

Валерия
Валетина

КОГДА БЕЗОПАСНОСТЬ ДОРОЖЕ ВРЕМЕНИ?

Стр. 6

Электронная
подпись

ПЕРСПЕКТИВЫ РАЗВИТИЯ ИТ В РОССИИ

Стр. 50

Блиц-опрос среди
ИТ-специалистов

ИМПОРТО- ЗАМЕЩЕНИЕ В ИТ-СФЕРЕ

Стр. 30

Исследование

КРИПТОВАЛЮТЫ И ЛЕГАЛИЗАЦИЯ

Стр. 36

Цифровые финансовые
инструменты

РЕШЕНИЯ

4 Автоматизированная система управления предприятием «Цифровые активы»

Компания ООО «Корпоративные Бизнес Системы» (далее – CBS) – ведущий российский разработчик отечественного программного обеспечения, а также системный интегратор, специализирующийся на предоставлении расширенного спектра услуг в сфере информационных технологий на территории России, Казахстана и стран Центральной Азии.

6 Электронная подпись

Когда безопасность дороже времени?

10 Дистрибьютор программного обеспечения для бизнеса любого масштаба

МОНТ – один из крупнейших в России дистрибьюторов программного обеспечения. Группа компаний МОНТ начала свою деятельность в 1991 году и в настоящее время насчитывает более 5000 организаций в своей партнёрской сети, охватывающей всю территорию России.

СОБЫТИЯ

14 «Работы ещё много»: на AntiFraud Russia подвели итоги борьбы с мошенничеством в 2022 году

17 Тренды развития бизнеса в России за последние полгода обсудили на TECH WEEK

20 XI торжественная церемония награждения «ComNews Awards 2022»

22 Цифровая трансформация в горной добыче, металлургии, энергетике и нефтегазовой отрасли – 2022

24 CDO/CDTO SUMMIT & AWARD

Осенняя сессия III Российского Саммита по цифровой трансформации организаций и Премия CDO/CDTO Award 2022

26 Центральный российский форум по информационной безопасности «Инфофорум-2023»

АНАЛИТИКА

30 Исследование процессов импортозамещения в ИТ

36 Цифровые финансовые инструменты: криптовалюты и перспективы их легализации

Глобализация мировой экономики и развитие ИТ-технологий в финансовой сфере сделали возможным возникновение нового вида денег – криптовалют – и их последующее стремительное распространение по всему миру.

ОПЫТ

46 Главная ценность СИГМА.Академии – знания наших экспертов

В ИТ-компании «СИГМА» есть внутреннее подразделение, нацеленное на работу со студентами и привлечение молодых специалистов, – СИГМА. Академия. Руководитель Академии Александр Ерошкин рассказал о проекте, работе со стажёрами и тенденциях в сфере ИТ-образования.

48 Учебный курс по продукту JMS 3.7

МНЕНИЯ

50 Блиц-опрос среди ИТ-специалистов

50 ActiveCloud

52 Group-IB

54 NordClan

56 Axoft

57 Аурига

58 Ctrl2GO

59 Национальная платформа

60 СИНТО

61 eXpress

62 Материалистическая диалектика и информационное общество

Наука и практика современного информационного общества показывают, что механизм взаимодействия материальных и духовных процессов продолжают усложняться. Это порождает множество подходов к концепции идеального и материального, предлагаются разные теоретические принципы осмысления нынешнего этапа общественного развития.

ТЕХНОЛОГИИ

66 Чипирование человека

Плюсы и минусы биочипов

ИТ-ГОРОСКОП

68 Гороскоп для ИТ-компаний на весну 2023 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 компании.

КАЛЕНДАРЬ

70 Календарь мероприятий

КРОССВОРД

71 Скандворд

От редактора

Дорогие читатели, вот что наша редакция ИТ-журнала CIS подготовила для вас в этом весеннем выпуске.

Журнал провёл ежегодный блиц-опрос среди ИТ-директоров и руководителей, чтобы узнать их мнения о перспективах развития сферы информационных технологий в 2023 году в России. Ознакомьтесь с ответами экспертов вы можете в этом выпуске.

Мы опубликовали статью-исследование процессов импортозамещения в ИТ с тем, чтобы изучить эти процессы, выявить потребности целевых групп и определить перспективные ниши для развития.

На страницах этого выпуска мы поговорим о проблеме слишком быстрого роста криптоиндустрии, которая выходит на первый план экономической повестки дня многих стран мира.

Любителям философских дебатов будет интересно ознакомиться со статьёй нашего эксперта Анатолия Орлюка о материалистической диалектике и информационном обществе.

Также мы затронем темы интеграции современных технологий в человека, а именно чипирование.

А ещё зададимся вопросом, как обстоит дело с электронной подписью – столь важным атрибутом современной цифровой среды.

И, конечно же, по старой традиции редакция ИТ-журнала CIS объявляет о начале всероссийского ИТ-конкурса красоты «Beauty&DigITal-2023» для девушек, работающих в ИТ и цифровизации. Присылайте заявки на нашу почту – мы ждём вас!

