контроля, так и у менеджмента, который считает проведение измерений и контроля излишне трудоёмким и затратным.

2. Невысокие значения имеет и показатель самосовершенствования (в среднем – 4, начальный стандартизованный уровень). Это означает, что мероприятия по совершенствованию проводятся регулярно, но без контроля, без установки на результат и не являются обязательной частью процесса.

3. Показатели стабильности процессов, их самосовершенствования, планирования и учёта показывают ровное, сбалансированное состояние во всех компаниях российского рынка, демонстрируя идентичность понимания и уровня развития, но средние показатели по данным факторам находятся на уровне лишь стандартизированных процессов.

4. Автоматизация процессов показывает больший, чем у иных исследуемых процессов, разброс значений. На рынке присутствуют компании как с очень высокой степенью автоматизации процессов производства ПО, так и с полным её отсутствием. Это в основном обусловлено специализацией компаний на определённых технологиях: кто-то работает с применением самых новейших стеков

и инструментов, кто-то поддерживает и кастомизирует ПО на устаревающих платформах.

5. В целом исследование показывает высокий уровень использования средств автоматизации везде, где используемый стек технологий позволяет это сделать, но на рынке существенную долю занимает устаревающее ПО, не позволяющее релевантно автоматизировать процессы разработки и поставки.
6. В отношении аспекта разделения ролей следует отметить системное отставание основной части исследуемых компаний от лидеров. Иными словами, в большинстве компаний разделение ролей проработано мало, или проработано, но не зафиксировано. И на этом фоне резко выделяются компании-лидеры, имеющие чёткие матрицы ролей, полномочий и ответственности, позволяющие чётко стандартизовать процессы и обеспечить их контроль.

Если подводить общие итоги, то можно утверждать, что результаты исследования ИТ-процессов российского рынка производства ПО показали высокую степень использования инструментальных средств и низкий уровень управления. Зрелость процессов находится под сильным влиянием со стороны бизнес-заказчиков: те процессы, с которыми они непосредственно соприкасаются, имеют более высокий уровень зрелости. Те процессы или их части, которые нужны самим менеджерам для управления (измерения, контроля, самосовершенствования) находятся на самых низких уровнях зрелости.

Явно выражена недостаточность зрелости процессов архитектуры и дизайна. Это можно назвать общей проблемой российского рынка производства ПО, приносящей в долгосрочной перспективе компаниям финансовые потери, связанные с потребностью дорогого сопровождения, решения постоянных сбоев и инцидентов, дорогой модернизацией ИТ-ландшафта и т. п.

Следующим ключевым направлением исследования стало определение готовности команд разработки к проектной работе. Изучались три составляющие: уровни обученности, готовности к проектной деятельности и культура среды разработки. Необходимо отметить, что разброс показателей по шкалам, если сравнивать результаты опросов представителей каждой компании отдельно, очень большой. Причин несколько:

- масштаб организаций и, соответственно, ресурсное и административное обеспечение;
- разноуровневая концентрация управленческих усилий на проблематике формирования проектных команд;
- субъективность восприятия требований критериев и оценки команд по ним;
- различные управленческие роли респондентов и их места в проектной структуре (т. е. взгляд на ситуацию под углом ролевого восприятия).

Этот разброс нивелируется различными статистическими методами, в том числе и опорой на средние показатели и показатели моды. Что же даёт нам аналитика?

Уровень обученности команд

1. По результатам можно говорить, что проблема подготовки команд разработки является достаточно актуальной, обучению и развитию проектных компетенций, в той или иной степени, уделяют внимание все. Но превышение среднего показателя над показателем моды (наиболее часто встречающийся показатель) говорит о наличии в отрасли компаний с выраженным лидерством в этих вопросах. Мода колеблется в диапазоне 1–3 балла по 10-балльной шкале, а среднее значение в диапазоне 5–6. Почти двукратное отличие значений определяют одни из ключевых факторов эффективности команд разработки – понимание сущности управления проектами, а также проектная слаженность. Основу конкурентного преимущества на рынке ИТ-услуг и в ИТ-сегменте рынка труда составляет возможность скорейшей проектной адаптации сотрудников, максимальное информационное обеспечение проектной деятельности (кто? что? когда? зачем?), возможность работать с современными инструментами автоматизации процессов.
2. Общение с респондентами после проведённого опроса дало основание для вывода о разных подходах к форматам обучения. Компании с большими ресурсами решают задачи обучения управления проектами в полном цикле: от теории к практикуму и далее к контролируемому применению в реальных процессах. Компании с меньшими ресурсами обучают в основном через рефлексию проектных ошибок. Ключевой проблемой результативности обучения является неспособность многих ИТ-специалистов оценивать трудозатраты и себестоимость проектов и процессов.
3. С предыдущим выводом напрямую связан и вопрос понимания принципов проектного взаимодействия и мотивации. Анализ интервью с респондентами, результаты консалтинга в ряде ИТ-компаний показывают, что для многих компаний является большой проблемой понимание сотрудниками системы мотивации, особенно финансовой. Например, в большой ИТ-структуре крупной российской компании оплата труда специалистов никаким образом не привязана ни к компетенциям, ни к результату. Сотрудники получают только оклады, размер которых не меняется длительное время. Такие подходы к стимулированию, безусловно, не позволяют управлять ни производительностью, ни эффективностью.
4. Исследования также выявили общую для большинства компаний проблему, связанную с «низкой вовлечённостью сотрудников в процессы». Только погружение в вопрос часто показывает, что это следствие, а не причина. К ключевым причинам следу-

ет отнести недостаточный и некачественный информационный обмен между членами команд и владельцами процессов или проектов (заказчиками), а также невысокий уровень развития управленческих компетенций у линейных руководителей, руководителей проектов и тимлидов. Результаты интервью показали, что многие из них считают, что вовлечённость – это только результат желания сотрудника. Своей роли в формировании вовлечённости многие руководители не понимают, об управляемости процесса приверженности к компании они даже не слышали.

Уровень готовности к проектной работе по разработке ПО

Готовность к проектной работе подразумевает понимание целей и задач, своей роли в проекте, спецификации, графиков работ, его общей модели и структуры. Для этого необходим эффективный коммуникативный обмен информацией, открытый доступ к ней. Кроме того, важен и доступ к технологиям и инструментам решения проектных задач.

Исследования показали позитивную картину, которая выразилась в достаточной однородности показателей. «Среднее» и «мода» не имеют значительных расхождений практически по всем факторам, влияющим на готовность команд разработки ПО к проектной работе. Но в то же время, наметились и проблемные факторы. Например, ключевой проблемой, по нашему мнению, является явный разрыв по качеству горизонтальных (внутрикомандных, внутрипроектных) коммуникаций и вертикальных: первые оцениваются значительно выше вторых. Кроме того, наблюдались и проблемы открытости необходимой корпоративной информации о месте и роли проекта в общей организационной системе, о принципах его ресурсного обеспечения.

Вторым настораживающим фактором становится отсутствие или размытость критериев, а следовательно, и показателей эффективности и результативности проектной деятельности. Всё это, во-многом, объясняет проблему невысокой мотивации и вовлечённости сотрудников.

Третий модуль кластера – сформированность культуры среды разработки ПО. Он включал в себя оценку атмосферы понимания сущности проекта, открытости и кооперации, взаимоподдержки и взаимопомощи, оперативного реагирования на возникающие проблемы. Результаты этого модуля также неоднородны, что может говорить о слишком разных подходах к формированию проектной среды.

В качестве причины несбалансированности культуры возможно рассматривать недостаточный контроль за реализацией делегированных тимлидам и руководителям проектов полномочий. Это приводит к отрыву их от стандартов проектного взаимодействия, формированию своих принципов управления, отличных от корпоративных. В основе подобных управленческих подходов лежит субъективность взглядов, значительная приоритезация решения процессных (проектных) задач над задачами по созданию среды для вовлечения сотрудников, люди рассматриваются лишь как средство достижения результата.

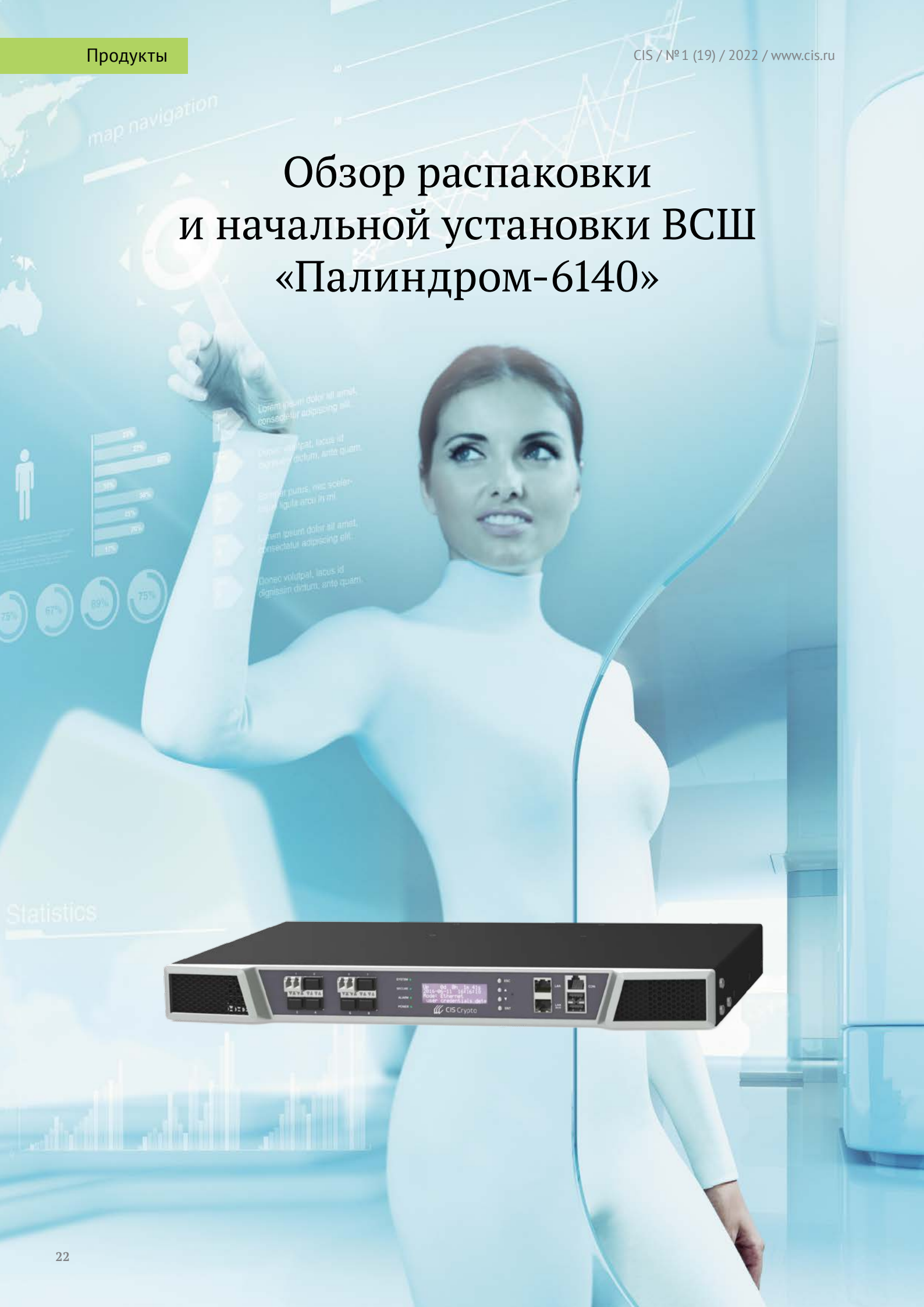
Кроме того, мы можем говорить и о наличии системных проблем в управленческой подготовке тимлидов и руководителей проектов, ответственных за оптимизацию коммуникаций, целеполагание и постановку процесса обучения в рамках проектов.

Подводя итоги, можно сказать, что ключевыми проблемами формирования зрелости команд разработки ПО являются:

- сложность определения критериев результативности деятельности;
- привязка материального стимулирования к процессу и результату разработки ПО с системами;
- балансировка внепроектных и проектных коммуникаций;
- трансформация культуры среды разработки ПО в условиях автоматизации и цифровизации процессов;
- низкий уровень управления («лень менеджеров»): больше внимания уделяется видимым (фасадным) процессам и меньше – процессам и задачам, нужным для адекватного управления;
- приоритет тактики над стратегией – в части выбора партнёров, в части предпочтения быстрого вывода продукта в эксплуатацию за счёт экономии на архитектурной проработке решений, в части принятия управленческих решений и совершенствования процессов;
- использование «чутья» и субъективных мнений работников вместо внедрения системы показателей и метрик, базирующихся на стратегических целях и задачах.

Пучкова И.О., коммерческий директор Logrocon,
Белолипецкий С.И., директор по консалтингу Logrocon,
Кармазин Т.И., директор по персоналу Logrocon

Обзор распаковки и начальной установки ВСШ «Палиндром-6140»



Распаковка

Перед нами высокоскоростной шифратор «Палиндром-6140» производства российской компании «СИС крипто». Он предназначен для шифрования трафика на L2 по алгоритмам ГОСТ в распределённых сетях Ethernet. Устройство работает в линейных и многоточечных топологиях без потерь кадров, с микросекундными задержками, практически не загружает сеть служебной информацией.

Шифратор легко встраивается в существующие сети по принципу «узел на проводе», а средства управления позволяют легко настраивать и контролировать политики безопасности. Механизмы управления групповыми ключами и разделения ролей соответствуют общепринятым практикам информационной безопасности.

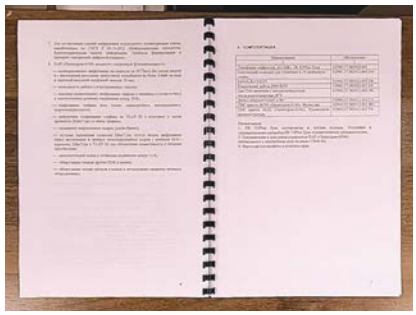
Шифратор поставляется в фирменной заводской упаковке с логотипами производителя.

На одной из боковых стенок – наклейки с названием модели, контактами производителя, серийным номером и комплектацией. Видим, что, кроме самого устройства, в комплект поставки входят модули формата SFP+, кабели питания, а также сертификат на расширенную поддержку. Таким образом, все принадлежности упакованы в одну коробку – очень удобно, ничего не потеряется. Один шифратор – одно место.

Видим, что внутри ещё одна коробка. Транспортировочная коробка может испачкаться, порваться, а внутренняя останется целой и чистой.

На внутренней коробке такие же стикеры и логотипы «СИС крипто».

Сверху лежат формуляр на устройство и два запечатанных конверта-секьюрпака. Под ними между ложементами из пенополиэтилена – коробка с принадлежностями и корпус устройства. Открываем формуляр.



На странице 7 вписан серийный номер. Сверяем его с номером на коробке, а потом и с номером на корпусе. На странице 6 приведена комплектация шифратора. Обратите внимание, что в ней перечислены только стандартные обязательные принадлежности, то есть то, что входит в первую строчку комплектации на коробке. Принадлежности, которые поставляются отдельно, перечислены на коробке. Таким образом, комплектацию нужно проверять по обоим спискам.

Например, по номеру на секьюрпаках определяем, что в них лежат USB-диски с вектором инициализации датчика случайных чисел.

Остальные принадлежности лежат в этой коробке.

Принадлежности

Тут и стандартные, и дополнительные принадлежности – те, что поместились. Смотрим и сверяем по списку.

Пара кабелей питания – это дополнительные принадлежности, в формуляре их нет, шифратор можно заказать и без них. В общем, подойдут любые кабели с разъёмом C13.

То же самое касается и интерфейсных модулей SFP+ (они же приёмопередатчики, или трансиверы). В каталоге «СИС крипто» есть таблица совместимости, так что можно использовать трансиверы, выпущенные под любым брендом, но с нужными кодами.

Вот так выглядят сертификаты на расширенную поддержку – по одному на каждый год.

Кабель RJ45-RJ45 для управления через сеть. Одним концом – в порт управления, другим – в коммутатор либо напрямую в станцию управления.

Консольный кабель. Разъём RJ45 – в консольный порт шифратора, разъём DB-9 – к терминалу или модему.

Сейчас, разумеется, в качестве терминала все используют персональный компьютер с программой-эмулятором. Если на компьютере нет такого разъёма, то потребуется адаптер USB – в поставке его нет.

Это монтажный комплект для 19-дюймовой стойки. Где винты? Прикручены к корпусу устройства.

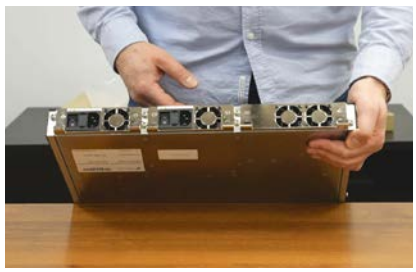
Это диск с руководством администратора и программой управления. Теперь переходим к самому устройству.

Платформа шифратора

Перед нами 19-дюймовый 1-юнитовый корпус специализированной платформы высокоскоростного шифратора. Корпус опломбирован специальными наклейками с контролем вскрытия, отрывать эти пломбы запрещено. Кроме того, в шифраторах «Палиндром» есть механизм противодействия взлому. Если снять эту крышку, то срабатывает датчик и шифратор сбрасывается в заводские настройки. Обратите внимание, что в корпусе нет сквозных отверстий, через которые можно было бы воткнуть щуп и добраться до электронных схем.

На нижней панели есть стикер с названием модели и серийным номером – проверяем его.

На задней панели есть вентиляторный модуль и пара дублированных блоков питания с тумблером и стандартными разъёмами C14.



Блоки питания универсальные, рассчитаны на переменное напряжение от 100 до 250 вольт и частоту от 50 до 60 герц, автоматически подстраиваются под входное напряжение. Устройство должно было подключено к заземлённым розеткам. Рекомендуется подключать его к источнику бесперебойного питания. Но даже если питание пропадает, то настройки не стираются, шифратор автоматически восстановит все защищённые соединения, как только питание будет подано снова. Вмешательство пользователя не потребуется.

Блоки питания работают по схеме «активный-активный»: когда оба блока подключены к сети, каждый из них подаёт питание на устройство, и нагрузка распределяется. Если один блок питания выходит из строя, то другой примет на себя всю нагрузку, пока неработающий блок не будет заменён. Несмотря на «горячую» замену, блок питания не подлежит обслуживанию пользователем и должен быть возвращён поставщику для замены. Крепится блок двумя винтами.

Теперь посмотрим на вентиляторный модуль, он тоже с «горячей» заменой и тоже прикручен двумя винтами.

В шифраторе «Палиндром-6140» используется встроенная литиевая батарея для питания часов реального времени и энергонезависимой памяти с информацией о конфигурации. Эта батарея имеет срок жизни свыше 10 лет. Напряжение батареи постоянно контролируется. Если батарея разряжена, то регистрируется аварийное состояние и индикатор на передней панели загорится красным. Батарея находится в модуле вентилятора и заменяется вместе с ним.

Вот что расположено на передней панели.

Вентиляционные решётки. Гнёзда для интерфейсных модулей SFP+. Слева так называемый локальный порт, который идёт к доверенному, контролируемому сегменту сети, подключается обычно к коммутатору или маршрутизатору. Трафик на этом порту не зашифрован.

Справа так называемый сетевой порт, он идёт к внешней (незащищённой) сети, трафик в которой и нужно зашифровать, потому что его можно перехватить. Этот порт обычно подключается к оконечному оборудованию сети оператора. На другой стороне неконтролируемой сети – другие такие же шифраторы (их может быть много). То есть шифратор включается в разрез сети и соединяет её физически защищённые и незащищённые сегменты, при этом сам он остаётся невидимым для трафика на L2 – это и есть принцип «узел на проводе».

Светодиодные индикаторы, которые показывают состояние устройства.

SYSTEM – сигнализирует об аварийном остановке шифратора (например, если он взломан). Сейчас горит зелёным – значит, все в порядке.

SECURE – режим работы шифратора. Горит красным – устройство не активировано и находится в режиме Discard, то есть будет сбрасывать весь трафик, который идёт во внешнюю сеть. Включать этот шифратор в рабочую сеть пока нельзя, потому что он заблокирует весь внешний трафик.

ALARM – сигнализирует о тревогах, в том числе о неотмеченных. Сейчас мигает – значит, есть неотмеченные тревоги. POWER – питание, горит зелёным.

Четырёхстрочный ЖК-дисплей для отображения информации. Белая подсветка означает исправность, красная – аварийный останов.

Кнопки для ввода. ESC отменяет предыдущие нажатия, стрелка вверх – вверх по меню (или, если мы в режиме ввода, последний доступный выбор для подсвеченного символа). Стрелка вниз – вниз по пунктам меню или же следующий доступный вариант для ввода символа. ENTER – вход в пункт меню или подтверждение выбора символа.

Кнопка стирания – не нужно путать стирание со сбросом. При сбросе удаляются только соединения и их политики, при этом шифратор остаётся активированным. Стирание – это возврат к заводским установкам, при этом стираются все сертификаты и учётные записи пользователей.

«Палиндром-6140» можно стереть несколькими способами. Первый – это удерживать кнопки ESC и ENT в течение 10 секунд до появления надписи **Erase and reboot?**

После этого нажать стрелку вверх и потом кнопку ENT. Нажатие других кнопок отменяет операцию. Второй способ, который используется, когда на устройстве нет питания – это нажать кнопку стирания, которая находится в отверстии рядом со стрелками вверх и вниз. Для этого понадобится скрепка или подобный мелкий предмет.

Также шифратор можно стереть из консоли командой erase.

Разъёмы RJ45 Ethernet с автоматическим согласованием скорости для управления по протоколу SNMPv3.

Разъём RJ45 RS-232 для управления через интерфейс командной строки. К нему последовательным кабелем подключается консоль.

Разъёмы USB для загрузки инициализирующей последовательности датчика случайных чисел и обновления встроенного программного обеспечения. Вот и всё.

Ссылка
на видеообзор
распаковки

РТП-Медиа: современная платформа дистрибуции ТВ-сигналов

Миронов Вячеслав Анатольевич
руководитель компании РТП-Медиа

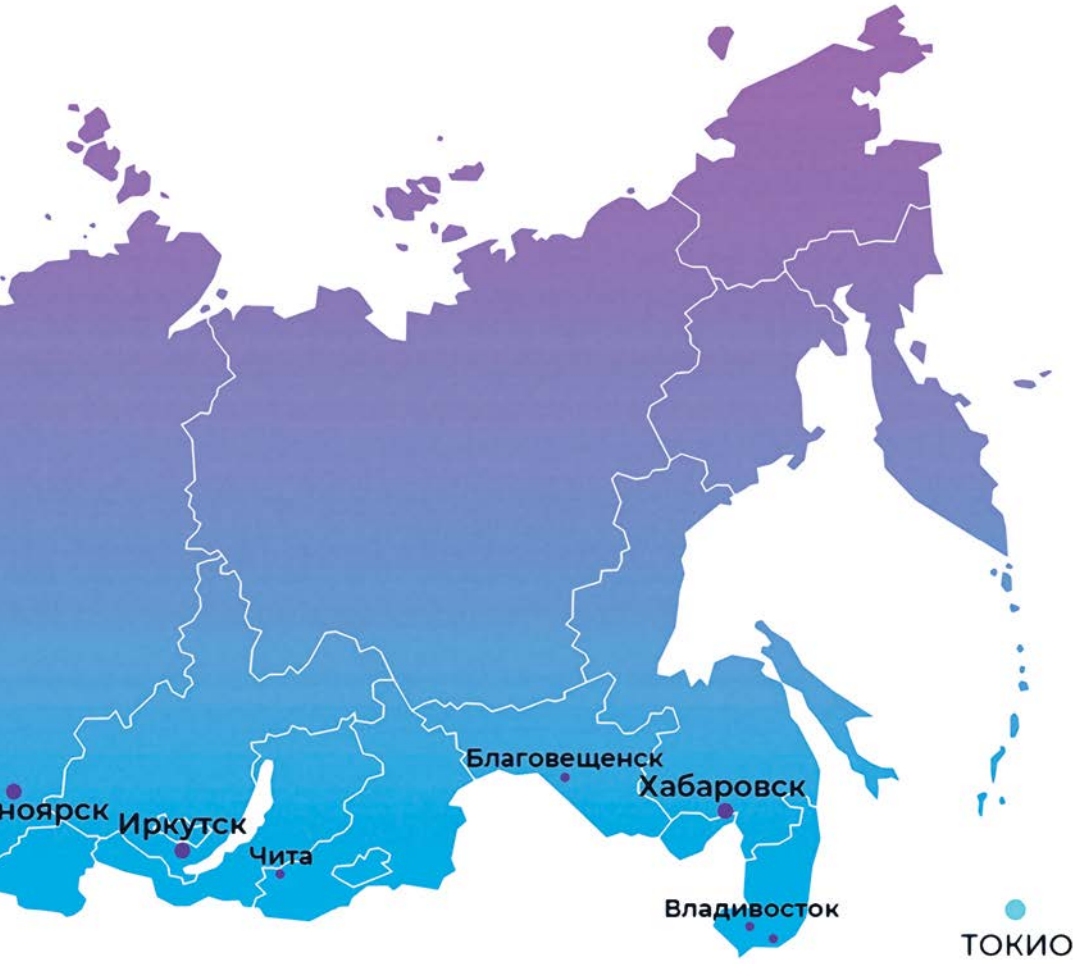
Вы когда-нибудь задумывались о том, какой путь проходит контент телеканала, чтобы зритель смог его увидеть? Наверняка нет. А ведь это целая история!

На сегодняшний день на российском рынке телеком и медиа представлено более 600 телеканалов отечественного и зарубежного производства, и существует более 2000 операторов ТВ-вещания как крупнейшие в стране федеральные и региональные компании, так и OTT-сервисы, доступные не только в нашей стране. Телеканалы заинтересованы в максимальном охвате аудитории и высоких рейтингах просмотра, в то же время операторы хотят получать в свою сеть востребованный контент в хорошем качестве, за который абоненты готовы платить. При этом пересечение интересов данных игроков индустрии далеко не всегда означает готовность идти навстречу друг другу. Каким же образом тогда в операторских сетях появляются телеканалы? Вот тут в игру вступаем мы. «РТП-Медиа» – это центровое звено в «круговороте контента в природе», которое связывает телеканалы и операторов и помогает доставлять контент из точки А в точку В.

Приём сигнала телеканала

Оптимальный способ приёма сигнала – это его получение из аппаратной или студии телеканала, поскольку именно такой способ гарантирует сохранение исходного качества сигнала. Также доступны способы приёма сигнала через спутник или с помощью Интернет-протоколов. За счёт наличия у компании «РТП-Медиа» собственной обширной волоконно-опти-

ГЕОГРАФИЯ УСЛУГ



РПТ-Медиа осуществляет доставку сигналов по всей России, в страны Балтии, СНГ и дальнего зарубежья.

ческой сети в Москве и Подмосковье порядка 80% сигналов телеканалов мы забираем «по земле» напрямую из студий. Остальные телеканалы принимаем на нашу платформу через Интернет-среду (по протоколам SRT, Zixi, RTMP, HLS и др.) или с помощью собственного антенного поста, оснащённого 17 спутниковыми антеннами, принимающими сигналы со спутников на позициях от 90о в. д. до 15о з. д.

Обработка сигнала

Поскольку принимаемые сигналы могут быть разных форматов, для дальнейшей их доставки или по индивидуальному запросу от оператора требуется сначала их обрабатывать: конвертировать из одного формата в другой, производить upscale (повышение разрешения кадров) или downscale (понижение разрешения кадров), энкодировать или декодировать, нормализовать звук и многое другое. Для осуществления данных процедур требуется не только соответствующее современное оборудование и программное обеспечение, но и квалифицированные кадры.

Доставка сигнала

Подготовленные сигналы теперь готовы к передаче оператору вещания. В зависимости от удалённости последнего и наличия/отсутствия прямых каналов связи или стыков с оператором в точках обмена трафиком выбирается оптимальный способ доставки: посредством собственных выделенных оптических волокон, с помощью виртуальных каналов связи (L2), через CDN сеть или Интернет. Современные технологии позволяют передавать сигналы в самые удалённые точки Земли, где есть доступ в Интернет.

Мониторинг качества

Основная задача при передаче телевизионных сигналов – осуществить доставку с гарантированным качеством и без потерь. Для этих целей на платформе «РТП-Медиа» осуществляется разносторонний мониторинг качества сигнала на разных этапах его доставки: на приёме сигнала, перед его выдачей, мониторинг сигнала по прохождению на узлах нашей сети и мониторинг на стороне клиента, если есть возможность установить собственное оборудование в точке выдачи. При этом служба технической поддержки функционирует в режиме 24/7 и находится в непосредственной близости от приёмопередаточного оборудования, что способствует самому скорейшему решению любых вопросов и проблем, связанных с доставкой сигналов.

В 2020 году «РТП-Медиа» построила собственный телекоммуникационный ЦОД площадью 100 кв. м., оснащённый самым современным оборудованием. Уровень надёжности дата-центра соответствует TierII/TierIII, в SLA составляет 99,99%.

Правовая сторона вопроса

До появления телеканала на нашей платформе требуется не только технически принять сигнал, но и получить официальное разрешение от телеканала на доставку его сигналов до операторов спутникового, кабельного, IPTV и OTT-телевидения. А каждый факт выдачи сигналов операторам сопровождается направлением соответствующего уведомления телеканалам. При этом операторы, желающие получить сигнал в свою сеть, сами напрямую связываются с правообладателями для заключения договорных отношений. Мы же на себя берём все вопросы, связанные с технической доставкой сигнала.

География услуг

За 5 лет «РТП-Медиа» сумела собрать на своей платформе более 700 сигналов телеканалов и их версий, а также расширить свою сеть до 50 городов присутствия в России. Благодаря наличию особого оборудования и технических специалистов доставка сигналов может осуществляться не только по нашей стране, но и в страны СНГ, Балтии, ближнего и дальнего зарубежья.

Планы на будущее

«В планах компании на ближайшие несколько лет дальнейшая экспансия в регионы РФ: организация точек присутствия в городах с населением 100000+. И как результат такой работы – организация собственной CDN-сети, специализирующейся на передаче потокового видео.

Технологическое развитие компании всегда в приоритете. Мы смотрим не только на востребованные услуги в настоящее время, но и работаем на перспективу, предвидя колебания спроса в будущем. Так, в наши планы входит развёртывание собственного облачного транскодинга, который позволит осуществлять функции формирования сигнала для различных OTT и стриминговых сервисов, популяризация которых растёт с каждым днём. Уже сейчас конечный потребитель ТВ-контента имеет доступ (то есть платит за услугу) как минимум к 2–3 онлайн-кинотеатрам и/или стриминговым сервисам. И эта тенденция будет только усиливаться.

Работая с телеканалами не только отечественного, но и зарубежного производства, мы получаем много запросов по услуге Playout, когда сигнал телеканала, прежде чем выходить в эфир, изначально формируется у нас на платформе. Объёмы по данной услуге будут только увеличиваться, в том числе за счёт развития сервиса облачного плейаута.

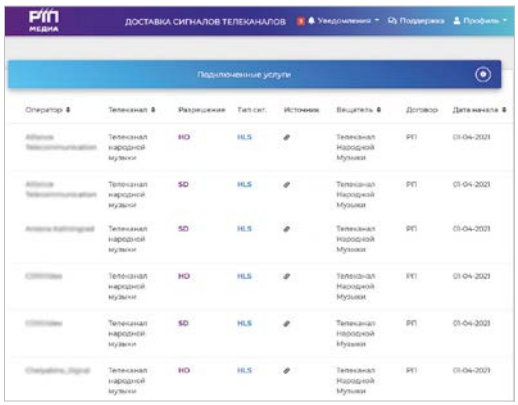
Скорость развития и модернизации современных технологий за последние десятилетия стала расти с геометрической прогрессией. И теперь, чтобы шагать в ногу со временем, приходится бежать».

Вячеслав Анатольевич Миронов
Руководителя компании РТП-Медиа

«РТП-Медиа»

119071, Москва, ул. Малая Калужская 15, стр. 16

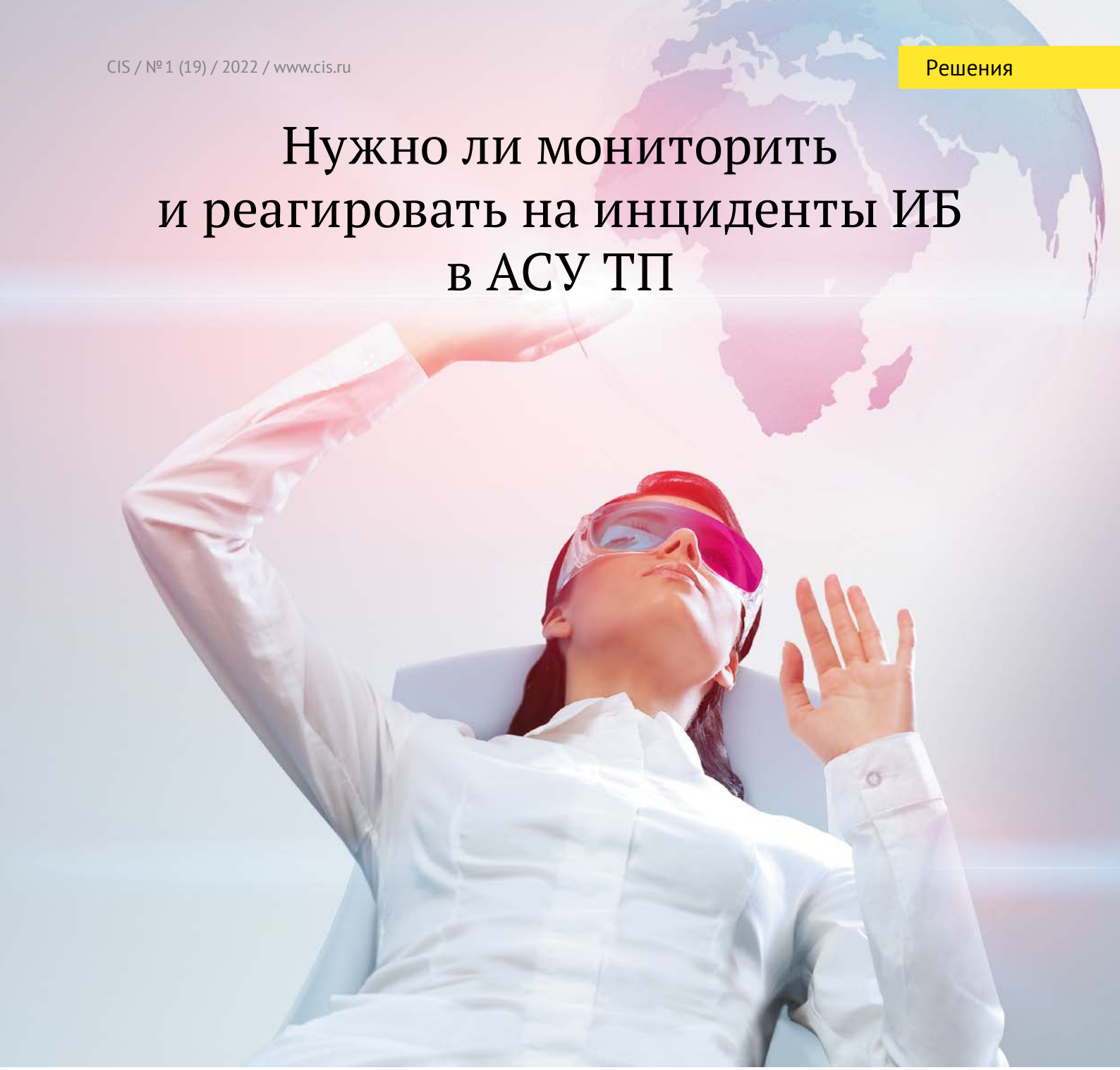
+7 (495) 3208080
info@rtp.media
www.rtp.media



Для удобства операторов вещания создан онлайн-портал с доступом в личный кабинет, где оператор может не только выбрать нужные сигналы телеканалов для доставки из общего списка, но и посмотреть всю информацию, касательно уже действующих выдач.

С целью защиты контента правообладателей (телеканалов) от несанкционированного распространения была внедрена новая технология – нанесение цифровых водяных знаков. Это простой и оперативный способ защиты контента от пиратства: вставка невидимых глазу «меток», по которым можно идентифицировать оригинальный контент.

Нужно ли мониторить и реагировать на инциденты ИБ в АСУ ТП



Руслан Амиров
директор USSC-SOC – центра мониторинга и реагирования на инциденты ИБ компании УЦСБ

Рассмотрим один немаловажный вопрос для промышленных объектов: нужно ли организовывать мониторинг информационной безопасности (ИБ) в автоматизированных системах управления технологическими процессами (АСУ ТП).

Следует обозначить, что для предприятий промышленного сектора наблюдается растущий с каждым годом интерес злоумышленников к промышленным объектам и, как следствие, рост числа кибератак. Также возрастают требования законодательства РФ, которые активно конкретизируются регуляторами. В то же время со стороны самих предприятий возрастает понимание необходимости общеуровневых изменений ИБ-инфраструктуры, повышение эффективности ИБ- и ИТ-подразделений и, конечно, целевое снижение рисков реализации угроз ИБ.

О наиболее эффективных инструментах мониторинга ИБ АСУ ТП, основных сложностях, существующих ограничениях и роли Security Operations Center (SOC) рассказывает Руслан Амиров, директор USSC-SOC – центра мониторинга и реагирования на инциденты ИБ компании УЦСБ.

Нужно ли организациям с АСУ ТП осуществлять мониторинг ИБ? Что является результатом мониторинга, можно ли снизить риски?

Данные вопросы являются первичными для любого бизнеса, и развёрнутый ответ требует учёта многих аспектов и должен рассматриваться в широком ключе возможностей.

Выделим ключевые моменты.

Во-первых, мониторинг позволяет обоснованно реализовать соответствие требованиям законодательства. Для организаций действует Федеральный закон 187-ФЗ «О критической информационной инфраструктуре Российской Федерации», приказы ФСТЭК России № 31, № 235, № 239 и прочие подзаконные акты, которые задают вектор обеспечения ИБ АСУ ТП и объектов критической информационной инфраструктуры (КИИ) в РФ. За невыполнение требований законодательства в сфере защиты информации предусмотрена уголовная и административная ответственность, в том числе присутствует и ряд принятых судебных решений.

Во-вторых, мониторинг предоставляет объективную оценку состояния защищённости АСУ ТП в режиме, близком к реальному времени, – режиме, который, конечно, зависит от условий SLA. Причём полученная оценка управляема, и её изменение достижимо посредством экспертного подхода к реагированию на выявленные негативные сдвиги.

В-третьих, требуется выявлять инциденты не после того, как они были зафиксированы, а чётко знать заранее, где именно и какой инцидент может возникнуть и по какой причине. В ходе анализа изменений АСУ ТП в ряде случаев можно превентивно определить, приведут ли последующие действия к инцидентам. Это сложная аналитическая работа, требующая понимания как особенностей функционирования АСУ ТП, так и имеющихся связей между различными АСУ ТП, их подсистемами и внешними по отношению к АСУ ТП системами и сетями.

В-четвёртых, система мониторинга ИБ должна осуществлять сбор и обработку значительных объёмов информации с высокой скоростью, ведь в конечном итоге цель заключается в том, чтобы максимально оперативно обеспечить реагирование на возможный инцидент ИБ (или угрозу инцидента) и не допустить или в исключительных случаях существенно снизить потенциальный ущерб в случае наступления инцидента. Причём система мониторинга ИБ не исключает собственный мониторинг АСУ ТП, органично дополняя технологический мониторинг, ведь реагирование в АСУ ТП производится обслуживающим персоналом, который глубоко разбирается в строении защищаемой системы и её процессах, может оценить влияние того или иного действия и принять правильное решение в критической ситуации.

В-пятых, необходимо учитывать такую цель мониторинга, как выявление инцидентов, которые уже произошли. Причём своевременная доставка сведений об инциденте ИБ ответственным подразделениям предприятия с понятным изложением выявленной ситуации играет ключевую роль в нейтрализации инцидентов и их возможных последствий. Взаимодействие между теми, кто осуществляет мониторинг, и выстраивание такого взаимодействия – обязательное условие для качественного мониторинга без учёта того, задействован ли собственный или внешний SOC в процессе мониторинга.

В-шестых, после выявления инцидента в рамках мониторинга проводится расследование и при необходимости восстановление хронологии событий, предшествующих возникновению инцидента. Эта информация критически важна для улучшения этапа реагирования и обязательно требуется при ликвидации возможных последствий инцидента, в связи с чем важно обеспечить своевременную локализацию инцидента.

Как правило, организации уровня Enterprise сегодня уже используют некоторые базовые средства и подходы к управлению и реализации ИБ. В случае с АСУ ТП, какие сложности могут возникнуть со стандартными SecOps?

Это ещё один традиционный вопрос по стратегической и операционной составляющим безопасности АСУ ТП. Сосредоточимся на тех самых составляющих, которые на регулярной основе существуют в АСУ ТП.

Обновление ПО

Без должной подготовки нельзя обновить базовое и прикладное программное обеспечение (ПО) АСУ ТП или ПО наложенных средств защиты информации. Преимущественно экспоненциально растут риски невозможности функционирования АСУ ТП после проведения стандартных операций по обновлению операционных систем (ОС) или средств антивирусной защиты. Особенно проблематичным обновление становится в отношении устаревших ОС.

Ограниченные сроки на техническое обслуживание АСУ ТП

Техническое обслуживание (ТО) традиционно производится в период вынужденного или планового останова АСУ ТП. Например, выделяются 1 сутки (или даже меньше) на выполнение ТО, причём не всё время необходимые компоненты АСУ ТП доступны для проведения работ.

Высокий риск ошибок при проведении ТО по ИБ

Данный пункт возникает как следствие из предыдущего и зависит, в том числе, от предыдущих двух пунктов: во время ТО могут быть некорректно уточнены параметры мониторинга ИБ и до следующего ТО АСУ ТП останется невидимой для SOC или подразделения, отвечающего за мониторинг и реагирование на инциденты ИБ.

Сложно получить данные с активов АСУ ТП

Сложности связаны с отсутствием штатных решений и механизмов для получения данных в АСУ ТП, с отсутствием возможности внесения изменений в АСУ ТП для передачи необходимых данных. Появляется потребность в применении специализированных средств мониторинга ИБ АСУ ТП. Также сложности вносят нестандартные протоколы передачи информации программных решений для функционирования АСУ ТП.

Проблематичная изоляция устройств из состава АСУ ТП, в отношении которых зарегистрирован инцидент ИБ

Часто отсутствует возможность изоляции компонента АСУ ТП в штат-

ном режиме работы АСУ ТП: в случае регистрации инцидента в АСУ ТП не всегда присутствует возможность изолировать устройство из состава АСУ ТП без прекращения работы всей АСУ ТП, что ведёт к незапланированному останову системы.