С уважением, редакция журнала CIS

Главный редактор: Станислав Понарин.
 Директор по маркетингу: Валерия Рябина.
 Дизайн и вёрстка: Алексей Дмитриев.
 Корректор: Оксана Макаренко.
 Отдел рекламы и распространения: magazine@sovinfosystems.ru.
 Сайт: www.cis.ru, интернет-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).

За содержание рекламного объявления ответственность несёт рекламодатель. Перепечатка, использование или перевод на другой язык, а так же иное использование произведений, равно как их включение в состав другого произведения (сборник, как часть другого произведения, использование в какой-либо форме в электронной публикации) без согласия издателя запрещены.
 Предоставляя (бесплатные) текстовые и иллюстративные материалы для их публикации в данном издании общества с ограниченной ответственностью «Современные инфосистемы» отправитель даёт своё согласие на использование присланных им материалов путём их распространения через любые виды электронных (цифровых) каналов, включая интернет, мобильные приложения, смартфоны и т.д.
 Фото на обложке: Валерия Валетина.
 Тираж 5000 экз. (отпечатанный тираж).
 Журнал предназначен для лиц старше 16 лет.
 © 2023, CIS (Современные Информационные Системы).

Автоматизированная система управления предприятием «Цифровые активы»

Компания ООО «Корпоративные Бизнес Системы» (далее – CBS) – ведущий российский разработчик отечественного программного обеспечения, а также системный интегратор, специализирующийся на предоставлении расширенного спектра услуг в сфере информационных технологий на территории России, Казахстана и стран Центральной Азии.

Представляем вашему вниманию автоматизированную систему управления предприятием «Цифровые активы» (далее – АСУП «Цифровые активы»). С её помощью решаются такие задачи как:

- автоматизированное планирование регламентных работ;
- автоматизированный онлайн-контроль исполнения технического обслуживания и ремонта любого оборудования и зданий;
- мониторинг состояния оборудования;
- автоматизированное формирование наряд-заданий по устранению пред-аварийных или аварийных ситуаций;
- автоматизированная инвентаризация основных средств и товарно-материальных ценностей;
- управление складами и автоматизация инвентаризации запасов;
- анализ потребления ресурсов с помощью различных приборов и датчиков;
- экологическая безопасность.

Данный комплекс является Российским аналогом таких продуктов, как SAP PM, SAP TOIP (техническое обслуживание и ремонт), IBM Maximo, ERP Infor.

Программный комплекс построен на базе отечественного программного обеспечения, является собственной разработкой CBS, получил международную награду и признание на ежегодной выставке RFID Journal в США, Орlando (2018), Las Vegas (2022) в номинации «Самое инновационное решение с применением RFID технологий». Наш комплекс входит в единый реестр отечественного программного обеспечения Министерства цифрового развития, а также зарегистрировано в странах Евразийского экономического союза.

Решение на базе АСУП «Цифровые активы» широко используются во многих отраслях, таких как промышленный сектор, нефтегазовый сектор, энергетический сектор, транспорт и авиация и других.

В большинстве предприятий управление товарно-материальными ценностями и автоматизация процессов технического обслуживания и ремонта ведётся на бумажных носителях, не имеет автоматизации или носит формальный характер.

Внедрение программного комплекса АСУП «Цифровые активы» позволит систематизировать и автоматизировать большинство процессов холдинга, минимизировать влияние человеческого фактора и сопутствующих ошибок на всех уровнях. Решение АСУП «Цифровые активы» позволит в короткие сроки повысить статус компании за счёт внедрения новых и современных технологий, организовать цифровизацию жизненного цикла активов компании, а также позволит выйти на один уровень автоматизации с мировыми гигантами. Система подобного уровня имеет высокий потенциал определить отраслевой стандарт между всеми подразделениями холдинга в части управления активами.

За счёт достоверности получаемой в системе информации комплекс позволяет автоматизировать мониторинг и планирование выполняемых работ собственными специалистами и сервисными компаниями, значительно увеличить производительность труда и повысить квали-

фикацию персонала. Своевременное обслуживание и ремонт оборудования позволит до 50% снизить затраты, связанные с простоем предприятия из-за аварийных и предаварийных ситуаций. Комплекс в целом существенно сократит общие производственные и сервисные расходы компании.

Программный комплекс АСУП «Цифровые активы» является универсальным для автоматизации процессов жизненного цикла активов предприятия. Единый центр принятия решения позволяет контролировать и управлять процессами с ситуационного центра предприятия, а различные варианты современных интерфейсов программного обеспечения, включая мобильную версию, позволит оперативно получать информацию всем ответственным лицам. Руководство предприятия получит мощный инструмент для принятия решений в части стратегического развития компании и её роста.