Ограничения для проведения полноценного расследования инцидента

Затруднительно провести полноценное расследование потенциального, ещё не подтверждённого инцидента: на этот процесс влияет ограниченный доступ к отдельным компонентам АСУ ТП и часто отсутствие возможностей передачи телеметрии для мониторинга и анализа.

Риски влияния средств мониторинга на компоненты АСУ ТП

Если для реализации мониторинга планируется взаимодействие, в рамках которого инструмент для мониторинга требует установки специального ПО (агента) на устройства АСУ ТП, то присутствует риск негативного влияния на функционирование АСУ ТП. Аналогичное влияние может оказывать наложенное средство защиты информации без прохождения должной процедуры тестирования совместимости с АСУ ТП.

Отсутствие вариантов передачи информации за пределы АСУ ТП

Причиной являются узкие низкоскоростные каналы связи, ограничение или отсутствие возможности подключения внешних носителей информации в пределах контура АСУ ТП. В результате довольно сложно получить информацию из АСУ ТП.

Проблематично выполнение рекомендаций по противодействию инциденту ИБ в АСУ ТП

Реагирование или дальнейшие действия по расследованию инцидента ИБ могут быть отложены до следующего технологического останова, который для некоторых систем наступает только раз год.

Отсутствие понимания эталонного состояния ИБ АСУ ТП

Сложно определить безопасное состояние системы в отсутствие разработчиков АСУ ТП или компетентных в вопросах функционирования АСУ ТП ответственных лиц.

Какие действия в АСУ ТП лучше выполнять самостоятельно или необходимо полностью полагаться на outsource-службы?

Выбор действий, которые следует выполнять самостоятельно, зависит от того, какой формат SecOps используется в вашей организации: inhouse (собственные подразделения и мощности) или outsource (внешняя экспертная организация). Также существуют гибридные варианты, при которых внутренние службы занимаются закреплённым объёмом обязанностей (например, реагированием), а внешний аутсорс осуществляет выявление инцидентов. Рекомендую организациям самостоятельно принимать решения по следующим вопросам:

1. Повышать уровень защищённости, выбирать способы защиты и решать вопросы привлечения собственных специалистов, аутсорс/аутстафф или же выбрать гибридную основу.
2. Останавливать или не останавливать функционирование АСУ ТП в случае инцидента.
3. Координировать регламентные работы по ИБ, участвовать в расследовании и ликвидации последствий инцидентов.

В случае если организация приняла решение о необходимости SOC в рамках своей ИБ-стратегии, какой SOC для АСУ ТП вы советуете выбирать: собственный или аутсорсинговый?

Выбор между созданием собственного SOC или выбором аутсорсинга данной услуги определяется исходя из практической ситуации с кадровым обеспечением, а также возможностями создания соответствующих технической и организационной структур. Чтобы определить нужный тип Security Operations Center для вашей промышленной инфраструктуры, предлагаю ответить на следующие вопросы:

1. Сможет ли собственное ИБ-подразделение технически отслеживать состояние ИБ АСУ ТП.
2. Присутствует ли готовность вкладываться в приобретение специализированных программных средств, а также в собственные кадровые ресурсы, которые будут заниматься только вопросами ИБ АСУ ТП в круглосуточном режиме и без выполнения других обязанностей.
3. Планируется ли поддерживать компетенции собственных сотрудников посредством обучений, мастер-классов, тематических конференций.
4. Имеется ли готовность самостоятельно поддерживать необходимый уровень технической оснащённости системы мониторинга, включая масштабирование такой системы.
5. Планируется ли развитие системы мониторинга ИБ АСУ ТП: внесение актуальных сценариев обнаружения, расширение области мониторинга, добавление новых источников, оптимизация способов нормализации и хранения результатов мониторинга.
6. Планируется ли отслеживать тенденции в области ИБ АСУ ТП, мониторинг сведений сервисов Threat Intelligence, отраслевых новостей и оперативно реагировать на изменения внешней среды.

Если на все вопросы получены уверенные положительные ответы, то inhouse-SOC будет эффективным инструментом для реализации вопросов мониторинга и реагирования на инциденты АСУ ТП. Однако, если хотя бы один из ответов был неопределённым или отрицательным, рекомендую обратить внимание на аутсорсинговые SOC, которые могут обеспечить требуемый или минимальный необходимый функционал мониторинга и реагирования. Кроме того, стоимость подключения к аутсорсинговому SOC будет существенно ниже, чем стоимость строительства и поддержки собственного SOC: при этом не стоит забывать о стоимости устранения последствий реализации угроз ИБ для имеющихся АСУ ТП.

Руслан Амиров, директор USSC-SOC – центра мониторинга и реагирования на инциденты ИБ компании УЦСБ.

soc.ussc.ru
soc@ussc.ru

Борис Иванович Щербаков
Вице-президент
и генеральный директор
Dell Technologies
в России

Dell и экология

В основе бизнеса Dell Technologies лежит концепция устойчивого развития, которая является комплексной и многофакторной. Одной из важнейших проблем, решаемых в рамках данной концепции, является борьба с изменением климата.

Изменение климата в результате деятельности человека – экономическая, социальная и экологическая проблема, вероятные негативные последствия которой вполне очевидны. Ближайшие десять лет определят наш успех в борьбе с изменением климата. Все государства-члены Организации Объединённых Наций в 2015 году приняли планы в области устойчивого развития на период до 2030 года, представляющие собой указание общих целей для сохранения планеты и процветания людей как сейчас, так и в будущем. Основу коллективных глобальных мер составляют 17 целей в области устойчивого развития. Инвестируя в «зелёные технологии», бизнес и правительства получают возможность внедрять ряд инноваций, которые ускоряют переход к углеродной нейтральности, создают устойчивые производства и целые сектора экономики с большим количеством новых рабочих мест.

Изменение климата – глобальная проблема!

Последствия климатических изменений гораздо ближе, чем кажутся: они не в отдалённом грядущем, они уже проявляются здесь и сейчас, оказывая растущее давление на государственный, частный и гражданский сектор. Большинство руководителей (91% по данным опроса Deloitte) говорят, что их компании уже почувствовали влияние изменения климата, а 77% – отмечают, что руководство их организаций очень обеспокоены изменением климата.

С этим глобальным вызовом и с его последствиями мы можем справиться, если применим конвергенцию инновационных технологий и обеспечим тесное сотрудничество всех заинтересованных сторон. Задача вполне решаемая. Межправительственная группа экспертов по изменению климата (МГЭИК) прогнозирует, что выбросы парниковых газов к 2030 году станут меньше на 45% и планируют достижение нулевого уровня к 2050 году.

Изменение климата приводит к тому, что и государственный и частный секторы во всём мире вынуждены брать на себя более серьёзные обязательства. Обязательства, взятые на себя Dell Technologies, не ограничены минимизацией негативного воздействия на окружающую среду от деятельности самой компании. Мы активно боремся за аналогичные результаты в деятельности заказчиков, партнёров и всего мирового сообщества. Dell Technologies нацелена на ускорение перехода к производствам замкнутого цикла, на защиту планеты и всестороннюю поддержку людей, взаимодействующих с нашей продукцией.

Мы в Dell Technologies приветствуем все компании и альянсы, ставящие перед собой цели природосбережения. Dell поддерживает работу The Climate Group, и мы согласны с тем, что необходимо принимать срочные меры, чтобы избежать худших последствий изменения климата. Компания является членом We Mean Business – коалиции, которая стимулирует действия бизнеса и продвигает программы ускорения перехода к нулевым выбросам углерода. Корпоративные закупки из возобновляемых источников энергии могут сыграть важную роль в поддержке восстановления европейской экономики после пандемии COVID-19.

Сокращение выбросов и переход к замкнутому циклу

Для борьбы с изменением климата нужно радикально сокращать выбросы углекислого газа и уменьшать нагрузку на природные ресурсы при создании продуктов. Во-первых, нужно минимизировать углеродный след уже сейчас, во-вторых, начать переход к замкнутому циклу, что предусматривает полное устранение отходов в процессе производства.

На сектор высоких технологий сегодня приходится лишь порядка 2% глобальных выбросов, однако и это совсем не мало. Ежегодно в мире пополняют 50 млн тонн электронных отходов. При имеющейся динамике к 2050 году будут производить уже 120 млн тонн ежегодно. По данным за 2019 год было переработано только 17,4%, причём из них повторно было использовано лишь 8,6% металла и пластика.

Отработка в «хай-тех» новых технологий и процессов для минимизации или даже для полного устранения выбросов – возможность более эффективно влиять на остальные 98%. Как показывает практика, придётся решить ряд подзадач, в частности обеспечение устойчивости, экологичности продуктов и услуг, сокращение выбросов как непосредственно на производстве (в идеале – переход на использование замкнутого цикла), так и во всех в цепочках поставок.

Цели, поставленные Dell Technologies на период до 2030 года, предусматривают уменьшение энергоёмкости производства, а также сокращение выбросов парниковых газов на предприятиях компании и в цепочке поставок продукции. Компания взяла на себя обязательство к 2050 году достичь нулевых выбросов парниковых газов. Мы стремимся контролировать любые отходы, возникающие в результате деятельности компании, а также рачительно относиться к любым ресурсам, которые нужны в процессе производства.

Для перехода к производству замкнутого цикла нужно неукоснительно соблюдать принципы устойчивого развития на всех этапах жизненного цикла продуктов: в устройства закладывать экологичные принципы на этапе проектирования, обеспечивать экологичность от производства продукта до его использования и последующей переработки. Dell Technologies придерживается данного подхода, обеспечивая соблюдение этих принципов во всём, что мы производим.

Замкнутый цикл представляет собой концепцию повторного использования ресурсов, технически реализованную «на максималках». Концепция, заметим, давно проникает в индустрию: за последние 50 лет в мире вторичное использование материалов увеличилось почти в четыре раза – с 26,7 до 100 млрд тонн. Как предполагают аналитики, тренд на повторное использование будет восходящим, и к 2050 году соответствующий объём вырастет 170–184 млрд тонн.

Население мира растёт, и, согласно прогнозам, к 2030 году достигнет 8,5 млрд. Это приведёт к увеличению спроса на продукты и услуги, что, если не будут предприняты соответствующие меры, окажет огромное давление на естественные экосистемы по всей планете.

Данные, технологии, экология и города

Изменения должны коснуться как индустрии, так и городских пространств. «Умные города» играют решающую роль в повышении безопасности, чистоты и устойчивости городской среды. Государственный и частный секторы могут способствовать экономическому возрождению городских территорий, созданию экологичных городских пространств, идущих по пути устойчивого развития.

Технологические компании должны играть практическую роль в обеспечении устойчивого развития городов. Применение ИТ-инструментов, работа с данными и технологиями способны революционизировать управления городами, в частности позволяя использовать ресурсы более рационально. Благодаря возможностям гибридного облака, датчикам интернета вещей и EDGE-вычислениям городское управление может анализировать данные в режиме реального времени и незамедлительно принимать меры. Например, решения Dell Technologies помогают в управлении дорожным трафиком с помощью интеллектуальных светофоров, способных оптимизировать транспортные потоки, что приводит к экономии времени водителей и к существенному сокращению углеродного следа городов.

Данный тренд будет восходящим: сотовые сети пятого поколения, вычисления на границе сети (EDGE) и искусственный интеллект обеспечат сбор, анализ огромных объёмов данных и мгновенные действия на основе полученной информации. Новые технологии обеспечат широкие возможности устойчивого развития в современных городах. Но требуется оптимизация внутри ИТ-решений, например развёртывание EDGE-вычислений сократит поток избыточных данных в ЦОД, что уменьшит потребности в охлаждении и обеспечит более устойчивое управление данными.

А что в России?

Уровень внедрения «зелёных технологий» в стране вряд ли можно охарактеризовать как высокий, как считают эксперты, также и проникновение экологичных решений идёт неравномерно. Однако в настоящее время в России происходит активизация технологической деятельности в рамках проектов по развитию инновационной экономики. Создают новые программы, в том числе на федеральном уровне разрабатывают планы и принимают законы.

Вступили в силу национальные «зелёные стандарты» с комплексным подходом к энергоэффективности, ресурсосбережению, экологической безопасности и комфортным условиям среды жизнедеятельности человека. Стандартами прописаны «зелёные термины» и определения, классифицированы актуальные признаки «зелёных технологий». За основу стандартов были взяты положения из международных аналогов, которые существенно переработали и дополнили уникальными наукоёмкими подходами.

Все понимают необходимость перенаправления экономики в сторону экологически ориентированного роста, разработки и внедрения инновационных ресурсосберегающих и экологически безопасных технологий. Растут инвестиции в экологические инновации, в том числе и со стороны российского бизнеса, создают различные институты развития инновационной экономики. Оформлена выраженная тенденция к развитию «зелёной энергетики», проникновению технологий энергосбережения и разработки электромобилей. Развитие экологических технологий в России имеет большие перспективы в случае реализации намеченного.

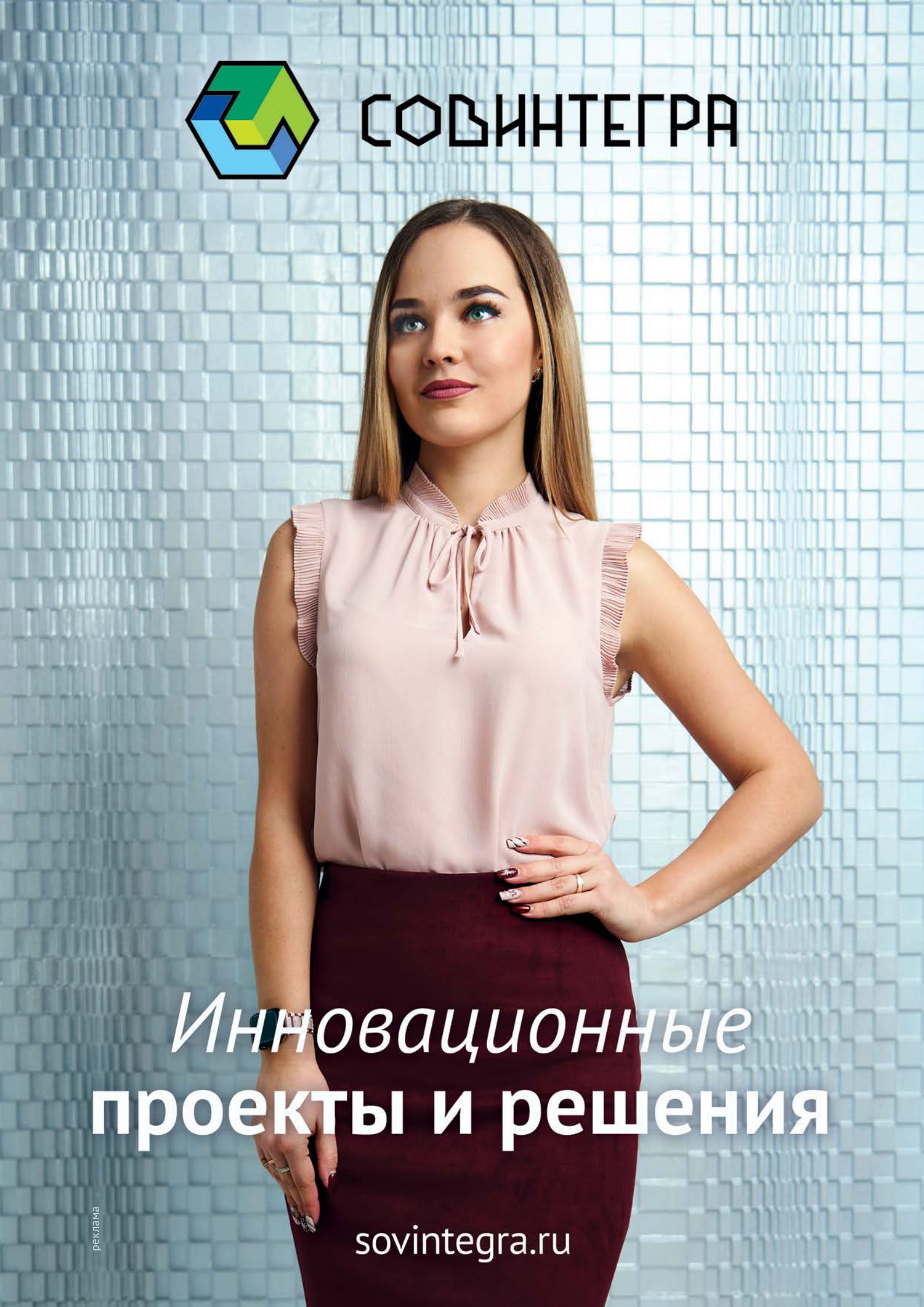
Глобальное сотрудничество

Мы уверены, что глобальное сотрудничество является ключевым элементом для достижения успеха. Сотрудничество – это метод, а технологии – средство.

Правительства, компании и гражданское общество должны сотрудничать, чтобы устойчивое развитие стало реальностью. Роль государственного сектора выходит за рамки общего управления и законотворчества: всесторонняя поддержка в развитии инновационных технологий, контроль за углеродным следом и снижение нагрузки на природные ресурсы будет иметь очень большое значение. Но для этого требуются колоссальные многосторонние усилия предприятий, правительств и организаций по всему миру.

В процессе цифровой трансформации (DX), которая затрагивает индустрию, транспорт, логистику, городскую среду и другие направления, должны быть внедрены различные решения для устойчивого развития и экологически чистых ИТ. DX, ориентированная на автоматизацию и работу с большими данными, будет играть центральную роль в обеспечении устойчивого развития всего общества. Помимо создания новых продуктов, добиться целей помогут инновационные бизнес-модели и технологии, такие как облачные вычисления, виртуализация и интернет вещей (IoT). Нам всем необходимо работать вместе над глобальной проблемой изменения климата, а также другими направлениями устойчивого развития и экологической повестки.

Борис Иванович Щербаков,
вице-президент и генеральный директор
Dell Technologies в России


СОВИНТЕГРА
Инновационные
проекты и решения
sovintegra.ru
реклама

Удобно или безопасно?

О недостатках парольной защиты написано много статей. Но проблема в том, что ничего не меняется. Основной недостаток паролей – сами пользователи, которые их создают, забывают, теряют.

Сегодня рекомендуемая длина паролей не менее 12 символов. Но кто этого придерживается? Люди используют один и тот же пароль на разных сервисах, а кто может гарантировать, что безопасность всех сервисов одинакова и при взломе самого слабого из них автоматически не будут взломаны все остальные.

Что делать?

На самом деле уже на сегодня существует несколько вариантов:

1. Парольная защита.
2. Двухфакторная аутентификация (аппаратный ключ, генератор второго фактора или SMS).
3. Биометрическая защита (отпечаток пальца, радужка глаза).

Но недавно компания Microsoft предложила отказаться от паролей, используя приложение Microsoft Authenticator.

Более того, по данным Microsoft, отсутствие пароля – это новое поколение защиты учётной записи. Просто, быстро, безопасно. Давайте посмотрим, насколько это просто, быстро (тут я согласен). С вопросом безопасности не всё так однозначно.

Будет ли моя учётная запись в безопасности?

При беспарольном входе, скорее, да, чем нет. Особенно если ваш пароль будет типа 12345678. Ведь вы используете альтернативные методы входа, такие как приложение Microsoft Authenticator, физические ключи безопасности и биометрию.

Но, с другой стороны, биометрия, как неоднократно заявляли сотрудники Microsoft, это скорее, удобство, чем безопасность. Сегодня биометрические датчики на ноутбуках, а тем более смартфонах, не умеют отличать живое от неживого. Эта задача не решена до сих пор. Создать перчатки с отпечатками пальцев не представляет ничего сложного. Более того, такие перчатки при наличии снимков отпечатков пальцев в высоком разрешении можно сделать менее чем за 20 долларов.

Итак, вы хотите использовать беспарольный вход. Значит ли это, что пароль вам больше не нужен? Нет конечно!

Для начала вам необходимо установить приложение Microsoft Authenticator (www.microsoft.com/authenticator). Кроме того, настоятельно рекомендую, чтобы на всех ваших устройствах были последние обновления программного обеспечения.

Либо войдите в свою учётную запись Microsoft и выберите «Учётная запись Microsoft» – «Безопасность» (рис. 1).

Вы можете скачать приложение Microsoft Authenticator с Google Play или Apple Store для Android или iPhone, соответственно.

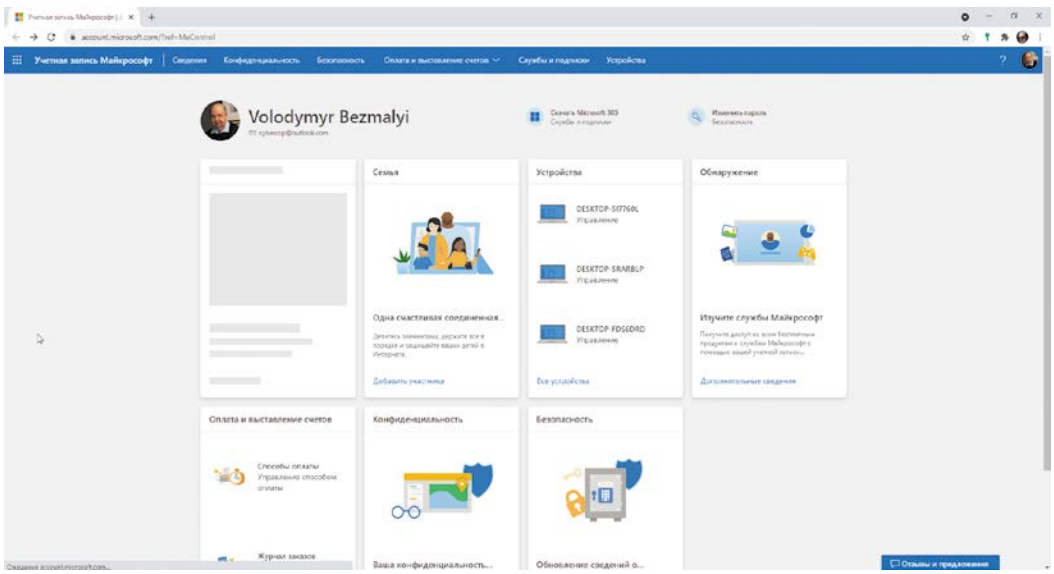
Настройка приложения Microsoft Authenticator достаточно детально описана в литературе и не вызывает особых вопросов, поэтому в данной статье рассматриваться подробно не будет.