Предлагаемое программное обеспечение позволяет использовать любые цифровые идентификаторы для учёта товарно-материальных ценностей и активов предприятия, а гибкие интерфейсы интеграции позволяют подключить к системе любые датчики и контрольно-измерительные приборы.

Экономический эффект от внедрения системы «Цифровые активы»:

- увеличение межремонтных периодов на 10–20%;
- сокращение до 0 количества аварийных ситуаций и отказов оборудования и соответствующих расходов по их устранению;
- повышение эффективности персонала на 20–50%;
- сокращение складских запасов на 10–30%;
- сокращение затрат на ТОиР на 10–30%;
- увеличение сроков службы оборудования на 10% и, соответственно, сокращение капитальных затрат;
- увеличение скорости получения и эффективности обработки оперативной информации на всех контролируемых уровнях;
- оптимизация оперативного контроля у руководства;



Дмитрий Олейник
Коммерческий директор
Corporate Business Systems

- минимизация потерь на всех этапах логистической цепочки;
- сокращение расходов на эксплуатирующий персонал;
- минимизация издержек на оперативный учёт;
- обеспечение прозрачности управления;
- повышение статуса компании за счёт внедрения новых технологий;
- получение достоверной информации;
- наличие мобильного приложения;
- сокращение общих производственных расходов.

Мы готовы провести демонстрацию наших продуктов и показать все функциональные возможности программного комплекса.



Дмитрий Олейник
Коммерческий директор Corporate Business Systems

Моб.: +7- (925) – 800-55-65
doleynik@cbs-group.ru
cbs-group.ru

Электронная ПОДПИСЬ

Когда безопасность
дороже времени?



Валерия Валетина
Менеджер по работе
с корпоративными
клиентами
«Актив», Рутокен

Любое решение для обеспечения информационной безопасности не может быть одновременно максимально простым и максимально защищённым: чем-то приходится поступаться.

Вот, например, личный смартфон. Вряд ли информация на нём (контакты, файлы и фотографии) настолько интересна для посторонних людей, чтобы требовать использования сложных и дорогих способов защиты (со смартфонами знаменитостей дело обстоит совершенно иначе, но давайте трезво оценивать собственную значимость). К тому же большинство ставит удобство превыше всего и информацию в памяти смартфонов никак не защищает. Меньшинство обходится простой встроенной биометрией (лицо, рисунок, радужки глаз, отпечатки пальцев). А по-настоящему надёжный пароль устанавливает единицы (которым есть что терять).

Иная ситуация сложилась с дверными замками. Несмотря на то, что уже несколько лет существуют электронные устройства, которые издали узнают смартфон хозяина и сами распахивают перед ним дверь, все устанавливают старые добрые стальные замки с ключами (да не один, а даже два или три). Ключи неудобные и тяжёлые, их всюду нужно носить с собой, да ещё тратить время на открывание замка, но всё равно в данном случае безопасность важнее.

А как обстоит дело с электронной подписью, столь важным атрибутом современной цифровой среды? Технология это новая (по сравнению с используемой на протяжении веков обычной подписью на бумаге), для большинства непонятная и даже внушающая опасение. Поэтому в российском законодательстве установлены строгие требования к программному обеспечению, используемому для создания электронной подписи, аккредитованным удостоверяющим центрам, выдающим сертификаты ключей её проверки и так далее. Кроме того, для защиты электронной подписи российскими разработчиками были созданы USB-токены и смарт-карты с криптографическим ядром, позволяющие использовать неизвлекаемые ключи.

Что такое неизвлекаемые ключи электронной подписи и в чём их преимущества

Ключ электронной подписи – это числовая последовательность, никак не привязанная к своему владельцу, поэтому ключ очень просто скопировать. А любой, у кого есть ключ, может подписывать с его помощью электронные документы от имени и без ведома законного владельца. Единственный способ защитить ключ от копирования – обеспечить защищённое хранение. Для этого есть несколько способов:

1. Ключи помещаем в реестр или в файл, а защищаем встроенными средствами операционной системы. У этого способа два недостатка. Во-первых, недостаточная мобильность: чтобы подписать документы на другом ПК, ключ нужно будет копировать. А во-вторых, нужно будет очень хорошо защитить саму операционную систему. Ведь если злоумышленник подсмолит (или перехватит) пароль, то ничто не помешает ему завладеть ключом. Вывод: если на ПК используется двухфакторная аутентификация, то можно выбрать и такой способ, но лучше не стоит.
2. Ключи копируем на флэш-накопитель. Теперь подписывать можно с любого ПК, к которому подключена флэшка. Только вот сам накопитель никак не защищён. Его нужно хранить в сейфе, а компьютер, на котором происходит подписание, стоит проверять на наличие вирусов. Ведь какой-нибудь «троян» способен запросто украсть ключ. Вывод: флэш-накопитель – самый неудачный вариант, крайне не рекомендуется.
3. Ключи помещаем на специальный физический носитель – смарт-карту или USB-токен в защищённую область памяти. Для доступа к ключам необходимо ввести PIN-код. Для вычисления электронной подписи используется специальное программное обеспечение, установленное на ПК. Таким образом, каждый раз при подписании электронных документов ключ электронной подписи передаётся в память рабочего компьютера. Но существует программное обеспечение, позволяющее

злоумышленнику извлечь и скопировать ключ. Для этого нужно подсмотреть PIN-код и на время получить доступ к токenu.