Если же вы уже установили приложение Microsoft Authenticator, то выполните следующее:

- Войдите в свою **учётную запись Microsoft. Дополнительные параметры безопасности.**

Владимир Безмалый
Microsoft Security Trusted Advisor
Microsoft MVP
Kaspersky Certified Trainer
Консультант ООН по информационной безопасности

Рисунок 1. Учётная запись Microsoft



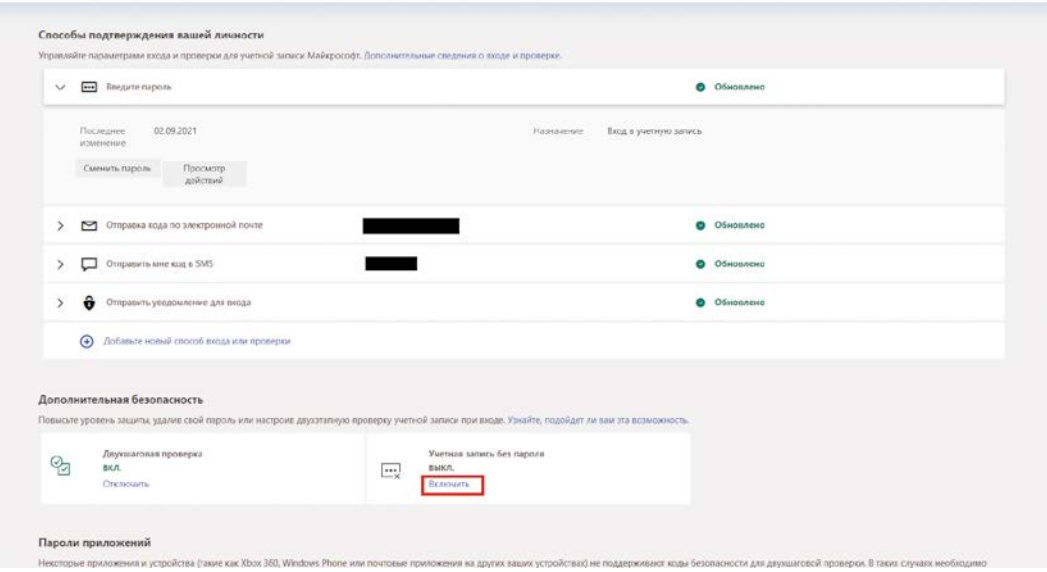


Рисунок 2. Вписать название

- В разделе «Учётная запись» без пароля выберите **Включить.**
- Следуйте инструкциям, чтобы подтвердить свою учётную запись.
- Утвердите запрос, отправленный в ваше приложение Microsoft Authenticator (рис. 2).

Переход без пароля означает удаление вашего пароля и использование метода без пароля для входа в систему.

Итак, с одной стороны, использование беспарольного входа – это удобно. Но давайте разберёмся, насколько это безопасно. Ведь фактически ваша безопасность в этом случае сводится к защищённости вашего смартфона и использованию биометрии, чаще всего отпечатка пальца, а при отсутствии данного датчика или каких-то проблем с вашими пальцами (травма, грязь, мокрые руки) потребуется ввод PIN-кода. А это, в свою очередь, зависит от длины и строгости вашего PIN-кода.

Что мы имеем в данном случае? У большинства пользователей PIN-код – это четыре цифры, в лучшем случае – шесть. Безусловно, в некоторых моделях это может быть буквенно-цифровая последовательность. Но ведь таких угрожающе мало. Сам знаю, что это неудобно, и уже после одного дня использования сложного PIN пользователь просто взвоет и отменит его. Что делать? На мой взгляд, – использовать Microsoft Authenticator как второй фактор.

Что следует отсюда? То, что, фактически, Microsoft предлагает ту же двухфакторную аутентификацию, но уже основанную не на пароль + код, а на биометрия + смартфон (приложение) или PIN-код + приложение.

Вместе с тем необходимо помнить, что в ряде случаев вам нужно использовать пароли. Например, использование почтовых приложений, таких как Microsoft Outlook 2010 и другие, в которых используется пароль приложения, создаваемый на основе вашего пароля.

Кроме того, нужно помнить, что ваш смартфон можно сломать, потерять, уронить, в конце концов. А также его просто могут у вас украсть. Как быть в таком случае?

Если вы потеряете доступ к приложению Microsoft Authenticator, вы всё равно сможете **получить доступ к своей учётной записи Microsoft,** используя альтернативный метод восстановления, например текстовое сообщение или резервный адрес электронной почты. Если у вас **включена двухэтапная проверка,** вам потребуется доступ к двум методам восстановления.

Если же вы снова захотите использовать пароль, просто выключите «Учётная запись без пароля».

Если у моей учётной записи нет пароля, как я могу войти?

Способов войти в учётную запись достаточно много. Вы сможете войти в систему используя, например, приложение Microsoft Authenticator, Windows Hello, ключи физической безопасности, коды SMS. Однако использовать коды SMS не рекомендуется, ведь сегодня их можно просто перехватить.

Варианты входа с помощью многофакторной идентификации

Фактически варианты входа отличаются только элементом, который вы выбираете в качестве второго фактора. Это может быть:

1. Телефонный звонок.
2. Текстовое сообщение (SMS).
3. Приложение аутентификации.

4. Другой метод, так как невозможно прямо сейчас использовать основной вариант.

Стоит учесть, что приложение Microsoft Authenticator необходимо использовать как для двухфакторной аутентификации в качестве генератора кодов второго фактора. Поэтому в любом случае вам потребуется установить приложение на смартфон.

Как войти в Windows без пароля

Microsoft недавно добавила возможность входа без пароля в учётные записи Microsoft для пользователей Windows на потребительском уровне, включая всех, кто использует Windows 10 Home Edition, а вскоре и Windows 11 Home Edition. До этого изменения вход без пароля был эксклюзивным для пользователей Windows корпоративного уровня, но теперь все пользователи смогут сделать это в настройках своей учётной записи Microsoft.

Включив эту опцию, пользователи могут использовать свою учётную запись Microsoft без пароля. Вместо этого вы войдёте в свою учётную запись, а также в некоторые приложения, службы и функции Windows, которые этого требуют, используя альтернативный метод аутентификации, такой как приложение Microsoft Authenticator, Windows Hello или коды подтверждения по тексту/электронной почте. Поддерживаемые продукты включают:

- Ваш ПК с Windows 10 или 11
- Ваш Xbox Series X/S или Xbox One
- Приложения Microsoft Office 365
- Microsoft Outlook
- Магазин Microsoft
- Веб-сайт учётной записи Microsoft
- И более.

Так зачем вам это делать? Кроме удобства, это безопаснее. Удаление пароля вашей учётной записи для повышения её безопасности может показаться нелогичным, но, как указывает сама Microsoft, пароли – ненадёжный метод безопасности. Фактически же вы используете не беспарольный вход, а двухфакторную аутентификацию.

Компании и приложения часто хранят данные паролей ненадлежащим образом, что приводит к их утечкам или утечкам данных. Но даже если пароли надёжно сохраняются на стороне сервера, есть много способов, которыми хакер может подобрать пароли для взлома чьей-либо учётной записи, например ввод учётных данных или распыление паролей. Любой человек уязвим для этих атак, даже те из нас, кто использует уникальные пароли, защищённые с помощью зашифрованных менеджеров паролей.

Конечно, идеального метода аутентификации нет. Общие альтернативы, такие как биометрия (сканирование отпечатков пальцев, разблокировка лица и т.д.) и текстовая проверка, имеют свои собственные уязвимости, особенно если вы используете их в качестве единственного метода входа. Тем не менее эти методы проверки более безопасны, чем пароли, особенно если вы используете многофакторный вход.

Как включить вход без пароля для ваших учётных записей Microsoft

- Войдите на страницу учётной записи Microsoft.
- Зайдите в Настройки> Безопасность.
- Выберите «Дополнительные параметры безопасности».
- При появлении запроса введите свой пароль.
- Перейдите на страницу «Дополнительная безопасность», затем прокрутите вниз до «Дополнительная безопасность». Нажмите «Включить» под опцией «Учётная запись без пароля». Для этого потребуется установить приложение Microsoft Authenticator на смартфон.
- Следуйте инструкциям на экране вашего ПК и мобильного устройства, чтобы завершить настройку.

Мы также рекомендуем включить **«Двухэтапную проверку»** в меню **«Дополнительная безопасность»** после включения входа без пароля, если вы ещё этого не сделали.

Теперь войти в свою учётную запись Microsoft без пароля. Обратите внимание, что для некоторых старых продуктов Microsoft и функций Windows по-прежнему требуется пароль, например:

- Почтовые службы IMAP и POP
- Office 2010 или более ранняя версия
- Office для Mac 2011 или более ранней версии
- Удалённого рабочего стола
- Диспетчер учётных данных Windows
- Windows 10 версии 1809 или более ранней, включая все версии Windows 8.1 и Windows 7
- Xbox 360 и оригинальные консоли Xbox.

Однако Microsoft, похоже, привержена экосистеме без паролей, поэтому будущие сторонние продукты должны поддерживать эту функцию.

Итак, что получается? Пароль – неудобно. Без пароля – страшно, особенно если PIN на телефоне «1111» или «0000».

Заключение

Помните, что наиболее устойчивую защиту обеспечит двухфакторная аутентификация. Увы, любой иной способ аутентификации – это просто удобство. Но удобство и безопасность в данном случае идут врозь.

Владимир Безмалый

Microsoft Security Trusted Advisor
Microsoft MVP
Kaspersky Certified Trainer
Консультант ООН по информационной безопасности

Елена Нагорная
начальник отдела
информационной безопасности
АО «Техснабэкспорт»

«3 кита» информационной безопасности объектов с государственным участием

Современные реалии таковы, что в век информатизации и цифровизации, всё больше объектов предприятий как крупных, так и мелких, подвергаются компьютерным атакам с целью получения выгоды злоумышленниками.

Это могут быть и мошенники, и специальные службы иностранных государств, и компании-конкуренты. Многие руководители компаний озабочены, чтобы в условиях минимальных затрат можно было построить эффективную систему защиты ИТ-инфраструктуры с учётом выполнения требований регуляторов, а если это касается компаний с государственным участием, то следует учитывать, что система защиты должна быть ещё и импортонезависимой.

И нередко специалисты, обеспечивающие информационную безопасность, задаются вопросом, как построить эффективную систему безопасности с минимальными затратами.

По моему мнению, любая система информационной безопасности предприятия в компаниях с государственным участием должна строиться по принципу «3-х китов»:

1. Соответствие требованиям регуляторов.
2. Эшелонированная защита информации.
3. Визуализация событий информационной безопасности и автоматическая регистрация инцидентов информационной безопасности.

Соответствие требованиям регуляторов

Несомненно, стоит отметить, что на компании с государственным участием в той или иной мере распространяется действие Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и подзаконных актов, изданных в целях его исполнения. Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях её устойчивого функционирования при проведении в отношении неё компьютерных атак.

На тему выполнения требований как организационных, так и технических, издано много публикаций, поэтому подробно разбирать требования в данной статье не буду.

Немного остановлюсь на изменениях в законодательстве за нарушения при защите критической ИТ-инфраструктуры. Административная ответственность будет грозить должностным и юридическим лицам за нарушения требований по обеспечению безопасности критической информационной инфраструктуры РФ и несвоевременное предоставление сведений органам, отвечающим за ликвидацию компьютерных атак (рис. 1).

Эшелонированная защита информации

Что же такое эшелонированная система защиты информации? В соответствии с ГОСТ Р 56205–2014 IEC/TS 62443-1-1:2009 «СЕТИ КОММУНИКАЦИОННЫЕ ПРОМЫШЛЕННЫЕ. Защищённость (кибербезопасность) сети и систем» под **эшелонированной защитой** понимается наличие множественной защиты, в частности в виде уровней, с целью предотвращения или хотя бы сдерживания атаки.

Эшелонированная защита предполагает наличие уровней защиты и обнаружения угроз даже на обособленных системах и обладает следующими признаками:

- злоумышленники сталкиваются с проблемой незаметного прохождения или обхождения каждого уровня;
- дефект на одном уровне может быть ослаблен возможностями других уровней;
- безопасность системы сводится к набору уровней, которые определяют также общую безопасность сети.

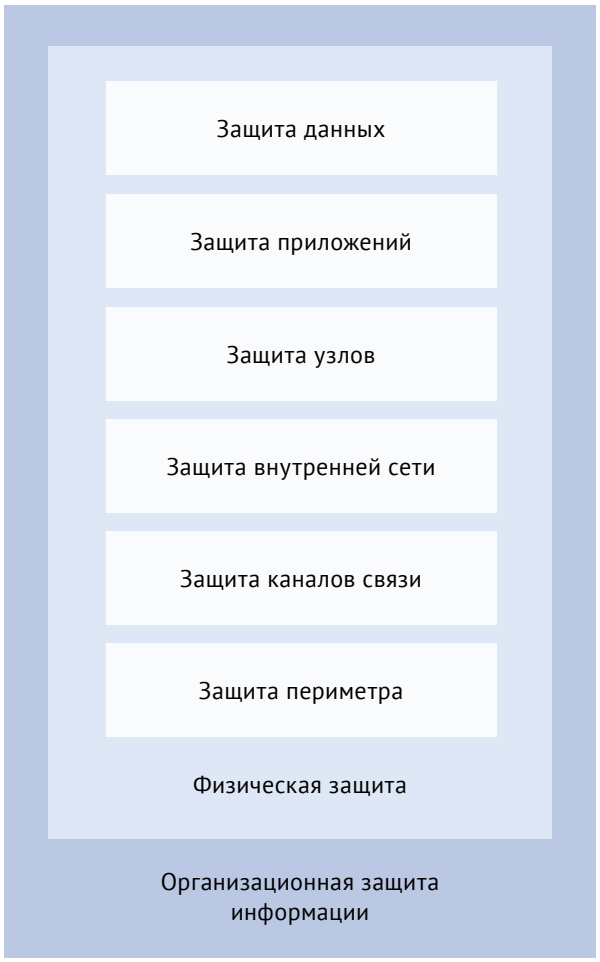
Эшелонированная защита определяет набор уровней защиты автоматизированной системы с учётом требований информационной безопасности. Правильная организация защиты на каждом из уровней позволяет уберечь автоматизированную систему от реализации угроз информационной безопасности.

На примере АО «Техснабэкспорт» покажем с практической точки зрения, как эффективно реализовать эшелонированную защиту автоматизированной системы (рис. 2).

Рис. 1. КоАП РФ Статья 13.12.1. Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

1. Нарушение требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования либо требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, если такие действия (бездействие) не содержат признаков уголовно наказуемого деяния.	Наложение административного штрафа на должностных лиц в размере от десяти тысяч до пятидесяти тысяч рублей; на юридических лиц – от пятидесяти тысяч до ста тысяч рублей.
2. Нарушение порядка информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации, установленного федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации.	Наложение административного штрафа на должностных лиц в размере от десяти тысяч до пятидесяти тысяч рублей; на юридических лиц – от ста тысяч до пятисот тысяч рублей.
3. Нарушение порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств , международными, международными неправительственными и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты.	Наложение административного штрафа на должностных лиц в размере от двадцати тысяч до пятидесяти тысяч рублей; на юридических лиц – от ста тысяч до пятисот тысяч рублей.

Рис. 2.



Уровень «Организационная защита информации» можно определить как базовый. Он включает в себя принятые политики информационной безопасности в организации, описывает процедуры обеспечения информационной безопасности и направлен на повышение осведомлённости работников организации по вопросам информационной безопасности.

Уровень «Физическая защита» включает меры по ограничению физического доступа к ресурсам системы: защита помещений, контроль доступа, видеонаблюдение и т.д.

Уровень «Защита периметра» определяет технические меры обеспечения информационной безопасности на внешнем периметре сети. В АО «Техснабэкспорт» в качестве периметровых средств защиты информации используются средства межсетевого экранирования, средства обнаружения и предотвращения вторжений, средства антивирусной защиты. Следует отметить, что все используемые средства защиты в нашей компании имеют сертификаты соответствия ФСТЭК по требованиям безопасности информации и в основном являются импортозамещёнными.

Уровень «Защита каналов связи» определяет криптографическую защиту каналов связи с использованием шифрования по ГОСТ. Данная мера на примере АО «Техснабэкспорт» обусловлена тем, что работники как российского, так и зарубежных офисов, используют защищённое

Рис. 3.

удалённое рабочее место. Вся обработка самой информации осуществляется в периметре автоматизированной системы и полностью исключает обработку на оконечных устройствах.

Уровень «Защита внутренней сети» обеспечивает безопасность передаваемого внутри сети трафика и сетевой инфраструктуры. Основными мерами, обеспечивающими данный уровень защиты, в АО «Техснабэкспорт» являются: построение ИТ-инфраструктуры на базе средств виртуализации, использование антивирусных средств защиты для среды виртуализации, микросегментация сети в частности, применяется изоляция (отсутствие взаимодействия между несвязанными сетями), сегментация (управляемое взаимодействие внутри сети) и безопасность с расширенными службами (тесная интеграция с реализованными решениями по обеспечению безопасности.

Уровень «Защита узлов» предполагает настройки, повышающие безопасность конфигурации (в том числе, отключение не использующихся или потенциально опасных служб), организация установки исправлений и обновлений, надёжной аутентификации пользователей, проведение регулярных сканирований сети с использований средств анализа защищённости, а также использование средств антивирусной защиты.

Уровень «Защита приложений» отвечает за защиту от целенаправленных атак, направленных на конкретные приложения – почтовые серверы, web- серверы, серверы баз данных. В рамках данного уровня защиты мы сейчас реализовываем внедрение системы защиты от целенаправленных атак, с интеграцией средств антивирусной защиты, защиты трафика, антиспам-системы.

Уровень «Защита данных» определяет порядок защиты обрабатывающихся и хранящихся в системе данных от несанкционированного доступа и других угроз. Данный уровень реализован разграничением прав доступа, применением сертифицированного средства аутентификации.

Визуализация событий информационной безопасности и автоматическая регистрация инцидентов информационной безопасности

Систему мониторинга событий информационной безопасности я целенаправленно выделила в отдельное направление, так как правильно настроенная система может заменить целый штат работников и оперативно, в режиме реального времени показывать руководителю, какие критичные угрозы в автоматизированной системе существуют именно сейчас.

Для информативной и эффективной работы системы мониторинга событий информационной безопасности необходима корректная, применимая к конкретному предприятию, настройка правил корреляции событий информационной безопасности. События же, в свою очередь, должны поступать от всех источников и узлов ИТ-инфраструктуры.

Выше представлена схема сбора событий информационной безопасности в системе мониторинга событий информационной безопасности (рис. 3).

CIS / № 1 (19) / 2022 / www.cis.ru

Тенденции развития беспилотных авиационных систем в гражданском секторе

В настоящее время в мире, в частности в России, наблюдается настоящий бум во всём, что касается гражданских воздушных беспилотников.

Во многих странах создаются системы регулирования применения беспилотных воздушных судов (далее — БВС), разрабатываются новые технологии в части конструкционных материалов, элементов БВС, программного обеспечения для их использования. При этом звучат громкие заявления о создании в ближайшие годы серийных больших дронов для перевозки грузов, об организации доставки товаров в городах, о создании экспериментальных правовых режимов для использования БВС на урбанизированных территориях и многое другое. Однако следует отметить, что большинство из этих заявлений далеки от реальности. Использование серийных грузовых дронов и разрешение на полёты в урбанизированных территориях ожидается не ранее, чем через 10–15 лет, что обусловлено в настоящее время как огромными рисками в части безопасности, так и несовершенством современных технологий. Кроме того, в большинстве стран наблюдается значительные пробелы в законодательстве для беспилотников, из-за чего у компаний возникают большие сложности даже при попытках сертификации БВС. Например, в России компания «Кронштадт» безуспешно пытается получить сертификат эксплуатанта уже несколько лет, затратив на этот процесс сотни миллионов рублей. Во многих странах объявлено о введении экспериментальных правовых режимов (далее — ЭПР), однако лишь в единицах данные режимы действуют в реальности.