4. Ключи электронной подписи создаются и хранятся в памяти криптографического токена, а значит, необходимость передавать ключи на ПК отпадает. Следовательно, такие ключи можно объявить неизвлекаемыми. Способа достать неизвлекаемый ключ из памяти токена (и скопировать его) не существует.

Фактически, использование активных криптографических средств электронной подписи (токенов и смарт-карт) – единственный по-настоящему надёжный способ защиты ключей электронной подписи от злоумышленников. Почему же он не используется в 100% случаев?

1. Токены с криптографическим процессором стоят немного дороже токенов без него. И уж, конечно, дороже обычных флэшек.
2. При выдаче ключей Удостоверяющие центры иногда рассказывают об опасностях, подстрекающих владельцев ключей, и о способах защиты. В результате пользователи зачастую выбирают более понятную им флэшку, чем совершенно неизвестный токен.

Виды электронной подписи: простая, усиленная и квалифицированная

Федеральный закон «Об электронной подписи» № 63-ФЗ говорит нам, что существует три вида электронной подписи:

- **простая**, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определённым лицом;
- **неквалифицированная**, полученная в результате криптографического преобразования информации с использованием ключа электронной подписи;
- **квалифицированная**, соответствующая всем признакам неквалифицированной электронной подписи, причём ключ проверки электронной подписи указан в квалифицированном сертификате (выданном

аккредитованным Удостоверяющим центром), а для создания и проверки используются сертифицированные средства.

Для непосвящённых звучит не совсем понятно, поэтому поясним попроще.

Простой подписью пользовался каждый из нас. Она применяется, например, в системах дистанционного банковского обслуживания, когда клиент банка пишет SMS для перевода денег или выполняет оплату в личном кабинете, предварительно введя пароль.

Плюс у простой подписи один (причём следующий из её названия) – простота реализации. А вот всё остальное – минусы. Дело в том, что поскольку у простой подписи нет единого вида и принципа формирования, то, с одной стороны, человеку бывает сложно осознать тот факт, что он что-то подписал, а с другой – владельцу подписанного документа бывает непросто доказать факт подписания. Обычно для этой цели используют журналы информационных систем, подтверждающие отправку SMS или аутентификацию пользователя.

Для использования простой подписи (как и для неквалифицированной) обязательно подписание регламента электронного документооборота, где (среди прочего) как раз и сказано, как будет проходить подписание и проверяться подпись. Составить правильный регламент не очень просто (особенно для простой подписи), юридические ошибки позволят оспорить факт подписания в суде. Именно поэтому для получения доступа к личному кабинету на сайте банка необходимо подписывать такие толстые соглашения.

Неквалифицированная подпись представляет собой цифровую последовательность, вычисленную с помощью специальных алгоритмов на основе исходного документа и ключей электронной подписи. Для проверки электронной подписи используется сертификат ключей её проверки. При этом участники электронного документооборота вольны выбирать, какие именно алгоритмы использовать, с помощью чего создавать ключи и сертификаты. То есть, в отличие от простой подписи, есть понятные

правила подписания и проверки, и главное – сторонам договориться и подписать регламент. Именно неквалифицированная подпись используется, например, в системах дистанционного банковского обслуживания юридических лиц.

Квалифицированная подпись во многом похожа на неквалифицированную, но есть два исключения. Во-первых, всё строго регламентировано. Криптографические алгоритмы – только ГОСТ. Программные и аппаратные средства криптографической защиты информации (СКЗИ) – только сертифицированные. Сертификаты проверки электронной подписи – только выданные аккредитованными государством Удостоверяющими центрами.

Но зато (и это, во-вторых) квалифицированная электронная подпись полностью аналогична (равнозначна) собственноручной на бумажном носителе и может использоваться без предварительного подписания соглашений и регламентов.

Но и в этой свободе есть минус. Если злоумышленник украдёт ключ квалифицированной электронной подписи, то сможет подписать всё, что захочет. Поэтому ключ и должен храниться на токене и быть неизвлекаемым.

Так что же делать? Где найти золотую середину между безопасностью и удобством? Давайте пройдемся по типичным задачам и выясним, насколько серьёзной должна быть защита в каждом конкретном случае.

Квалифицированная электронная подпись слишком ценна, а последствия кражи ключей слишком опасны, чтобы экономить на защите. Поэтому в данном случае рекомендовано использование активных криптографических ключевых носителей (токенов), генерирующих неизвлекаемые ключи.

Если Удостоверяющий центр не хочет такие ключи создавать (или выписывать сертификат на уже созданные) – идите в другой, безопасность тут дороже времени. Если программное обеспечение для подписи электронных документов не может работать напрямую с криптографическим токеном

(как, например, все токены линейки Рутокен ЭЦП), используйте криптопровайдер КриптоПро CSP 5, который умеет работать с неизвлекаемыми ключами.

Неквалифицированную электронную подпись зачастую используют не ради экономии (на поддержание собственного УЦ и выдачу сертификатов тоже тратятся ресурсы), а для того чтобы полностью контролировать процесс (например, выдавать сертификаты только проверенным контрагентам) и ради отсутствия ограничений (любое ПО, алгоритмы и пр.). К тому же необходимую для неквалифицированной электронной подписи инфраструктуру открытых ключей (PKI) можно использовать для двухфакторной аутентификации.

Итак, при выборе вида электронной подписи необходимо ответить на два главных вопроса: где хранить ключи и с помощью какого устройства подписывать. Ключи в реестре или файловой системе требуют усиленного контроля за тем, кто именно работает на ПК (что обычно решается с помощью двухфакторной аутентификации на основе токенов, но в чём же тогда экономия?), а также снижает мобильность пользователей, не позволяя им подписывать документы с любого компьютера.

Ключи на флэшках хранить можно только в том случае, если сама флэшка хранится в персональном сейфе, а во время работы владелец ни на секунду не спускает с неё глаз.

Токены были и остаются решением, специально созданным как для хранения ключей, так и для вычисления электронной подписи. Причиной их не повсеместного использования является, с одной стороны, цена (никто не любит платить за безопасность), а с другой – нежелание носить с собой и безопасно хранить ещё одну «штуковину». Кстати, те же самые токены можно использовать как для локальной, так и удалённой двухфакторной аутентификации.

Хранить ключи на смартфонах и использовать сами смартфоны для подписания можно, но только если вы уверены в отсутствии троянов и средств удалённого управления. Для персональных смартфо-



нов, используемых для множества задач с кучей установленных приложений, такое слабо достижимо (даже при наличии антивируса). Поэтому для таких целей лучше всего использовать отдельный аппарат, правда в этом случае затея становится экономически не особо привлекательной. Гораздо дешевле и удобнее для мобильной подписи использовать те же токены: как бесконтактные NFC и Bluetooth, так и контактные с интерфейсом USB Type-C. Они могут и ключи хранить, и электронную подпись вычислять вне смартфона.

При работе с **простой электронной подписью** автор рекомендует следующий подход: используйте её для работы с теми документами, оспаривание которых наименее ве-

роятно. Например, при кадровом документообороте сотрудники вполне могут подписывать простой подписью заявление на отпуск или отчёт о командировке. Проблемы у вас могут возникнуть разве что с налоговой, но они решаются с помощью грамотно составленных регламентов.

А вот подписание простой подписью заявлений на увольнение – это уже большой риск для работодателя. Потому что сегодня человек поставит галочку, что документ он подписал, а через месяц пойдёт в суд, заявляя, что ничего не подписывал и его незаконно не допускают на рабочее место. Если выиграет, то компания заплатит и компенсацию, и штраф.

В общем, всё, как обычно. Необходимо помнить, что из триады целей

«Дёшево – Удобно – Надёжно», достижимы только две. И не стоит верить на слово рекламе: всегда нужно проверять, насколько безопасно предлагаемое решение.

**КОМПАНИЯ
ПРАКТИВ**

*Валерия Валетина
Менеджер по работе с корпоративными
клиентами*

«Актив», Рутокен

www.rutoken.ru

Дистрибьютор программного обеспечения для бизнеса любого масштаба

MONT – один из крупнейших в России дистрибьюторов программного обеспечения. Группа компаний MONT начала свою деятельность в 1991 году и в настоящее время насчитывает более 5000 организаций в своей партнёрской сети, охватывающей всю территорию России.

КЛАССИЧЕСКАЯ ДИСТРИБУЦИЯ

Классическая дистрибуция MONT – способ доставки ПО от ведущих зарубежных и отечественных вендоров через физические поставки в виде корпоративных лицензий, «коробочных» продуктов и OEM-версий.



ЭКСПЕРТНЫЕ РЕШЕНИЯ

MONT помогает партнерам решать проблемы заказчика, не ограничиваясь выбором продукта. Мы поможем сократить расходы, повысить безопасность и эффективность ИТ-инфраструктуры и решить другие задачи.