При этом на данный момент беспилотные авиационные системы (далее — БАС) уже применяются во многих отраслях и сегментах рынков гражданского сектора. Но они используются в первую очередь для различных задач мониторинга, как например мониторинг нефтегазовых объектов, линий электропередач, строительства, дорожной ситуации, лесного и сельского хозяйства, геодезии, картографии, видеосъёмки, для проведения авиахимических работ для нужд сельского хозяйства, а также в достаточно специфических направлениях — гонках и шоу дронов. При этом потенциально беспилотники могут использоваться (и уже используются в пилотных проектах) для решения логистических задач, проведения геологических исследований, мониторинга природных и техногенных катастроф, городской среды, экологического мониторинга, услуг связи, авиахимических работ несельскохозяйственного назначения (дезинфекция и дезинсекция, окраска, борьба с экологическими катастрофами, например разливами нефти, и пр.), посевных работ. Среди уникальных примеров применения БАС можно отметить дрон, стреляющий лазерными дротиками-датчиками для организации экологических исследований в труднодоступных местах, что позволяет сформировать на беспроводной основе информационную систему экологической обстановки.

Уже сейчас можно сказать, что БВС выигрывают конкуренцию у традиционных способов в ряде сегментов (в первую очередь при работах по мониторингу и съёмке) как по параметрам экономической эффективности, так и по росту качества работ и сокращению сроков. Постоянное технологическое развитие позволит увеличить конкурентоспособность беспилотников и в других сегментах.

В настоящее время разработки в части развития БВС наблюдается ряд основных тенденций, связанных в первую очередь с использованием цифровых технологий.

Искусственный интеллект

Одной из основных тенденций цифровой трансформации в области услуг с использованием БАС можно обозначить внедрение искусственного интеллекта (далее — ИИ) в управление БВС и полезными нагрузками, а также в обработку (интерпретацию) полученной с БВС информации.

В первую очередь происходит развитие технологий БВС, позволяющих с помощью ИИ (машинного обучения, в том числе самообучающихся систем) без участия человека управлять сразу большим количеством БВС (роем). В настоящее время подтверждена актуальность создания полностью децентрализованных алгоритмов управления роем БВС, позволяющих создавать формации, произвольные по относительным расстояниям между аппаратами, при этом учитывающих нелинейный характер структуры реальных систем автопилотирования.

Анна Никитченко
Управляющий партнёр O2Consulting

Развиваются новые комплексные подходы, которые позволяют автономно управлять БВС в сложных природных и искусственных средах на высоких скоростях, используя исключительно бортовые датчики и автоматические вычисления без участия наземных пилотов[1].

Кроме того, наблюдается тенденция интеграции ИИ с БВС для мониторинга, что позволяет лучше распознавать снимаемые объекты и окружающую среду, точно и своевременно отображать конкретные объекты, отслеживать и контролировать их движение и состояние, а также предоставлять точную аналитическую обратную связь.

Увеличение мощности устройств для БАС

В данном аспекте наблюдаются тенденции увеличения памяти на устройствах для хранения большего количества отснятого материала в лучшем разрешении.

Кроме того, предполагается рост скорости и объёмов обработки информации полезной нагрузкой БАС ещё до начала интерпретации данных на наземной станции.

Обработка и аналитика с помощью ИИ больших данных, полученных

1. www.rpg.ifi.uzh.ch/AgileAutonomy. html

посредством аэрофото- и видеосъёмки, также представляет собой одно из направлений наиболее активных разработок с целью решения двух основных задач: повышения точности получаемого результата и сокращения времени обработки данных.

Расширение функционала ПО для БАС

В части развития функционала программного обеспечения для БАС можно отметить тренд на модернизацию существующей инфраструктуры БАС путём интеграции новых датчиков и устройств, а также расширенных цифровых решений с целью выполнения за один полёт максимального количества поставленных задач.

Подключение БАС к сетям 4G и 5G

В последнее время разрабатываются технологии, которые помогут передавать информацию не по радиоканалам БАС, а по сетям 4G и 5G, что позволит БВС не зависеть от дальности связи по радиоканалу, а также ускорить передачу информации (там, где сеть в наличии).

Автономность БАС в пространстве

Следует отметить тренд на автономность дронов, которые за счёт цифровой системы будут способны самостоятельно ориентироваться в пространстве, то есть без использования систем спутниковой навигации.

Создание автономных дронопортов

Ведутся и реализуются разработки автономных роботизированных систем, которые автоматически меняют батареи БВС с помощью роботов-манипуляторов, что позволяет дрону летать 24/7 без ожидания подзарядки и потери времени.

БАС в роли станций связи

В настоящее время наблюдается тенденция развития технологий предоставления телеком-услуг на базе дронов. В данном сегменте создаются миниатюрные мобильные базовые станции стандарта LTE (5G) в виде БАС, которые позволят обеспечивать сотовую связь и интернет в местах, где доступ к ним ограничен или сигнал сети низкого качества, а также в отдалённых районах и на специальных мероприятиях.

Цифровые экосистемы

Отраслевые цифровые экосистемы с использованием БАС

На данный момент уже разработаны или развиваются отраслевые ERP-системы и цифровые экосистемы, работающие с использованием БАС.

Среди них, например, можно отметить проекты в сфере точного земледелия для сельского хозяйства: российскую разработку «История поля» от компании «Геомир» и зарубежную Cropwise Operations от компании Syngenta Group. Деятельность данных систем подразумевает следующий функционал: планирование и контроль выполнения технологических операций на полях, мониторинг сельхозтехники, получение метеоданных, электронный журнал агронома, электронные учётные листы, справочники сорняков, болезней и вредителей, анализ снимков, контроль топлива и урожая, планфакт анализ выполненных операций, кадастровый учёт, модуль точного земледелия, осмотры полей.

В настоящее время в таких системах используются БАС только для целей мониторинга, но функционал систем будет усложняться и расширяться, и ожидается, что в перспективе в него войдут модули использования БАС для авиахимических работ под управлением ИИ.

Создание подобных цифровых экосистем ожидается в лесотаксации, управлении строительством и прочих направлениях.

Также в некоторых странах, например в России, БАС планируется встроить в национальную систему пространственных данных.

Цифровые экосистемы организации воздушного движения с учётом БАС

Кроме того, следует упомянуть тенденцию создания и развития цифровых экосистем с целью организации воздушного движения (далее — ОРВД) с учётом БАС.

Одна из основных сфер исследований в данном аспекте — обеспечение технической безопасности дронов — технологий, позволяющих обнаруживать и избегать столкновения с различными препятствиями, а также их интеграция в существующие авиадиспетчерские системы. Предлагаемые в этой области решения должны также учитывать нормативно-правовую базу, регулирующую производство и эксплуатацию беспилотных летательных аппаратов в каждой конкретной стране.

Кроме того, в рамках необходимого функционала цифровой экосистемы ОРВД с учётом БАС следует отметить:

- технологические решения по предотвращению ущерба, причиняемого людям и имуществу при потере управления беспилотными воздушными судами;
- система мониторинга инфраструктуры связи и систем наблюдения, предоставляющих информацию об их состоянии;
- требования к кибербезопасности (для предотвращения незаконного вмешательства в деятельность беспилотных авиационных систем);
- организация наблюдения за БВС в несегрегированном воздушном пространстве;
- «цифровой двойник» воздушного пространства (трёхмерная модель с указанием зон, запрещённых для полёта);
- системы авиационного наблюдения;
- технологии защищённого хранения на борту БВС и передачи на НПУ данных аэрофотосъёмки для рассекречивания.

Антидрон

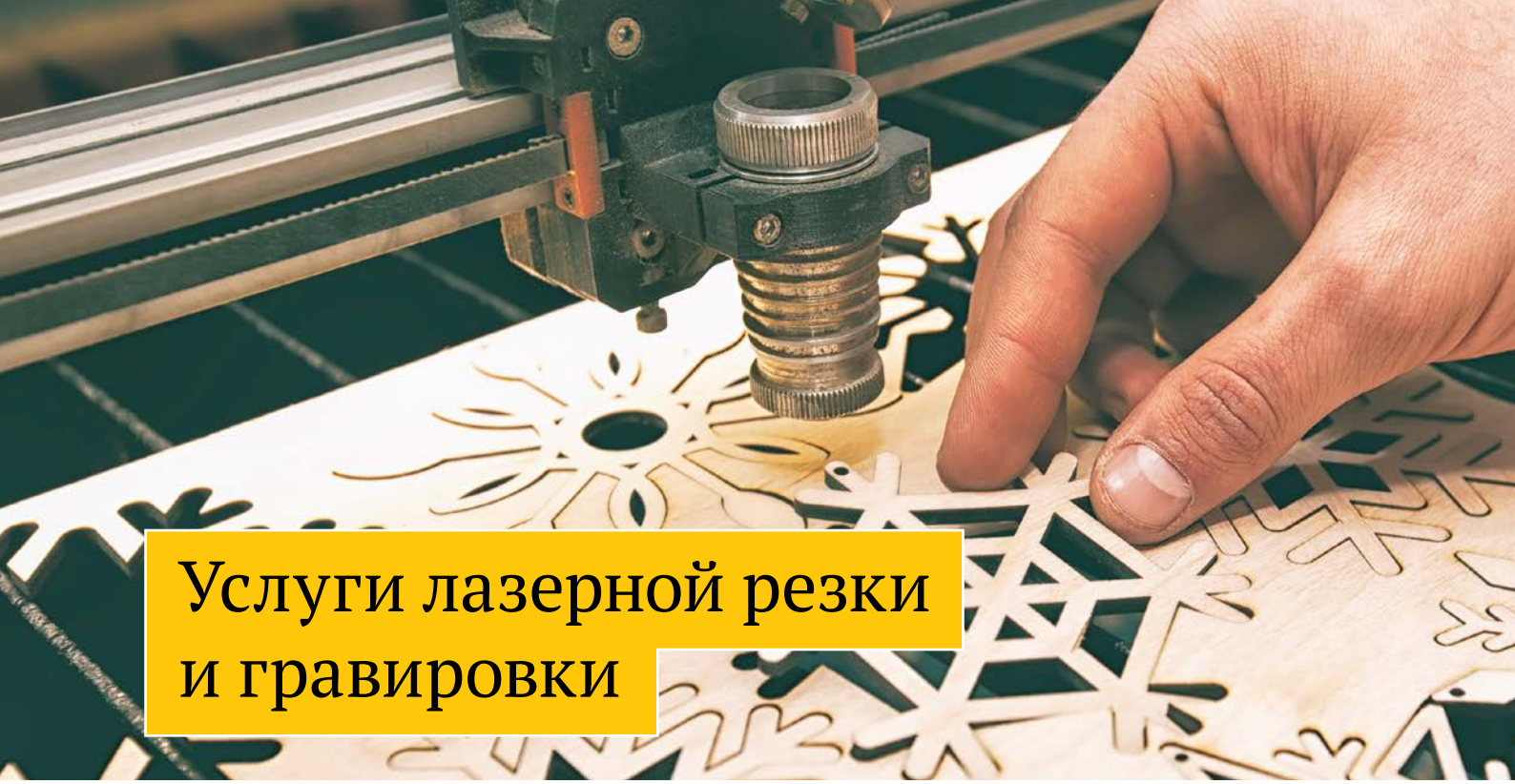
Следует отметить, что активно развиваются цифровые системы, направленные на предотвращение ущерба и защиту людей и объектов от БАС, так называемые «Антидрон». В данные системы входит функционал распознавания дронов, нейтрализация дронов или перехват управления, определение местонахождения оператора дрона.

O2CONSULTING

Анна Никитченко
Управляющий партнёр O2Consulting

Тел.: +7 926 810 60 23

anna@o2consulting.ru



Услуги лазерной резки и гравировки

Лазерная резка – современная и инновационная технология контурной резки всевозможных листовых материалов.

Эта передовая технология стала ведущим методом раскроя акрила, который осуществляется с помощью лазерного луча. Процесс резки производится с ювелирной точностью, оставляя при этом незначительное количество отходов. Метод лучевой резки даёт возможность эффективно, быстро и качественно выполнять сложные задачи по обработке акрила. Благодаря уникальности технологии лазерной резки оргстекла изделия получаются с идеально ровными гранями, которые не нуждаются в дополнительной обработке среза и их шлифовке. Данный способ позволяет получить максимальную продуктивность производственного процесса и точность исполнения задачи.

Применение лазерной технологии

Благодаря высокоточным лазерным станкам стало возможным быстро создавать изделия не только любой сложности, но и в любом количестве.

Наша компания профессионально занимается лазерной резкой любой сложности в Москве. У нас имеется новейшее автоматизированное оборудование. Наши станки позволяют очень быстро (до 400 мм/с), точно (0,1 мм) и аккуратно выполнить художественный раскрой. Мы делаем резку как единичных изделий, так и крупными партиями.

Заказав услугу лазерной резки, вы гарантировано получите именно тот результат, который ожидаете увидеть.

WhatsApp: +7-926-171-67-82
info@sovinfosystems.ru

1 Современное высокоточное оборудование

2 Круглосуточный приём заказов

3 Индивидуальный подход

4 Профессионализм мастеров

5 100% гарантия качества

CIS / № 1 (19) / 2022 / www.cis.ru

Мечтам свойственно сбываться

Дарья Ягода
Корреспондент ИТ-журнала CIS «Современные Информационные Системы»

Когда ты чего-то очень хочешь и что-то для этого делаешь, возможности сами появляются на твоём пути. Так произошло и со мной...

Я всегда мечтала стать телеведущей. Однако родители зачастую хотят от нас серьёзности, чтобы не стыдно было рассказать друзьям про свою дочь и её образование. Я на время поместила зёрнышки своей мечты в мешочек и запрятала подальше в сердце. Так я стала студенткой по специальности «Менеджмент».

Но моя душа всегда тянулась к творчеству и самовыражению. Очень хотелось «глаголом жечь сердца людей». И вот настало время достать свой мешочек и подготовить почву для посева. Я делала всё, что хоть немного приблизит меня к цели в нынешних условиях. Если хочешь съесть слона, каждый день ешь по бутерброду от этого слона, а аппетит у меня всегда был прекрасный. Итак, я начала с КВНа, буквально «приросла» к сцене. В институте я бралась абсолютно за всё: от ведения крупных концертов до интеллектуальных игр и литературных вечеров. Устроилась работать ведущей в караоке, чтобы хоть как-то развивать навыки, которые нужны для профессии моей мечты.

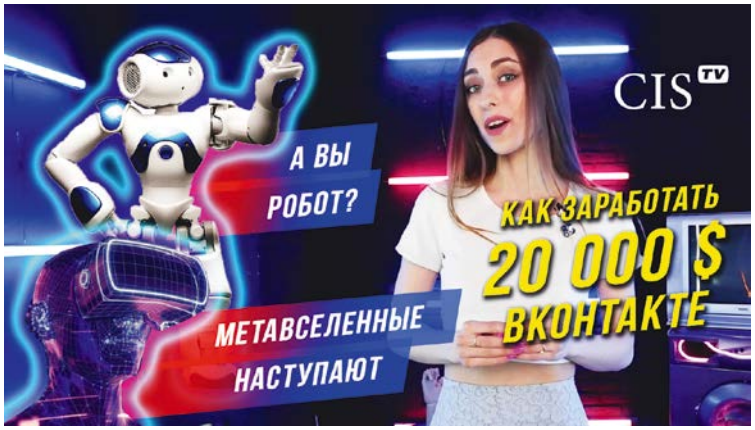
И вот красный диплом у меня в руках. Добби свободен! Теперь пора исполнять свою мечту. Я поехала учиться в самую престижную в нашей стране Высшую школу кино и телевидения Останкино на теле- и радиожурналистику. Моими учителями стали ведущая программы «Вести» на телеканале «Россия» Мария Ситтель, телеведущий шоу «Прямой эфир» Михаил Зеленский, ведущая и продюсер программы «Ревизорро» Елена Летучая и многие другие мастера своего дела из мира российского телевидения. Я снимала свои первые репортажи, сюжеты и интервью. Далее череда неудачных кастингов, которые укрепили мой иммунитет к страхам и сомнениям.

В какой-то момент я отчаялась, потому что не получалось устроиться на местное телевидение или радио. Парней там всегда ждут, но для девушек свободного места не находится. Я мысленно готовилась идти на нелюбимую работу и прожигать свою жизнь впустую.

Однажды я со скучающим видом листала почту и увидела письмо с пометкой «Телеведущая ИТ-новостей». В нём меня приглашали на работу корреспондентом в ИТ-журнал CIS. Я подумала, что это какой-то спам, и не поверила. Ведь я не отправляла туда своё резюме. Да и в голове не укладывалось, что меня нашли и так просто приглашают в новый необыкновенный проект. Но всё это оказалось правдой, и я уже четыре месяца как ведущая ИТ-новостей на ютуб-канале CIS-TV. Понимаю, что я только в начале пути и мне предстоит очень многому научиться. Но это ещё больше мотивирует меня развиваться и совершенствоваться. А мои близкие приняли мои мечты и поддерживают во всех начинаниях.

О проекте CIS-TV

Когда мне предложили эту работу, из темы ИТ я знала только буквы «И» и «Т». Но мне было так интересно, словно слепому котёнку, «прощупывать» дорогу в сферу цифровых инноваций. Я открыла для себя огромный мир



волшебства и технологий, о которых раньше и не догадывалась.

С чистого листа я познавала не только область информационных технологий, но и платформу YouTube. Наша редакция создала новый канал для ИТ-новостей, которому предстояло с нуля завоёвывать аудиторию, а это очень непросто. Ведь мы хотим делать контент не только для ИТ-специалистов, но и для людей, далёких от цифровых инноваций.

Наша цель – коротко, доступно и полезно рассказывать о сложных вещах, чтобы как можно больше людей открыли для себя мир информационных технологий. В XXI веке время – самый ценный ресурс. Чтобы помочь самой разной аудитории ориентироваться в бесконечном потоке информации, мы делаем выжимку из наиболее важных и интересных ИТ-новостей. Ведь мы ценим время каждого зрителя.

Подготовка к съёмкам равносильна свадебным хлопотам. Нужно продумать каждую мелочь: антураж студии, свет, звук, ракурсы, образ и макияж ведущего. Подвести может что угодно. Лицо не должно блестеть. Микрофон – удобно крепиться на одежду и не оттягивать её. Одежда – только однотонная, сочетаться с цветом фона и быть из определённого материала. И это лишь малая часть правил, от которых кругом идёт голова. Но это приятные заботы, которые приносят удовольствие.

До съёмки я подбираю инфоповоды, которые затем одобряет главный редактор Станислав Понарин. Далее пишу сценарий, который также проверяет главный редактор. Я обожаю вставлять шутки, яркие фразы, личные комментарии, чтобы оживить выпуск и сделать его интересным и уникальным. Да и пятилетний опыт в КВН даёт о себе знать: сформировались особая манера и подача материала через призму юмора. Я постоянно пересматриваю свои выпуски, чтобы подмечать ошибки и исправлять их. Самокритика и рефлексия помогают мне становиться лучше.

Я веду еженедельный дайджест ИТ-новостей, а в конце месяца директор по маркетингу Валерия Рябинина подводит итоги. Не хочется ограничиваться только новостями. Сейчас мы работаем над новой рубрикой. Стараемся создавать разнообразный и интересный контент. В ближайшем будущем планируем снимать больше роликов и делать их максимально полезными и познавательными. Однако и о развлекательном формате мы не забываем. Иногда хочется отдохнуть от сложной информации и просто от души посмеяться.

На международном фестивале команд КВН в городе Сочи мы проверяли, смогут ли весёлые и находчивые найти ответы на наши вопросы об ИТ-технологиях. Что у нас получилось, можно увидеть на нашем канале. В конце выпусков мы проводим конкурсы и дарим подарки нашим самым активным участникам. Так что не упускайте возможность получить приз от нашей редакции.

Мы открыты для новых идей и предложений и с радостью делимся успехами наших коллег. Если у вас есть что рассказать об информационных технологиях, пишите на нашу почту magazine@sovinfosystems.ru. Мы осветим ваши новости в выпуске.

CIS Современные Информационные Системы

Дарья Ягода
Корреспондент ИТ-журнала CIS «Современные Информационные Системы»

www.cis.ru

CIS TV

ИТ-НОВОСТИ

Новостной ИТ-канал
о цифровых и информационных
технологиях в России

YouTube

CIS – Современные Инфосистемы
www.cis.ru

CIS / № 1 (19) / 2022 / www.cis.ru

Этические проблемы, связанные с применением систем технологий и искусственного интеллекта в России и Мире

Александр Юрьевич Чесалов
д.т.н.

Что такое этика искусственного интеллекта?

Что такое этические проблемы, связанные с применением технологий и использованием систем искусственного интеллекта?

На эти и многие другие вопросы, интересующие читателя, я постараюсь ответить через призму анализа содержания двух действительно уникальных документов: Рекомендации Организации Объединённых Наций по вопросам образования, науки и культуры (ЮНЕСКО) по этике искусственного интеллекта и Кодекс этики в сфере искусственного интеллекта Российской Федерации.

***

24 ноября 2021 года Генеральная конференция Организации Объединённых Наций по вопросам образования, науки и культуры (ЮНЕСКО) в ходе своей 41-й сессии, проходившей в Париже с 9 по 24 ноября 2021 года, приняла очень важный документ: «Рекомендация по этике искусственного интеллекта», который, в том числе, определяет основные принципы и подходы к решению этических проблем применения систем ИИ во всём мире[1].

Разработка данного документа была инициирована ещё в ноябре 2019 года на 40-й сессии Генеральной конференции ЮНЕСКО (резолюция 40 C/37), которая запустила процесс разработки международного нормативного акта по этическим аспектам искусственного интеллекта в форме рекомендации[2].