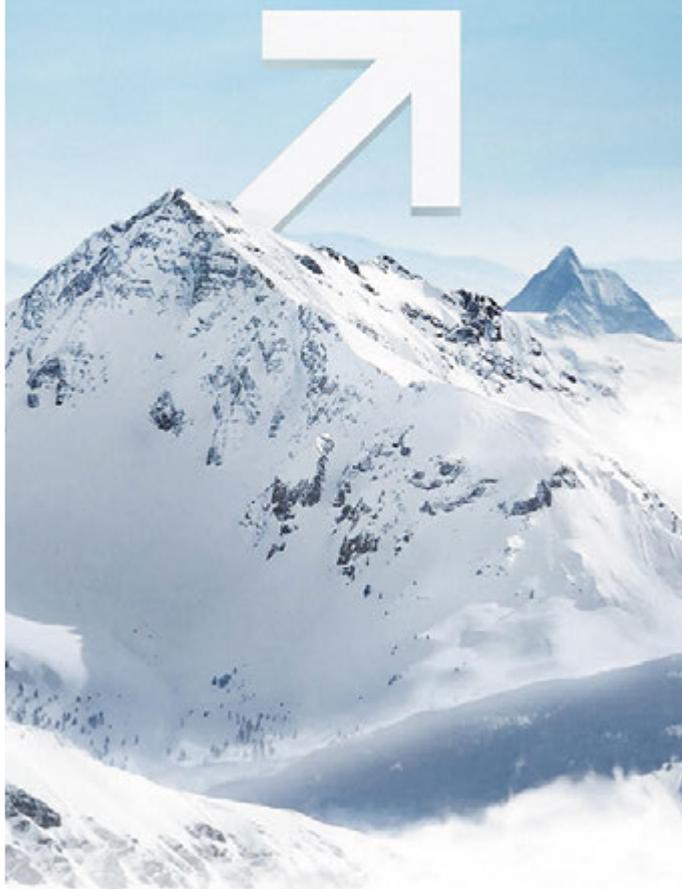


Сегодня MONT – это:

- Максимальный географический охват: присутствие в 20 городах, во всех федеральных округах России.
- 5000+ партнёров, среди которых есть и ведущие системные интеграторы со штатом в несколько тысяч сотрудников, и небольшие компании, в которых один человек часто выполняет функции и директора, и менеджера по закупкам, и розничного продавца. Мы стремимся обеспечить одинаково высокий уровень сервиса в работе со всеми партнёрами.
- Широкий продуктовый портфель, включающий как давно и хорошо известные программные продукты, так и решения от совсем молодых и перспективных игроков рынка.
- Экспертиза и консультации. Специалисты MONT оказывают профессиональную поддержку по самым разным вопросам: от подбора технического решения, расчета спецификации и правил лицензирования ПО до правовой поддержки.

ЭЛЕКТРОННАЯ ДИСТРИБУЦИЯ

MONT ESD (Electronic Software Distribution) – это канал для получения электронных ключей для программного обеспечения и цифрового контента напрямую от вендора в онлайн-режиме.



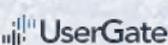
ОБЛАЧНАЯ ДИСТРИБУЦИЯ

MONT Cloud Distribution помогает партнёрам построить с нуля, трансформировать и автоматизировать бизнес по продаже ИТ-решений, поставляемых в виде облачных и подписных сервисов.



MONT является авторизованным дистрибьютором решений российских и зарубежных вендоров в сфере информационной безопасности, инфраструктуры, прикладного ПО, САПР и графики.

ПОРТФЕЛЬ ВЕНДОРОВ
ПО ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

		Категория	Антивирусы	NGFW и UTM	WAF	Защита от DDoS атак	Защита почты	Sandbox	NTA	Сканер уязвимостей	DLP	СЗ от НСД и МФА	СКЗИ	Privileged Access Management	Анализ исходного кода на уязвимости	Защита файловых хранилищ	SIEM	SOAR	XDR	Защита от кибермошенничества	Защита АСУ ТП	Защита облачных и виртуальных сред	Обучение персонала защите от киберугроз	
		Вендор																						
	ANY.RUN							+																
	Check Point	+	+	+	+	+	+	+			+	+	+		+	+				+	+	+	+	+
	Group-IB						+	+	+							+			+	+			+	
	InfoWatch										+				+							+		
	Mitigator				+																			
	Phishman																							+
	Positive Technologies			+		+	+	+	+	+					+	+			+	+	+			
	Pro32	+																						
	ruSIEM																+							
	R-Vision																	+		+				
	SkyDNS																							
	StaffCop										+													
	UserGate		+			+											+	+	+		+			
	Zecurion										+				+									
	Айдеко		+	+																				
	Актив (Рутокен)										+													
	Аладдин Р.Д.										+	+	+		+									
	АЛТЭК-СФОТ (RedCheck)									+														
	ГазИнформСервис										+	+									+			

С полным перечнем вендоров MONT можно ознакомиться по ссылке mont.ru/ru-ru/vendors



Категория		Антивирусы	NGFW и UTM	WAF	Защита от DDoS атак	Защита почты	Sandbox	NTA	Сканнер уязвимостей	DLP	СЗ от НСД и МФА	СКЗИ	Privileged Access Management	Анализ исходного кода на уязвимости	Защита файловых хранилищ	SIEM	SOAR	XDR	Защита от кибермошенничества	Защита АСУ ТП	Защита облачных и виртуальных сред	Обучение персонала защите от киберугроз
Вендор																						
	Доктор Веб	+				+	+															
	Интернет Контроль Сервер		+																			
	Киберпротект									+												
	Код Безопасности		+	+									+	+								+
	Компания Индид												+	+								
	КриптоПро												+	+								
	Лаборатория Касперского	+			+	+	+	+							+	+		+	+	+	+	+
	НТБ (SafeInspect)													+								
	Ростелеком-Солар				+	+		+	+	+	+			+	+							+
	Сакура																					
	Смарт-Софт (Traffic Inspector)		+																			
	Стахановец									+												
	С-Терра												+									
	Фактор-ТС		+										+									
	Цифровые технологии (КриптоАРМ)												+									
	Эшелон	+							+					+	+							



Обратитесь к своему ИТ-поставщику, если вас заинтересовало какое-либо из решений, предлагаемых MONT. Либо оставьте заявку на www.mir.mont.com, и мы обязательно свяжемся с вами.

Если ваш бизнес связан с поставкой/продажей лицензионного программного обеспечения

конечным пользователям (организациям или физическим лицам), станьте нашим партнёром www.mont.ru/ru-ru/becomeapartner, чтобы полностью удовлетворять спрос ваших клиентов.

www.t.me/komandamont
www.vk.com/komandamont



«Работы ещё много»: на AntiFraud Russia подвели итоги борьбы с мошенничеством в 2022 году

В Москве успешно прошёл XIII Национальный форум AntiFraud Russia, организованный Академией Информационных Систем – ведущим учебным центром по ИБ, ИТ, ЭДО, экономической безопасности и конкурентной разведке.

Форум традиционно стал площадкой, где представители профильных ведомств и регуляторов, а также лидеры рынка кибербезопасности и телекома подвели итоги года в сфере борьбы с мошенничеством, обратили внимание на важные тренды и рассказали о планах на будущий год.

Открыл мероприятие вице-президент ГК «Цитадель» **Борис Мирошников**, который также является председателем оргкомитета AntiFraud Russia с момента его основания.

«Много лет назад, когда мы с директором АИС Юрием Малинымым затевали AntiFraud Russia, мы думали: «Вот

победим мошенников и заживём спокойной жизнью». Так вот работы у нас ещё много – технический прогресс идёт вперёд. К сожалению, он не только создаёт для всех удобства пользоваться технологиями, но и представляет возможность преступному миру совершенствовать свои преступные навыки», – сказал вице-президент в своей вступительной речи.

Г-н Мирошников обратил внимание, что среди участников форума стало больше новых участников. В подтверждение этого тезиса сразу после него на сцену вышел представитель законодательной ветви власти сенатор **Артём Шейкин**, который вошёл в состав Совета Федерации только в прошлом году.

Парламентарий активно участвует в разработке законодательных инициатив в области кибербезопасности. По его словам, решение этой проблемы стало бы **«реальной помощью гражданам»** страны.

Он рассказал о ряде принятых и готовящихся к принятию законопроектов в области борьбы с мошенничеством,

в том числе об инициативе, которая **внесёт изменения в ФЗ «О связи»**. Главное задачей документа станет борьба с подменой номеров. Он предусматривает ответственность для операторов и вводит обязанность предоставлять в Минцифры сведения, необходимые для установления всей цепочки операторов связи, участвующих в соединении и непосредственного оператора связи, подтвердившего номер.

«Именно установление такой цепочки и нахождение оператора-нарушителя занимает значительную часть времени у правоохранительных органов, потому что порой таких операторов связи может быть больше семи, – объяснил сенатор Шейкин. – Когда мы ускорим получение этой информации, количество дел, раскрываемых МВД, станет значительно выше».

Телефонное мошенничество

Подробнее о телефонном фроде и истории борьбы с ним в 2022 году рассказал директор Департамента обеспечения кибербезопасности Минцифры России **Владимир Бенгин**. По его словам, общими усилиями регуляторов,

правоохранительных органов и операторов связи, которые в этом году **начали «беспрецедентную кооперацию»**, удалось значительно снизить количество звонков мошенников россиянам.

После 24 февраля количество телефонного фрода в России рухнула так сильно, что, как признался главный эксперт «Лаборатории Касперского» **Сергей Голованов**, многие аналитики фрода опасались остаться без работы.

Владимир Бенгин объяснил, что кроме технических сложностей телефонные мошенники, работавшие из-за рубежа, были вынуждены перестраивать схемы по выводу украденных у россиян средств. На всё это понадобилось время, но уже к концу весны они возобновили свою работу, а к июлю показатели, в разы превышавшие прошлогодние, уже **достигали исторического пика**.

«К концу лета у нас появились методы, с помощью которых можно снизить объём вызовов мошенников, поступающий на телефоны граждан. И с конца августа началось падение таких вызовов», – сообщил представитель Минцифры.

Уже к октябрю статистика по числу звонков мошенников **вернулась к значениям за аналогичный период 2021 года**, рассказал г-н Бенгин и подтвердили другие участники пленарного заседания AntiFraud Russia.