В докладе комиссии по социальным и гуманитарным наукам (SHS), который был сделан на этой конференции, отмечается: «Принимая во внимание, что технологии ИИ способны принести человечеству огромную пользу и их преимуществами могут воспользоваться все страны, но при этом поднимают фундаментальные вопросы этического порядка, касающиеся, в частности, предвзятости, которую такие технологии могут порождать и усугублять, что потенциально может вести к дискриминации, неравенству, цифровому разрыву и маргинализации, ставить под угрозу культурное, социальное и биологическое разнообразие и усугублять социальное или экономическое расслоение; необходимость обеспечения прозрачности и понятности работы алгоритмов и данных, на основе которых проводится обучение интеллектуальных систем; и потенциальные последствия их применения, в частности с точки зрения уважения человеческого достоинства, прав человека и основных свобод, гендерного равенства, демократии, участия в социально-экономических, политических и культурных процессах, научной и инженерной практики, защиты прав животных, а также состояния окружающей среды и экосистем», «признавая, что нравственные принципы и ценности могут способствовать выработке и осуществлению мер политики и норм правозащитного характера и выступать в качестве ориентиров с учётом высоких темпов технологического развития», «принимает настоящую Рекомендацию об этических аспектах искусственного интеллекта»[3].

Что подразумевается под этичным применением искусственного интеллекта?

В документе говорится, что это «…систематическое нормативное осмысление этических аспектов ИИ на основе эволюционирующей комплексной, всеобъемлющей и многокультурной системы взаимосвязанных ценностных установок, принципов и процедур, способное ориентировать общества в вопросах ответственного учёта известных и неизвестных последствий применения ИИ-технологий для людей, сообществ, окружающей природной среды и экосистем, а также служить основой для принятия решений, касающихся применения или отказа от применения технологий на основе ИИ».

Какие же вопросы касаются этики применения систем искусственного интеллекта?

В докладе комиссии по социальным и гуманитарным наукам подчёркивается, что «Развитие систем на основе ИИ поднимает этические вопросы нового типа, касающиеся, в частности, их влияния на процессы принятия решений, проблему занятости и рынок труда, взаимодействие между людьми в обществе, медицину, образование, средства информации, доступ к информации, цифровое неравенство, защиту персональных данных и потребителей, окружающую среду, демократию, верховенство закона, обеспечение безопасности и правопорядка, двойное использование, а также права человека и основные свободы, включая свободу выражения мнений, неприкосновенность частной жизни и отсутствие дискриминации».

Каким образом будет осуществляться мониторинг и оценка реализации Рекомендаций по этике искусственного интеллекта?

Согласно указанному документу всем государствам рекомендуется разработать соответствующую нормативную базу и выполнять

1. Рекомендация по этике искусственного интеллекта. [Электронный ресурс] // en.unesco.org. URL: www.en.unesco.org/artificial-intelligence/ethics#recommendation (дата обращения: 30.01.2022).
2. Предварительное исследование возможности подготовки нормативного акта по вопросам этики применения искусственного интеллекта. [Электронный ресурс] // unesdoc.unesco.org. URL: www.unesdoc.unesco.org/ark:/48223/pf0000369455_rus (дата обращения: 30.01.2022).
3. Доклад комиссии по социальным и гуманитарным наукам (SHS). [Электронный ресурс] // unesdoc.unesco.org. URL: https://unesdoc.unesco.org/ark:/48223/pf0000379920_rus. page=16 (дата обращения: 29.01.2022).

мониторинг, оценку политик, программ и механизмов, касающихся этических аспектов ИИ. ЮНЕСКО, в свою очередь, готово оказать содействие в подготовке методологии для оценки этического воздействия ИИ-технологий, методологии для оценки готовности к разработке и использованию ИИ-систем, методологии по оценке ожидаемой и фактической результативности и эффективности стратегии этичного применения ИИ, а также оказать содействие в подготовке в совершенствовании научного и фактологического анализа и отчётности в отношении правил и стандартов, сбор и распространение отчётов о достигнутых результатах, инновациях и научно-исследовательской работе, в том числе научных публикаций, данных и статистики, касающихся реализации стратегий этически корректного применения ИИ.

Важно отметить, что *целью Рекомендации является формирование основы, которая позволит использовать ИИ на благо всего человечества, отдельного человека, обществ, окружающей среды и экосистем и не допустить причинения им вреда. Её цель также состоит в том, чтобы стимулировать использование систем на основе ИИ в мирных целях.*

В Рекомендации заложены следующие ценностные установки:

1. Уважение, защита и поощрение прав человека и основных свобод и человеческого достоинства.
2. Благополучие окружающей среды и экосистем.
3. Обеспечение разнообразия и инклюзивности.
4. Жизнь в мирных, справедливых и взаимосвязанных обществах.

Чтобы избежать основных этических проблем (таких как ответственность, предубеждённость или предвзятость, прозрачность, приватность или конфиденциальность, надёжность, манипуляция поведением и многие другие), связанных с применением систем ИИ, необходимо учитывать, закладывать и реализовывать во всех создаваемых системах ИИ на всём протяжении их жизненного цикла следующие этические принципы:

1. Соразмерность и непричинение вреда.

- Метод реализации ИИ должен быть подходящим и пропорциональным для достижения законной цели, не противоречить базовым ценностным установкам (его использование не должно привести к нарушению прав человека или злоупотреблению ими), подходить для конкретных условий и основываться на подтверждённых результатах научных исследований.

2. Безопасность и защищённость.

- Оценка рисков и меры по исключению вероятности причинения вреда. Следует избегать непреднамеренного причинения вреда (риски безопасности), а также уязвимости перед кибератаками (риски защищённости), учитывать, предотвращать и ликвидировать эти риски.

3. Справедливость и отказ от дискриминации.

- Инклюзивный подход к обеспечению распространения и всеобщего доступа к полученным благодаря ИИ благам с учётом специфических потребностей разных возрастных групп, культурных систем, языковых сообществ, инвалидов, женщин и девочек, малообеспеченных, социально незащищённых и уязвимых категорий населения либо лиц, находящихся в незащищённом положении.
- Соблюдение принципов многоязычия и культурного разнообразия.
- Преодолением различных видов разрыва в цифровых технологиях (цифровое рабство, цифровое неравенство, цифровой феодализм и т.д.).
- Обеспечение равенства всех граждан вне зависимости от расовой принадлежности, цвета кожи, происхождения, гендерной принадлежности, возраста, языка, религии, политических или иных убеждений, национального, этнического, социального происхождения, экономических или социальных условий рождения, инвалидности и любых иных факторов.
- Обеспечение инклюзивного доступа к разработке ИИ.
- Солидарность в обеспечении совместного использования полученных благодаря технологиям ИИ благ.
- Установление справедливого международного порядка в сфере информации, коммуникации, культуры, образования, научных исследований, а также обеспечения социально-экономической и политической стабильности.

4. Устойчивость.

- Применение технологий на основе ИИ должно неизменно проводиться с должным учётом их влияния на устойчивость развития обществ в странах с различным уровнем развития, которое требует решения сложного комплекса задач, охватывающих ряд взаимосвязанных человеческих, социально-культурных, экономических и экологических аспектов.

5. Право на неприкосновенность частной жизни и защита данных.

- При разработке, эксплуатации и развитии систем ИИ должна уважаться, защищаться и поощряться защита человеческого достоинства, личной независимости и способности человека выступать субъектом действия.
- Сбор, использование, передача, архивирование и удаление данных, применяемых в ИИ-системах, должна осуществляться в соответствии с международным правом и цен-

ностными установками и принципами, изложенными в настоящей Рекомендации, при одновременном соблюдении соответствующих национальных, региональных и международных правовых норм.

- Системы ИИ требуют надлежащей оценки последствий на предмет соблюдения неприкосновенности частной жизни, в том числе социальных и этических аспектов их применения, а также инновационных подходов в отношении неприкосновенности частной жизни на этапе концептуальной проработки.

6. Подконтрольность и подчинённость человеку.

- Термин «подконтрольность» подразумевает не только контроль со стороны отдельного человека, но и в необходимых случаях инклюзивный контроль со стороны общества.

7. Прозрачность и объяснимость.

- Людям следует предоставлять полную информацию о том, какие решения принимаются с использованием алгоритмов ИИ или на основе полученных с их помощью данных, в том числе решения, затрагивающие их безопасность и права.
- Высокий уровень прозрачности обеспечивает возможность контроля со стороны общества, что в свою очередь может способствовать снижению уровня коррупции и дискриминации, а также помочь в выявлении и предотвращении негативных последствий для прав человека.
- Термин «объяснимость» касается обеспечения понятности и представления разъяснений в отношении полученных с помощью ИИ-систем результатов.
- Термины «прозрачность» и «объяснимость» являются неотъемлемыми критериями оценки так называемых систем «доверенного» ИИ.

8. Ответственность и подотчётность.

- Этическая ответственность за решения и меры, принятые с использованием в той или иной форме систем ИИ, во всех случаях должна в конечном счёте возлагаться на субъекты связанной с ИИ деятельности в соответствии с их функциями в рамках жизненного цикла ИИ-систем.
- Техническая и организационная концепция создаваемых ИИ-систем должна обеспечивать возможность проверки, отслеживания и корректировки работы, устранения коллизий и ошибок, связанных с нарушением норм и стандартов прав человека или угрозой здоровью окружающей среды и экосистемы.

9. Осведомлённость и грамотность.

- Для обеспечения реального общественного участия и возможности принятия всеми гражданами обоснованных решений в отношении использования ИИ-систем и защиты от неправомерных последствий их применения необходимо содействовать повышению осведомлённости населения и улучшению понимания им ИИ-технологий.

10. Многостороннее и адаптивное управление и взаимодействие.

- Государства, руководствуясь нормами международного права, определяют порядок обращения с данными, генерируемыми на их территории или передаваемыми через их территорию, и принимают меры по эффективному правовому регулированию их использования, включая защиту данных, на основе уважения права на неприкосновенность частной жизни в соответствии с нормами международного права в области прав человека.

Далее в документе подробно рассматриваются области, требующие принятия стратегических мер, такие как:

1. Оценка этического воздействия.
2. Этичное управление и руководство.
3. Политика в отношении данных.
4. Развитие и международное сотрудничество.
5. Окружающая среда и экосистемы.
6. Гендерное равенство.
7. Культура.
8. Образование и научные исследования.
9. Коммуникация и информация.
10. Экономика и рынок труда.
11. Здоровье и социальное благополучие.

Важным моментом для уважаемого читателя должно стать осознание того, что этические аспекты ИИ, принятые 41-й Генеральной конференцией Организации Объединённых Наций по вопросам образования, науки и культуры, являются очень важными не только для Российской Федерации или какой-то отдельно взятой страны, они крайне важны как для всего мирового сообщества, так и для каждого из нас в отдельности.

В документе говорится о том, что он разработан с учётом Декларации 1986 года Организации Объединённых Наций о праве на развитие, Декларации 1997 года об ответственности нынешних поколений перед будущими поколениями, Всеобщей декларации 2005 года о биоэтике и правах человека, Декларации Организации Объединённых Наций 2007 года о правах коренных народов, Декларации этических принципов в связи с изменением климата 2017 года, а также на основе принятой 26 сентября 2019 года Советом по правам человека резолюции по вопросу о праве на неприкосновенность частной жизни в эпоху цифровых технологий (A/HRC/RES/42/15) и резолюции Совета по правам человека о новых и появляющихся цифровых технологиях и правах человека A/HRC/41/11 (2019 г.) и т. д.

Если вы захотите ознакомиться с данным документом подробнее, я предлагаю обратить внимание на главу «III. 1 Ценностные установки: Жизнь в мирных, справедливых и взаимосвязанных обществах». Приведу две фразы из этой главы, которые произвели на меня очень сильное впечатление: **«Субъекты связанной с ИИ деятельности должны играть роль участника и мотиватора деятельности по становлению мирных и справедливых обществ в интересах достижения всеобщего благополучия в условиях будущего взаимосвязанного мира», «в основе принципа взаимосвязанности людей лежит понимание того, что каждый человек является частью большего целого, которое процветает, когда процветают все составляющие его компоненты. Жизнь в мирных, справедливых и взаимосвязанных обществах требует наличия естественных, непосредственных и лишённых корысти уз солидарности, выражающихся в постоянном стремлении к мирным отношениям и в заботе о других людях и окружающей природной средой в самом широком смысле этого слова».**

Задумайтесь над смыслом, заложенным в этих фразах!

Они не только фундаментальны, но и являются, по моему мнению, важным вектором развития нашего с вами общества – общества будущего.

Эти тезисы важны ещё и потому, что «в долгосрочной перспективе системы искусственного интеллекта смогут соперничать с человеком в его уникальной способности оценивать свой опыт и самостоятельно действовать, что поднимает новые вопросы, касающиеся, среди прочего, самосознания и самопознания человека, его взаимодействия с социумом, культурным окружением и природой, а также вопросы автономии, свободы действий, ценности и достоинства человека».

***

Сделаю небольшое отступление и приведу пример из личного опыта.

Вышло так, что в 2020–2021 годах мне представилась уникальная возможность принять участие, в числе прочих специалистов, в работе над концепцией создания Государственной информационной системы «Уполномоченный по правам человека». В начале 2021 года я опубликовал на эту тему книгу «Цифровая экосистема Института омбудсмена: концепция, технологии, практика».

В тот период времени, работая над концепцией, мне иногда приходила мысль о том, что рано или поздно все цифровые экосистемы будут активно использовать технологии машинного обучения и ИИ. Но я совсем не задумывался о том, что все эти системы в ближайшем времени будут обладать некой степенью автономности и на них будет возложена ответственность в принятии тех или иных решений.

Сегодня, спустя совсем немного времени, я осознаю для себя тот факт, что этика применения технологий ИИ должна проходить, если так можно сказать, красной нитью через весь процесс создания и развития абсолютно всех цифровых систем во всех отраслях экономики и, прежде всего, в Государственных информационных системах.

Как подчёркивается в Рекомендациях по этике искусственного интеллекта ЮНЕСКО, «Этическая составляющая характерна для всех этапов жизненного цикла искусственной интеллектуальной системы», кроме того, «функции контроля за системами ИИ должны всегда оставаться за человеком, так как в отличие от человека «ИИ-система никогда не сможет заменить человека в качестве конечного субъекта ответственности и подотчётности. Как правило, вопросы жизни и смерти не должны передаваться ИИ-системам».

Несомненно, «учёт рисков и этических аспектов не должен препятствовать инновациям и развитию, а напротив, должен обеспечивать новые потенциальные возможности и стимулировать этичную научно-исследовательскую и инновационную деятельность, способствующую тому, чтобы ИИ-технологии были неразрывно связаны с правами человека и основными свободами, нравственными ценностями, принципами и морально-этическими воззрениями».

***

Сделаю ещё одно небольшое отступление…

Как мы уже с вами знаем, в 2019 году в целях обеспечения ускоренного развития ИИ в Российской Федерации, проведения научных исследований в этой области, повышения доступности информации и вычислительных ресурсов для пользователей, совершенствования системы подготовки соответствующих кадров был опубликован Указ Президента Российской Федерации от 10.10.2019 г. № 490, который утвердил Национальную стратегию развития искусственного интеллекта на период до 2030 года (далее – Стратегия ИИ).

В Стратегии ИИ подчёркивается, что одной из основных задач развития ИИ является создание комплексной системы регулирования общественных отношений, возникающих в связи с развитием и использованием технологий ИИ. Для решения этой задачи необходимы адаптация нормативного регулирования в части, касающейся взаимодействия человека с ИИ, и выработка соответствующих этических норм.

В Стратегии ИИ также подчёркивается, что к основному направлению создания ком-

плексной системы регулирования общественных отношений, возникающих в связи с развитием и внедрением технологий ИИ, относится вопрос разработки этических правил взаимодействия человека с ИИ.

Также отмечается, что в целях аналитической поддержки её реализации должны проводиться научные исследования, направленные на прогнозирование развития технологий ИИ, а также на прогнозирование социальных и этических аспектов их использования.

В 2021 году Минэкономразвития России в целях реализации Национальной стратегии развития ИИ на период до 2030 года разработало паспорт федерального проекта «Искусственный интеллект».

Финансирование Федерального проекта «Искусственный интеллект» в 2021–2024 гг. составляет 31,5 млрд рублей, из которых 24,6 млрд рублей выделяется из федерального бюджета, а также привлечено из внебюджетных источников 6,9 млрд рублей.

Соответственно, 5,7 млрд рублей выделялось на проведение конкурса по отбору получателей поддержки исследовательских центров в сфере ИИ, в том числе в области «сильного» ИИ, систем доверенного ИИ и этических аспектов применения ИИ.

Так вышло, что в этом конкурсе я принял самое непосредственное участие, и мне выпала роль написать программу и план мероприятий Центра сильного и прикладного искусственного интеллекта МГТУ им. Н. Э. Баумана. Подробнее об этом читатель может узнать из моей книги «Как создать центр искусственного интеллекта за 100 дней».

В августе 2021 года Аналитическим центром при Правительстве России был проведён конкурс по отбору получателей поддержки исследовательских центров в сфере ИИ, в том числе в области «сильного» ИИ, систем доверенного ИИ и этических аспектов применения ИИ.

Согласно требованиям конкурсной документации для участников отбора были определены 14 передовых направлений развития сферы ИИ, в том числе «сильного» ИИ, систем доверенного ИИ и этических аспектов применения ИИ (направление 14 «Этические аспекты применения искусственного интеллекта»).

В конкурсной документации «этическим аспектам применения искусственного интеллекта» даётся следующее определение: «Этические аспекты применения искусственного интеллекта – это свод норм, правил и разработанных центром методических рекомендаций, регламентирующих применение систем искусственного интеллекта в рамках направления деятельности центра, обеспечивающих соблюдение прав и свобод человека, гарантированных Конституцией Российской Федерации».

Здесь сделаю небольшую ремарку и скажу, что из этого определения было не совсем ясно, о каком «центре методических рекомендаций» идёт речь и где искать упомянутый свод норм и правил, разработанных этим самым центром? Потому как над похожим документом под названием «Кодекс этики искусственного интеллекта» работала так называемая «группа «Альянс» (правильное наименование – Ассоциация «Альянс в сфере искусственного интеллекта»), в который входят такие компании, как Яндекс, VK, МТС, РФПИ и Газпром. Да, и сам Кодекс был утверждён и принят несколько позже, после проведения самого конкурса (о чём поговорим далее).

По результатам конкурса в одном из шести высших учебных заведений нашей страны должен был быть создан центр, результатами деятельности которого должны были стать «решения» и «продукты», содержащие научно обоснованные этические подходы и ориентиры, востребованные и доступные для практического применения представителями государства, бизнеса, экспертного и научного сообщества, а также широкой общественности, в том числе международной. Эти «решения» и «продукты» должны были служить основой при разработке государственными органами документов стратегического планирования, нормативно-правовых актов и иных инструментов регулирования и саморегулирования в сфере ИИ.

НИЦ «Курчатовский институт» подал единственную заявку по «этике ИИ».

Как отметил заместитель председателя Правительства Российской Федерации Дмитрий Николаевич Чернышенко, **«Обществу нужен надёжный ИИ с вероятностью ошибки ниже, чем у человека. Права и свободы граждан гарантированы Конституцией. Наша обязанность – реализовать механизмы по их защите независимо от среды, в которой находится человек. Соблюдение этических норм при работе с ИИ позволит предотвратить их нарушение. Поэтому правительство приветствует подписание профессиональным сообществом Кодекса этики ИИ, он позволит повысить уровень доверия граждан к новым технологиям. Опираясь на лучшие практики, Россия входит**

в десятку стран, для которых этичность развития важнейшей технологии XXI века имеет государственное значение»[4].

Но, к сожалению, по результатам конкурсного отбора Аналитический центр при Правительстве Российской Федерации не выбрал ни один ВУЗ по теме «Этические аспекты применения искусственного интеллекта». Таким образом людьми, принимающими решения в интересах нашего с вами государства, не были учтены ни основные положения Национальной стратегии развития искусственного интеллекта на период до 2030 года, ни положения Рекомендаций ЮНЕСКО по этике искусственного интеллекта по стимулированию этичной научно-исследовательской и инновационной деятельности.

***

Но вернусь к основной теме этики и этических проблем, связанных с применением технологий и систем ИИ.

26 октября 2021 года состоялся Первый международный форум «Этика искусственного интеллекта: начало доверия». В рамках этого форума была организована церемония торжественного подписания «Национального кодекса этики искусственного интеллекта».

Форум стал первой в России специализированной площадкой, где около полутора тысяч разработчиков и пользователей технологий ИИ обсудили в рамках пяти параллельных секций шаги по эффективному внедрению этики ИИ в приоритетных отраслях экономики Российской Федерации. Вопросы, которые обсуждались на форуме вызвали у меня, как и у многих других, самый что ни на есть живой интерес, и порой было сложно выбрать, кого из докладчиков и на какой сессии слушать.

Я обратил особое внимание на то, что не остался незамеченным вопрос, связанный с религией и ИИ. Приятно осознавать, что в этом вопросе мы солидарны с мнением ЮНЕСКО: «Государствам-членам следует принять регламентирующие положения, которые на всём протяжении жизненного цикла ИИ-систем обеспечат согласованность мер, принимаемых субъектами связанной с ИИ деятельности, с международными нормами, стандартами и принципами в области прав человека при всестороннем учёте существующих социально-культурных различий, в том числе местных обычаев и религиозных традиций, а также приоритета и универсальности прав человека».

Что же касается меня, то мне повезло выступить с докладом на тему «Роль искусственного интеллекта в образовании».

Первыми к Кодексу присоединились порядка двадцати компаний, среди которых Сбер, Яндекс, МТС, VK, «Газпромнефть», Российский фонд прямых инвестиций (РФПИ) и другие.

10 ноября 2021 года на Международной конференции по искусственному интеллекту и анализу данных AI Journey к подписанию Национального Кодекса этики искусственного интеллекта присоединились МГТУ им. Баумана, «Вижн Лабс», «Лаборатория «Наносемантика», Cognitive Pilot, VEB Ventures, группа компаний «ЦРТ», «Программные системы Атлансис» и АНО «Диалог».

Что же это за документ «Кодекс этики в сфере искусственного интеллекта»?

Как отмечается в самом документе, «Кодекс этики в сфере искусственного интеллекта (далее – Кодекс) устанавливает общие этические принципы и стандарты поведения, которыми следует руководствоваться участникам отношений в сфере искусственного интеллекта (далее – Акторы ИИ) в своей деятельности, а также механизмы реализации положений настоящего Кодекса. Кодекс распространяется на отношения, связанные с этическими аспектами создания (проектирования, конструирования, пилотирования), внедрения и использования технологий ИИ на всех этапах жизненного цикла…»[5].

К главным приоритетам развития технологий ИИ в защите интересов и прав людей и отдельного человека относятся:

1. Человеко-ориентированный и гуманистический подход.
2. Уважение автономии и свободы воли человека.
3. Соответствие закону.
4. Недискриминация.
5. Оценка рисков и гуманитарного воздействия.

Кодекс призывает к ответственности Акторов (в том числе физических и юридических лиц, присоединившихся к нему) посредством реализации следующих принципов:

1. Риск-ориентированного подхода в разработке технологий и эксплуатации систем ИИ.
2. Ответственного отношения к вопросам влияния технологий и систем ИИ на обще-

4. Этику ИИ определит Кодекс. [Электронный ресурс] // www.comnews.ru URL: www.comnews.ru/content/217122/2021-10-27/2021-w43/etiku-ii-opredelit-kodeks

5. Кодекс этики в сфере ИИ. [Электронный ресурс] // a-ai.ru URL: www.a-ai.ru/code-of-ethics/ (дата обращения: 31.01.2022).

ство и граждан на каждом этапе их жизненного цикла.

3. Предосторожности, которая выражается в предотвращении или ограничении наступления событий морально неприемлемых для человека и общества последствий.
4. Непричинения вреда жизни и здоровью человека, имуществу граждан и юридических лиц, окружающей среде.
5. Процедуры идентификации ИИ в общении с человеком и информирования людей об их взаимодействии с системами ИИ.
6. Безопасности работы с данными посредством обеспечения их охраны и защиты.
7. Реализации процедур информационной безопасности посредством обеспечения защиты от несанкционированного вмешательства в работу систем ИИ третьих лиц и информирования людей об инцидентах информационной безопасности.
8. Добровольной сертификации и соответствия положениям Кодекса в соответствии с законодательством Российской Федерации.
9. Контроля рекурсивного самосовершенствования систем ИИ, а также выявления и проверки информации о способах и формах создания так называемых универсальных или «сильных» систем ИИ и предотвращении возможных угроз, которые они несут.
10. Поднадзорности со стороны человека на всех этапах жизненного цикла функционирования систем ИИ.
11. Ответственности. За все последствия работы систем ИИ всегда должен отвечать человек (физическое или юридическое лицо, признаваемое субъектом ответственности в соответствии с действующим законодательством Российской Федерации).

Также в Кодексе подчёркивается, и с этим нельзя не согласиться, что технологии ИИ нужно применять по назначению и внедрять там, где это принесёт пользу людям, а также с тем, что нужна максимальная прозрачность и правдивость в информировании об уровне развития технологий ИИ, их возможностях и рисках.

В качестве инструмента реализации вышеупомянутых принципов и положений Кодексом предусмотрено назначение Акторами уполномоченных по этике ИИ и создание внутренних отраслевых комиссий, а также создание комиссии по реализации Национального кодекса в сфере этики ИИ. Как отмечается в Кодексе, «комиссия может иметь рабочие органы и группы, состоящие из представителей бизнес-сообщества, науки, государственных органов и иных заинтересованных сторон. В рамках комиссии рассматриваются заявления Акторов ИИ на присоединение к положениям настоящего Кодекса и ведётся реестр Акторов ИИ, присоединившихся к Кодексу. Обеспечение деятельности комиссии и ведение её секретариата осуществляется Ассоциацией «Альянс в сфере искусственного интеллекта» при участии иных заинтересованных организаций».

Какие же остаются впечатления после ознакомления с Кодексом в сфере этики ИИ, разработанным «Альянсом в сфере искусственного интеллекта»?

А впечатления смешанные…

С одной стороны, и это несомненно, Кодекс – это большой и очень важный шаг вперёд на пути к становлению мирных и справедливых обществ в интересах достижения всеобщего благополучия в условиях будущего, я бы сказал, взаимосвязанного цифрового и реального мира.

С другой стороны, на момент начала 2022 года, на мой скромный взгляд, – этот документ ещё «сыроват» и требует качественной детальной проработки (в том числе в уточнении терминов и определений), а также наполнения его полезной и грамотно структурированной информацией. «Альянсу» же хотелось порекомендовать в качестве экспертов выбрать не только представителей бизнеса и сотрудников своих организаций, но и экспертов и учёных в этой и смежных предметных областях из других уважаемых ВУЗов и организаций.

Уверен, уважаемый читатель, если ему будет необходимо, ознакомится с оригиналами документов самостоятельно и сможет сделать свои собственные выводы.

Подводя итог, процитирую мнение Татьяны Владимировны Матвеевой, начальника Управления Президента РФ по развитию информационно-телекоммуникационных технологий и инфраструктуры связи, которая немало сил вложила в развитие «этики искусственного интеллекта» и отметила, что **«самым главным принципом развития, наивысшей ценностью искусственного интеллекта остаётся человекоцентричность. Он должен быть нацелен на благо человека, развитие его возможностей, созидание и помощь», а также подчеркнула, что «… важно, чтобы в рамках критически важной инфраструктуры работали такие же и алгоритмы искусственного интеллекта, и сам искусственный интеллект, который разработан, безусловно, российскими разработчиками, для того чтобы мы понимали, какие можем получить результаты его работы»**[6] [7].

Александр Юрьевич Чесалов

д.т.н.

6. Глава IT-управления Кремля назвала неэтичным навязывание решений искусственным интеллектом. [Электронный ресурс] // tass.ru URL: www.tass.ru/ekonomika/12767521
7. Искусственный интеллект должен делать все, чтобы уважать своих «родителей» и помогать им. [Электронный ресурс] // www.hse.ru URL: www.hse.ru/news/expertise/462998246.html

Чем для отрасли кибербезопасности ознаменовался 2021 год?

2 декабря профессионалы по ИБ собрались в Москве на конференции «Код ИБ: ИТОГИ», чтобы подвести итоги года и поделиться выводами и аналитикой.

Стартовали с вводной дискуссии и вместе с приглашёнными экспертами – Николаем Зубаревым (АНО «Цифровая экономика»), Валерием Комаровым (Департамент информационных технологий г. Москвы), Виталием Терентьевым, (HeadHunter Group), Евгением Питолиным (независимым экспертом) и Владимиром Ульяновым (компания Zecurion) – обсудили ключевые события и выводы прошедшего 2021 года.

Эксперты отметили, что с каждым годом изменяется отношение бизнеса к ИБ. С одной стороны, бизнес хочет всё больше, при этом тратя на это меньше денег. С другой стороны, безопасникам нужно по-прежнему учиться общаться с бизнесом на одном языке и доносить необходимость вложений в безопасность.

Поговорили о том, как меняется роль государства и насколько законодательные инициативы помогают или, наоборот, мешают бизнесу.

Обсудили, как меняется ландшафт угроз и как при этом должны меняться стратегии защиты.

От вводной дискуссии плавно перешли к прикладным темам, и на секции «Защита инфраструктуры», модератором которой выступил Евгений Питолин – независимый эксперт по ИБ, посмотрели на данные аналитики, говорящие, что:

- концепцию Zero Trust, о которой сейчас так много говорят, начали применять лишь 14% респондентов, участвовавших в опросе. Ещё 34% отметили, что планируют заняться реализацией концепции в ближайшее время, при этом 52% пока вообще об этом не думают;
- самыми актуальными способами защиты ИТ-инфраструктуры чаще всего называют проверку актуальности обновлений безопасности и регулирование правила и исключения для файрволов;
- основной стратегией защиты инфраструктуры большинство обозначили следующую: каждый день улучшать систему безопасности и искать лучшие варианты обновления.

Продолжили работу секции выступлениями экспертов:

- Сергей Чекрыгин – менеджер по работе с заказчиками компании Check Point, который поделился секретом, как безопасно работать на удалёнке;
- Дмитрий Хомутов – директор ООО «Айдеко», поделившийся опытом, как компания ответила

на вызов Covid-19 при организации удалённого доступа и защиты периметра;

- Роман Подкопаев – генеральный директор компании Makves, раскрывший основные результаты аудита рисков ИТ-инфраструктуры.

Модератором секции «Защита от внутреннего нарушителя» (спонсор – компания Zecurion) стал Иван Бируля, руководитель службы безопасности REDMOND, где с экспертами и участниками обсудил, как за год продвинулись технологии защиты от внутренних угроз.

Секцию тоже начали с аналитики, которая показала, что:

- наиболее серьёзными угрозами корпоративной безопасности по-прежнему называют фишинг и социальную инженерию. Далее идут целенаправленные кражи информации, таргетированные атаки и саботаж сотрудников;
- большинство компаний используют DLP-системы и в целом довольны, при этом есть существенный процент компаний, которые DLP не пользуются и не планируют;
- наиболее популярными инструментами для решения проблем внутренней безопасности респонденты отмечали обучение сотрудников, доведение информации об ответственности и строгое ограничение пользователей в правах доступа;
- самыми сложными задачами для службы ИБ по-прежнему остаются выявление эмоционального состояния сотрудников и прогнозирование их поведения.

Продолжили секцию выступления экспертов:

- Алексей Раевский – генеральный директор компании Zecurion, поделился тем, как DLP-системы перешли от разбора инцидентов к рисковой модели;
- Даниил Бориславский – руководитель отдела аналитики компании StaffCop, рассказал, какие результаты дал контроль за сотрудниками;
- Сергей Волдохин – директор ООО «Антифишинг», поделился историями о том, как атаковали людей в 2021 году и как защитить своих сотрудников в 2022 году;
- Харитон Никишкин – коммерческий директор, соучредитель компании Secure-T, поговорил о фишинге, его последствиях и о том, как с этим бороться.

В следующей секции «Мониторинг. Расследование инцидентов», которую модерировал Аркадий Грановский – главный специалист по защите информации компании HeadHunter Group, обсудили, что нового с точки зрения мониторинга событий ИБ, выявления и расследования инцидентов произошло за последний год;

- Александр Булатов – коммерческий директор компании RuSIEM, поделился итогами компании за прошедший год и планами на грядущий;
- Ольга Гутман – генеральный директор ООО «Оксиджен софтвер», говорила о форензиковом продукте в расследовании инцидентов;
- Лука Сафонов – директор ООО «Киберполигон», рассказал, как эволюционировали вирусы-шифровальщики.

Продолжили программу итогами от экспертов:

- Роман Жуков – Product Security Manager компании Intel, рассказал, как воспитывать у сотрудников «безопасное поведение»;
- Алексей Мунтян – эксперт по защите персональных данных, соучредитель компании РРРА, говорил о том, как меняется законодательство о защите персональных данных;
- Алла Горбушина – старший юрист практики государственного регулирования, интеллектуальной собственности, медиа и технологий компании Hogan Lovells, поделилась бесценной информацией о том, какие громкие дела, связанные с ИБ, прошли через российские суды в 2021 году и главное – чего ждать в 2022 году;
- Александр Кондратенко – начальник управления ПАО Росбанк, поделился опытом, как банк реализовал SGRC;
- Николай Казанцев – начальник отдела ИБ НТФФ «Полисан», поделился кейсом, как компания связала риски, комплаенс, каталоги угроз и что из этого вышло.

Благодарим всех участников и партнёров и ждём встречи в следующем году.

Отзывы участников конференции:

- Семенычев Алексей – технический специалист по ИБ ООО «Гарда-Технологии»: *«Динамично, интересно и по-домашнему. Код ИБ, как всегда, радует высоким качеством информации и материалов. Удачи вам!»*
- Буренков Виктор – специалист по ИБ АО «Неофлекс Консалтинг»: *«Полезное мероприятие для обмена отраслевой информацией».*
- Иванюгин В.М. – доцент МИРЭА – Российский технологический университет: *«Особенно понравилась общая оценка состояния проблемы безопасности с призывом к экспорту отечественных продуктов. Высший профессиональный уровень! Спасибо!»*

Партнёр по защите информации от утечек:
Zecurion

Партнёры мероприятия:
Makves, Ideco, RuSIEM, StaffCop, ООО «Оксиджен Софтвер», Check Point, Secure-T

Генеральный медиапартнёр:
Xakep

Медиапартнеры:
Jobsora, Codeby, Jooble, SPB CIO Club, ООО «Берза», компания «БИТ», Iso27000, Wadline, Ciso Club, «Выберу», Портал ЭЦП, ООО «Системный администратор», Center Cio, Jetinfo, CTF News, World expo, ЯиТЫ, Mobile Business, ООО «Первый цифровой», компания «Админим с буквой», Global CIO, 4CIO, IT World, Национальный банковский журнал, ICT2GO, Bis Journal, IT Events

Контакты для связи:

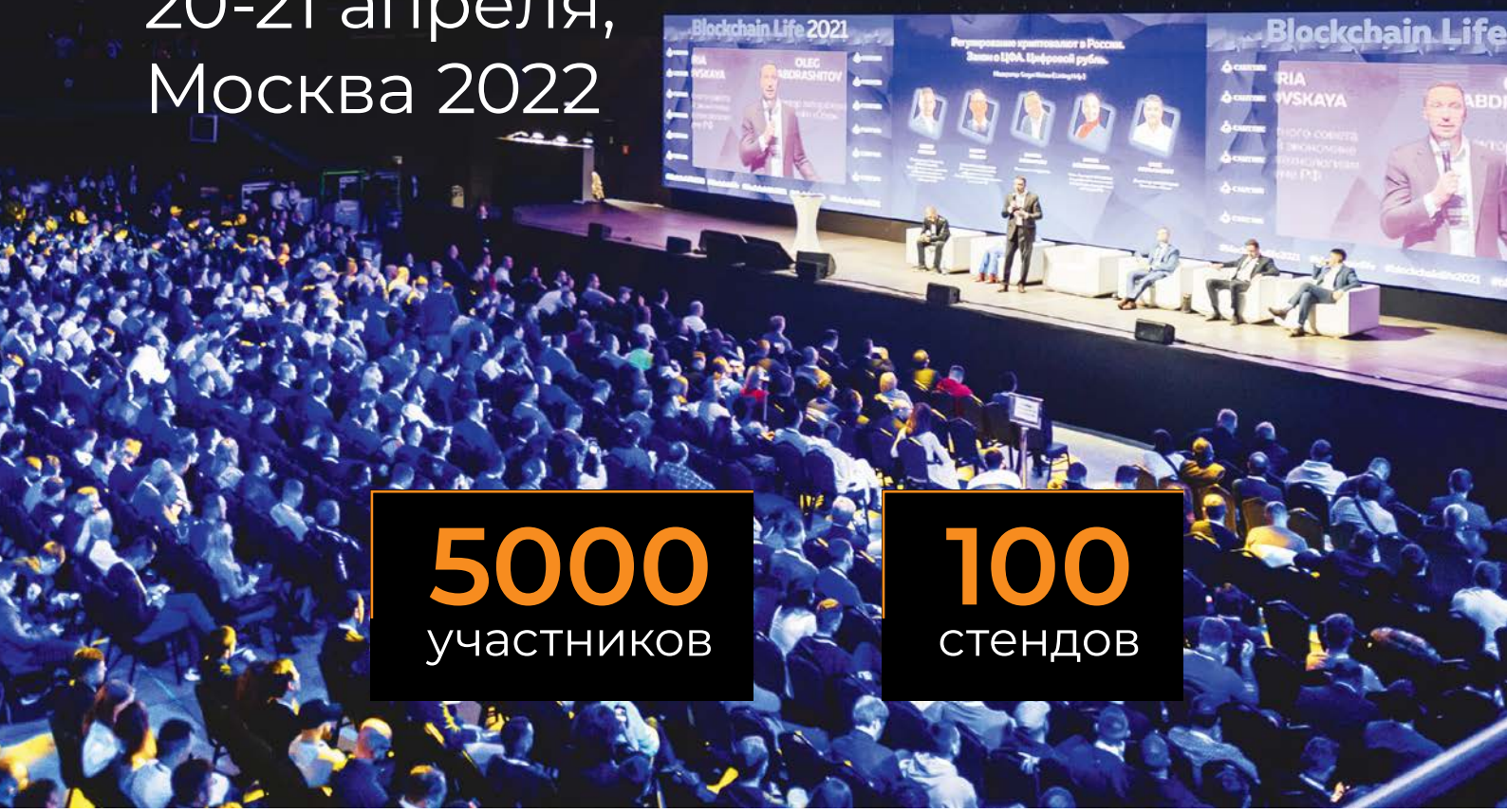
Цвариани Мария

E-mail: pr@expolink-company.ru

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Blockchain Life 2022

20-21 апреля, Москва 2022



20–21 апреля в Москве состоится 8-ой Международный форум по блокчейну, криптовалютам и майнингу – Blockchain Life 2022.

Форум собирает более **5000 участников** и **100 стендов.**

Среди гостей форума как **профессионалы** индустрии, так и те, кто только **начинает** свой путь: трейдеры, майнеры, предприниматели из крипто и классического бизнеса, инвесторы, блокчейн-разработчики, представители государственной власти и многие другие. Участие в форуме позволяет получить **передовые знания** и обзавестись **множеством** новых контактов, оказавшись среди лидеров мирового крипто сообщества. На форуме будут обсуждаться самые **актуальные темы** индустрии, такие как: **способы заработка** на криптовалютах в 2022 году, **развитие DeFi и метавселенных, особенности эффективного майнинга, перспективы NFT,** внедрение блокчейна в бизнес и государство и многое другое.

Среди ведущих спикеров форума:

- Сергей Хитров, основатель Listing.Help
- Владислав Мартынов, предприниматель, глава центра компетенции Ethereum Россия, основатель BlockGeeks.
- Глеб Костарев, директор Binance в Восточной Европе.

- Вадим Крутов, CEO Bitfury Russia.
- Тон Вэйс, криптотрейдер и биткоин максималист.
- Иван Чебесков, Директор Департамента финансовой политики Министерства Финансов РФ.
- Анатолий Каплан, основатель Forklog.

В рамках форума традиционно состоится международная премия **Blockchain Life Awards** и конкурс перспективных стартапов **StartUp Pitch**. Организатором форума уже в 8-ой раз выступает крупнейшее агентство по листингу на биржах – **Listing.Help**.

Полный список спикеров доступен на сайте.

Билеты доступны на официальном сайте.

Всероссийский форум «Защита и безопасность Умного города»

2 февраля в Москве состоялся форум «Защита и безопасность умного города», организованный центром конференций «Сегодня».

Эксперты обсудили реализацию концепций Умного города – Smart City, Безопасного города – Safe City и Электронного города – E-City на пути к построению «Безопасных умных городов». В форуме приняли участие представители НИОКР АПК «Безопасный город», Агентства инноваций города Москвы, проектного офиса Lean Smart City АО «Русатом Инфраструктурные решения», компании «КорКласс», Московской ТПП, РФРИТ, НИУ ВШЭ, Госинспекции по недвижимости города Москвы, компаний «АКТИВ», НТЦ «Система», NETVISION, «ИТР» и другие участники.

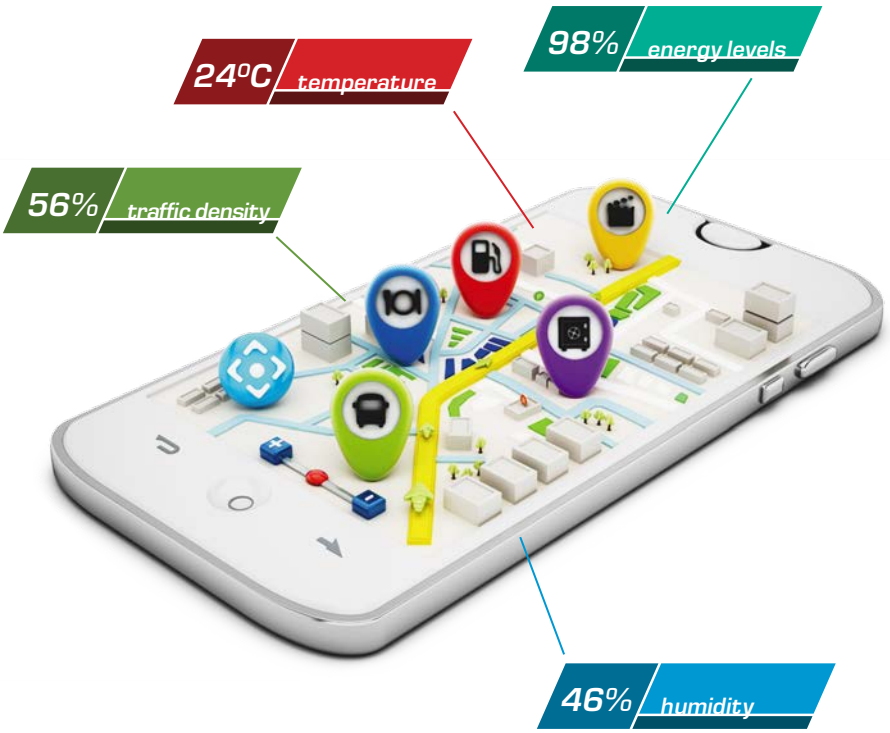
О новых возможностях, обязательствах, участниках проекта Федерального закона о «Безопасном городе» в своём докладе сообщила Оксана Якимюк – генеральный конструктор АПК «Безопасный город». С 2014 года, когда координатором «Безопасного города» начал выступать МЧС России, планомерно формируется и продолжает кристаллизироваться Единая система обеспечения общественной безопасности, общественного порядка и безопасности среды жизнедеятельности, в рамках которой ведётся мониторинг и предупреждение более 100 видов угроз. Средством автоматизации Единой системы является АПК «Безопасный город».

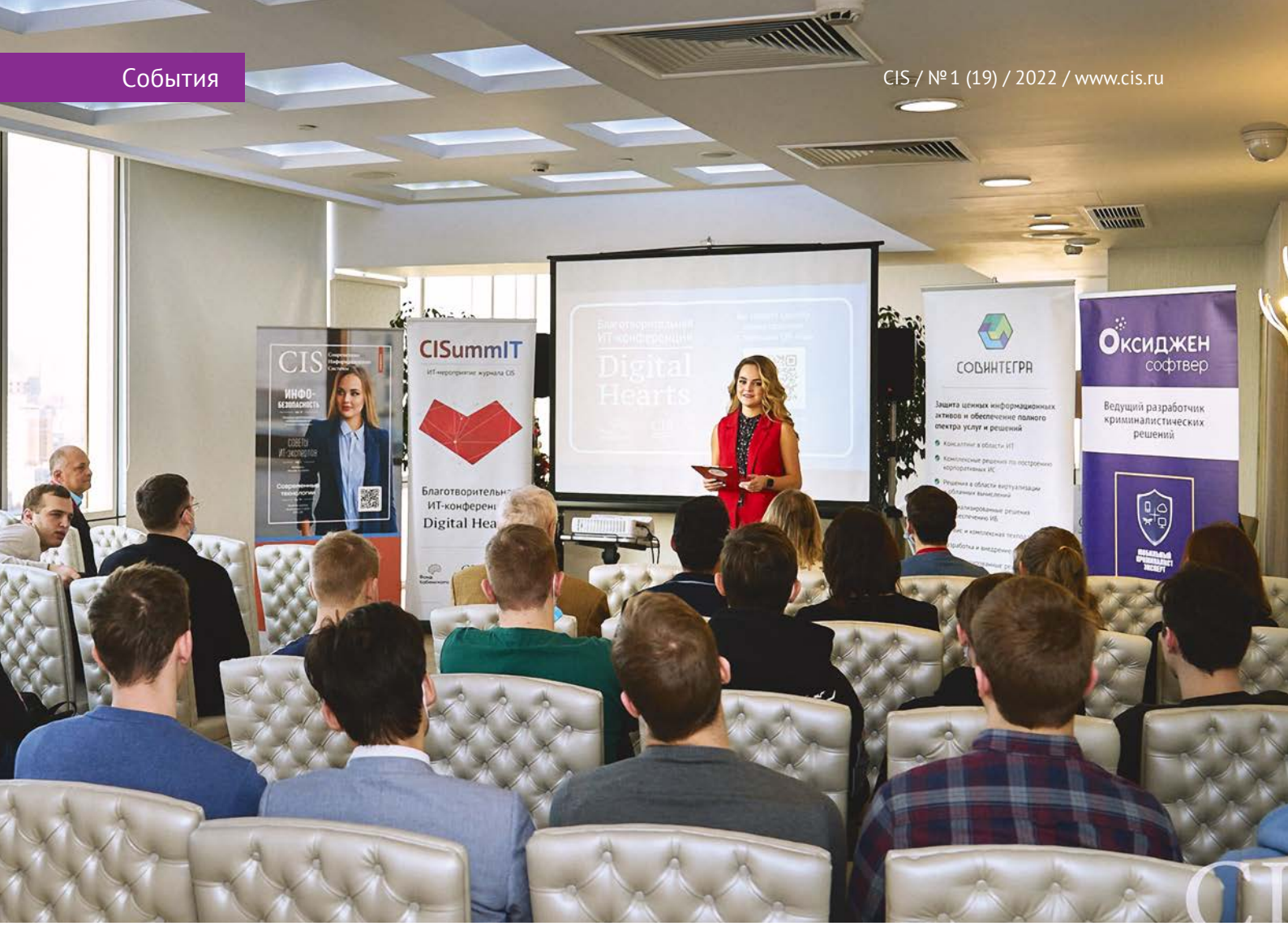
В рамках НИОКР по «Безопасному городу» были разработаны научные и технические подходы для автоматизации мониторинга угроз и реагирования на них. Задача Безопасного города построить умное реагирование, а не просто автоматизировать существующие процессы. Если автоматизировать хаос – получится автоматизированный хаос, у нас же совсем другая цель. «За 2021 год только 10 регионов внедрили БГ (прим. «Безопасный город»), и то не в полной мере. Поэтому приняли решение о том, что должен быть ФЗ (прим. Федеральный закон) о БГ, раньше – только концепция, у региона появятся обязательства по внедрению систем», – сообщила Оксана Якимюк.

Городская среда – это сложнейшая экосистема, в которой взаимосвязаны объекты городской инфраструктуры, жители, службы и власть. По мнению генерального директора «КорКласса» Антона Гуренко, «критически важно понимать существующие связи, процессы и закономерности функционирования этой экосистемы, поскольку они описываются информационной моделью, которая лежит в основе программной

платформы «Безопасного города». Мне было приятно увидеть интерес гостей форума к опыту нашей команды, накопленному за годы внедрений «Безопасных городов», решениям и технологиям, которые мы разработали. Для нас было важно синхронизировать позиции с наукой, услышать о практиках применения «умных» технологий и цифровизации в смежных областях городского управления».

В деловой сессии обсуждались следующие вопросы: разработка согласованной стратегии цифрового развития систем безопасности города и региона, ответственность бизнеса при внедрении решений в области умной безопасности, кадровый «голод», работа государственных механизмов поддержки и коммерциализации инновационных разработок. Модератором сессии выступил Владимир Ульянов – руководитель аналитического центра Zecurion.





Фотоотчёт благотворительной ИТ-конференции Digital Hearts

Вот уже в пятый раз редакция ИТ-журнала CIS собрала гостей и участников мероприятия, объединяя познавательную и благородную цели воедино – заслушать и обсудить актуальные и самые интересные доклады в сфере информационных технологий, информационной безопасности и цифровизации, а также собрать средства для помощи детям с заболеваниями головного и спинного мозга.

На зимней благотворительной ИТ-конференции Digital Hearts – 2021 с докладами выступили:

- **Федотов Валентин** – руководитель отдела информационной безопасности компании «Протект Информ»
- **Хоменко Ануш** – заместитель директора «Высшей Школы Программирования»
- **Лебедев Анатолий** – доцент кафедры информационной безопасности МГТУ им. Н. Э. Баумана
- **Иванов Михаил** – генеральный директор компании S-Terra.

Все собранные денежные средства перечислены в благотворительный фонд Константина Хабенского. Отметим, что нам уже удалось помочь 16-ти детям побороть недуг.

До новых встреч на конференции Digital Hearts от ИТ-журнала CIS!

CIS Современные Информационные Системы

Сайт конференции: www.cisevent.ru


для директоров и руководителей
CIS


CIS
Современные Информационные Системы
Информационные технологии, безопасность и защита данных


CISSummIT


для директоров и руководит
CIS


CIS


CIS
SummIT
ИНФО-БЕЗОПАСНОСТЬ
СОВЕТЫ ИТ-ЭКСПЕРТОВ
CIS


с помощью QR-кода
1. Отсканируйте QR-код.
2. Пожертвуйте желаемую сумму.
ÖMANKÖ


CIS


CIS
Современные Информационные Системы
CISummIT
ИТ-мероприятие журнала CIS
ИНФО-БЕЗОПАСНОСТЬ
СОВЕТЫ ИТ-экспертов
Современные технологии
Digital Hearts
БЛАГОДАРНОСТЬ
ИТ-жур
CIS


CIS


Вы можете сделать пожертвование с помощью QR-кода
1. Отсканируйте QR-код.
2. Пожертвуйте желаемую сумму.
Digital Hearts
Digital Hearts
ПРОГРАММА
CIS


ИТ-ж ал CIS
для директо руководителе
CIS


CIS


CIS


ИТ-журнал CIS
для директоров и руководите.
CIS


SummIT
Благотворительная
ИТ-конференция
Digital
Hearts
CIS


CIS


ИТ-журнал CIS
CIS


CISummIT

Гороскоп для ИТ-компаний на весну 2022 года

Зная, под каким знаком зодиака была основана ваша компания, и руководствуясь нашим гороскопом, вы будете в курсе того, что её ожидает и к чему надо готовиться для роста и развития бизнеса.

Овен
21 марта – 20 апреля

Овны будут крутиться как белки в колесе. То одно, то другое потребует внимания. Чтобы не сбиться с толку, нужен продуманный производственный график или чёткий бизнес-план. Кто-то из партнёров станет очень рассчитывать на помощь вашей компании.

Руководству компании нужно позаботиться о том, чтобы рядом всегда была «правая рука», которой можно доверить все дела. Когда производство слишком загружено, трудно успеть всё делать в одиночку.

В апреле удачно пройдут сделки, которые давно планировались. Позаботьтесь о репутации компании. Нужно искать новые концепции в работе и правильно презентовать бизнес.

В период с 10 по 20 апреля остерегайтесь легкомысленных предприятий и не вкладывайте крупные суммы в сомнительные сделки.

Телец
21 апреля – 21 мая

Тельцы очень придирчивы как к своему бизнесу, так и к партнёрам. Хотят, чтобы всё, что делают выглядело безупречно. Если что-то не получается, то всё выходит из-под контроля, что ещё больше усугубляет положение компании на рынке. Если хотите блестяще завершить крупные сделки – работайте в сотрудничестве с успешными партнёрами, которые мыслят категориями вашего бизнеса.

В апреле можно выполнить любой поставленный план, если не работать в одиночку. Руководителям нужно ослабить давление на коллектив, тогда можно добиться большего.

Сейчас компаниям может повезти в новых проектах, реализуются те, что давно задумывались. Возможно, придёт помощь в продвижении ваших продуктов или услуг. Не останавливайтесь на полпути. Если не хватает средств, то возьмите кредит. Успех не заставит себя долго ждать.

Близнецы
22 мая – 21 июня

Компанию приятно порадует высшее руководство (Совет директоров или госчиновники), особенно если ваш бизнес связан с финансами. Можно рассчитывать на неожиданную прибыль. Деньги достанутся компании легко, и потратить их можно на незапланированные проекты. Но не стоит злоупотреблять везением, это может не понравиться партнёрам, коллективу, – лишние слухи ни к чему.

Если хотите больших доходов, будьте готовы усилить производство, изменить режим работы и запланировать длительные командировки для сотрудников.

Рак
22 июня – 22 июля

На производстве вероятна неразбериха, дезинформация и аврал. Неожиданно свалятся проекты, которые ранее казались завершёнными. Компании нужно готовиться к форс-мажорам, внезапной смене направления деятельности. Могут поступить предложения о смене руководящего состава тем, кто более опытен, не стоит отказываться. Но помните, что это большая ответственность.

На слишком высокие доходы можно не рассчитывать. Предстоят большие траты, связанные с производством. Кроме того, есть риск нарваться на штраф.

Если деятельность компании связана с творчеством, стоит подумать, прежде чем публиковать новый шедевр. Сейчас можно оказаться не в топовом направлении, что принесёт разочарование.

Лучшими днями апреля станут 20, 25 и 26 число. О планах компании не стоит делиться даже с близкими партнёрами. Если хотите внести новшества в производство, придётся придумать что-то более оригинальное, чтобы удивить заказчиков.

Лев
23 июля – 22 августа

В работе компаний Львов грядут перемены. Возможно, это глобальная перестройка, которая ожидалась. Компании могут сделать интересное предложение, связанное с повышением её статуса. Не стоит пасовать перед новыми направлениями деятельности – это отличный повод выделиться на рынке. В переговорах с партнёрами стоит проявить инициативу и не упустить возможность продемонстрировать сильные стороны бизнеса.

Есть возможность столкнуться с финансовыми сложностями. Придётся искать новые способы расширить бизнес. Можно проявить креативность, привлечь новых людей – любые способы хороши, чтобы защитить дело.

Приятно удивят давние партнёры, которые предложат помощь в непростое время. Сейчас лучше отказаться от серьёзных сделок и рискованных вложений.

Дева
23 августа – 22 сентября

Компаниям Девам нужно проявить оригинальность. Если хотите добиться высокого рейтинга, придётся проявить креативность. Не исключены дальние поездки за границу, которые могут показаться неожиданными и пугающими. Но это шанс заработать дополнительный капитал и преуспеть на рынке в будущем.

Молодым компаниям трудно найти своё место среди предприятий – китов. Финансовый вопрос не останется без внимания. Вы всегда контролируете свой бюджет, что очень хорошо, однако всё равно возникнет ситуация, которая не входила в планы.

Весы
23 сентября – 22 октября

У компаний Весов есть проблема с пониманием их дальнейшего развития. Сложилась неприятная ситуация? Обратитесь к партнёрам или к бизнес-наставникам, чтобы получить подробные разъяснения по выходу из кризиса. Не бойтесь того, что могут появиться недочёты в управлении бизнесом.

Есть вероятность, что вас хотят подставить или втянуть в неприятную ситуацию конкуренты. Стоит задуматься о том, кто вас окружает. При подписании серьёзных контрактов советуйтесь с юристами или с компетентными партнёрами, которым доверяете.

Финансовое положение относительно стабильно, однако не стоит совершать крупных сделок, особенно это касается недвижимости. Если хотите вложить средства в крупное предприятие, совершайте сделку в конце апреля.

Скорпион
23 октября – 22 ноября

Скорпионы хотят преуспеть в финансовых делах, поэтому стараются браться за любой объём работ. В апреле представится много шансов увеличить свой бюджет. Не беритесь за проекты, если не уверены в их завершении в срок. Возникнут непредвиденные обстоятельства, которые потребуют помощи от партнёров или коллектива.

Беритесь за финансовую дисциплину. Тщательно планируйте бюджет и расходы: есть риск попасть в финансовую кабалу. Не допускайте этого. Придётся попрощаться с некоторыми ценностями.

Стрелец
23 ноября – 21 декабря

У Стрельцов наступает очень напряжённое время. Будьте готовы к авралу. Внезапно возникнут происшествия на производстве, и рядом должны быть надёжные партнёры и персонал. Руководству не следует всё тянуть в одиночку, обязательно найдите партнёров-помощников. Если чувствуете, что зашли в тупик, возьмите перерыв, смените направление деятельности.

Руководству придётся проявить строгость к коллективу, чтобы добиться положительных результатов в развитии компании. Многие подчинённые пользуются добротой топ-менеджеров и служебным положением, нужно уделить этому внимание.

Может возникнуть неприятная ситуация на производстве, которую придётся долго разрешать.

Козерог
22 декабря – 20 января

Меньше всего Козерогов будет волновать их статус на рынке. Они полностью погружены в посторонние от бизнеса дела. Это не останется без внимания со стороны госорганов. Компанию могут поставить перед серьёзным выбором или наложить штраф из-за несоблюдения каких-то законов. Необходимо серьёзно пересмотреть приоритеты, иначе рискуете потерять компанию.

Если давно планировали сменить вид деятельности, то лучшим временем станет первая декада апреля. Но нужно адекватно оценивать потенциал компании: проявить истинные возможности и не слишком задирать нос перед заказчиками.

Водолей
21 января – 19 февраля

Перед Водолеями встанет непростой выбор относительно дальнейшего развития и выбора направления. Компания может получить сразу два совершенно противоположных предложения. Чтобы принять правильное решение, прислушайтесь к опытным коллегам и партнёрам. Дельный совет даст влиятельный человек.

Чтобы приумножить свой бюджет, можно открыть новое направление, которое принесёт дополнительный доход. Но и здесь без вложений не обойдётся. Придётся внести первоначальный капитал, но можно быть уверенным, что дело быстро окупится.

Есть опасность потери финансов в последней декаде апреля. Будьте осторожны при заключении сделок с малознакомыми поставщиками.

Рыбы
20 февраля – 20 марта

В бизнесе будет складывается не так, как запланировано. Вероятны различного рода форс-мажоры и внештатные ситуации. После середины апреля компании придётся выполнять двойной план или усилить штат. Если не получится собраться с силами, лучше взять перерыв, чтобы набрать мощности.

Руководство компании могут попросить о помощи члены коллектива, не стоит им отказывать, ведь вас считают надёжным авторитетом. Своим примером вы показываете, как нужно работать.

Финансовая сторона будет относительно нестабильна. Чтобы выровнять ситуацию с расходами и доходами, выберите особую тактику. Попробуйте несколько способов сохранить капитал или обратитесь к опытным партнёрам, у которых это получается.

Календарь мероприятий

1–2 апреля
Н.-Новгород • Онлайн-трансляция • Конференция
Конференция «Digital-Оттепель»

6 апреля
Онлайн-трансляция • Митап
DevOps meetup (Online)

7–8 апреля
Москва • Онлайн-трансляция • Конференция
БИТВА ЗА IT | 7 апреля 2022 | HR IT DAY | 8 апреля 2022 | TEAM LEAD DAY

7–8 апреля
Онлайн-трансляция • Конференция
DotNext 2022 Spring

8–9 апреля
Иннополис • Конференция
CrossConf – IT-конференция № 1 | Иннополис 8–9 апреля 2022

12–14 апреля
Онлайн-трансляция • Конференция
Heisenbug 2022 Spring

13 апреля
Онлайн-трансляция • Митап
Python meetup (Online)

18–21 апреля
Онлайн-трансляция • Конференция
HolyJS 2022 Spring

20 апреля
Онлайн-трансляция • Митап
GO meetup (Online)

25–28 апреля
Онлайн-трансляция • Конференция
JPoint 2022

28–29 апреля
Москва • Онлайн-трансляция • Конференция
TestDrivenConf++

11 мая
Онлайн-трансляция • Митап
Ruby meetup № 18 (Online)

20–21 мая
Иннополис • Конференция
IT-конференция Merge 2022

23–26 мая
Онлайн-трансляция • Конференция
Mobius 2022 Spring

26–27 мая
Москва • Конференция
DevGAMM Moscow 2022

31 мая–2 июня
Москва • Конференция
TECH WEEK 2022: новая реальность для инноваций в бизнесе

1–3 июня
Онлайн-трансляция • Конференция
Hydra 2022

6–9 июня
Онлайн-трансляция • Конференция
C++ Russia 2022

10–11 июня
С.-Петербург • Онлайн-трансляция • Конференция
HR API 2022

23 июня
С.-Петербург • Конференция
ZeroNights 2022

29 июня
Онлайн-трансляция • Митап
GO meetup (Online)

6 июля
Онлайн-трансляция • Митап
Frontend meetup (Online)

24 августа
Онлайн-трансляция • Митап
Ruby meetup № 19 (Online)

7 сентября
Онлайн-трансляция • Митап
Python meetup (Online)

1 октября
Москва • Мероприятие
ИТ-конкурс красоты «Beauty&DigITal» 2022

6–8 октября
С.-Петербург • Онлайн-трансляция • Конференция
INFOSTART EVENT 2022

19 октября
Онлайн-трансляция • Митап
GO meetup (Online)

2 ноября
Онлайн-трансляция • Митап
Python meetup (Online)

Сканворд

Пришлите разгаданный сканворд на почту info@sovinfosystems.ru
до 15-го июня и получите приз от редакции журнала «CIS».

Паля-щий зной июля

Швейцар. «Живопи-сец»

Лёгкие туфли без каблуков

Бруклин-ское «чудо» в Нью-Йорке

Одна из 4-х главных точек горизонта

«Разве-ла» на сыр Ворону

Кетчупное название помидора

Деловой портфель

Водоём надежды (песен.)

Яркая певчая птаха

«Федо-рино...» (К. Чуков-ский)

Малочис-ленный народ на Сахалине

Фран-цузский десерт

Отверстие в иголке

Прыщи, сбившие-ся в стадо

Аксессу-ар, стя-нувший талию

Учитель красно-байства

Зодиа-кальное созвездие

Авто-мобиль «Чайка»

Самый близ-кий сосед чеха

Собрание жителей (истор.)

Ступень в органах власти

«Индей-ская» рубашка

Отдел на заводе

Крякква в нежном возрасте

Налог на добав-ленную стоимость

Колёсный стержень

Мастер музыкал. инстру-ментов

Равен-ство ча-стот двух звуков

Жилая постройка

Шпионка ... Хари

Единица измерения яркости

Нити, идущие вдоль ткани

Свёрнутая хомутом шинель

Мама для бабушки

Короткая комедийная пьеса

Русскоя-зычная часть сети Интернет

Копчёная свинина

У рим-лян Марс, у гре-ков ...

ICQ устами програм-мистов

Место для разгово-ров в сети

Порошок в бетономешалке

Сокра-щённый Николя

Впадинка на щеке девушки

Наличный подергун-чик

ИТ-конкурс красоты

«Beauty&DigITal» 2022

Приглашаем к участию девушек работающих в ИТ-сфере к участию в ежегодном всероссийском ИТ-конкурсе красоты «Beauty&DigITal» 2022.

Миссия конкурса — выявить самых красивых и талантливых ИТ-девушек и сделать из обладательницы короны символ информационных и цифровых технологий России.

CIS Современные Информационные Системы

Участвуй

cismiss.ru