Ведомству также удалось почти полностью исключить звонки на номера с **домашним кодом «495» или «499»**. Если раньше на них приходилось порядка 80%, то сегодня – всего 10%.

Новые вызовы

Впрочем, даже если удастся полностью исключить телефонное мошенничество



через операторов и подмену номера, оно просто **перетечёт в мессенджеры**.

«Злоумышленники в массовом порядке переключаются на мессенджеры. Проблема в том, что на современных телефонах, особенно фирмы Apple, человек почти не может отличить вызов через Viber или WhatsApp от вызова с обычных телефонных сетей», – пояснил Владимир Бенгин.

На мессенджеры приходится уже порядка 30% телефонного фрода

В качестве одной из мер борьбы с «новым вызовом» представитель Минцифры призвал повышать осведомлённость граждан об этой схеме и **«продвигать историю с недоверием к вызовам с чужих номеров с мессенджера»**. Особенное внимание он уделил информационным кампаниям банков, отметив, что им такая коммуникация удаётся лучше всего.

Впрочем, фрод через мессенджеры прекратить куда проще, чем через сотовую связь, ведь, как правило, приложения позволяют в два клика запретить любые вызовы с неизвестных номеров.

Банковский фрод

Как противодействовать мошенничеству с банковскими картами и счётами россиян, на AntiFraud Russia рассказал директор Департамента информационной безопасности Банка России **Вадим Уваров**.

Он сообщил, что **средний чек хищения** с 2019 года вырос на 30% и сейчас составляет **14,5 тысячи рублей**, а только за 9 месяцев 2022 года мошенники уже похитили у россиян около 10 млрд рублей.

«Киберпреступность – проблема не отдельно взятого государства. Ущерб от него носит глобальный масштаб. Россия, по данным MasterCard, не входит в число стран-лидеров по уровню мошенничества в мире. Показатель доли объёма операций клиентов в общем объёме операций по переводу денежных средств в России существенно меньше общемирового в целом и по Европе в частности», – добавил представитель Банка России.

За последние три года, по данным ЦБ, наблюдается рост как объёма, так и числа мошеннических операций с согласия клиентов. Объём хищений вырос почти на 39%, а число операций без согласия клиентов – на 34%.

«Тема противодействия фроду для нас является одной из наиболее значимых и актуальных», – сказал представитель регулятора, указав на работу, которая ведётся в этом направлении.

В первую очередь, **г-н Уваров** указал на уже утверждённую инициативу ЦБ по **взаимодействию с МВД России**. После полного вступления в силу 21 октября 2023 года мера позволит МВД оперативно получать информацию, что позволит уменьшить сроки раскрытия преступлений. При этом, подчеркнул





представитель регулятора, передача данных в МВД **«будет происходить с соблюдением банковской тайны».**

Кроме того, благодаря оперативному **взаимодействию ЦБ с Генеральной прокуратурой** существенно выросло число заблокированных мошеннических ресурсов: если в 2021 году речь шла о 180 тысячах, то в 2022 году их уже **500 тысяч**, включая 1600 страниц в соцсетях.

«Ключевым фактором в такой работе является скорость, – пояснил Вадим Уваров. – Чем быстрее мы блокируем инструменты мошенников, тем меньшее количество людей страдает от их действий».

Возврат средств

Другое важное направление работы ЦБ – возврат похищенных средств. Сейчас их доля едва превышает 3%, но регулятор намерен исправить ситуацию, в том числе с помощью нового законопроекта, который согласован с бизнесом, Генпрокуратурой и МВД и уже готовится к внесению на рассмотрение Государственной Думой.

Новый механизм порядка возврата денежных средств, как объяснил Вадим Уваров, заключается в том, что информация будет направляться не только банкам-получателям, но и банкам-отправителям, которые обязаны будут учитывать это в своих бизнес-процессах.

Если банк будет видеть, что средства переводятся на счёт мошенников и пропустит их, то его обяжут **вернуть их жертве в полном объёме.**

Также ЦБ последовательно продвигает идею с введением **периода охлаждения**, позволяющий гражданам обдумать

необходимость перевода, если они стали жертвами социальной инженерии, доля атак, по словам **сенатора Шейкина**, с помощью которой по России достигает 25%, а в Москве, Московской области и в Санкт-Петербурге – 40%.

Борьба с дропперами

Летом этого года Банк России подготовил рекомендации об отключении электронного средства платежа на стороне банков-получателей при выявлении рисков. Как рассказал **Вадим Уваров**, последние 3,5 месяца регулятор проводил анализ действия этой меры, на основании которого предлагает **сделать её обязательной** при получении банками соответствующей информации от МВД России.

Из общего числа случаев, по которым проводилось исследование, примерно в 320 тысячах была произведена приостановка его использования и **только в половине случаев банки получили обращение от клиентов** о возобновлении действий электронного средства платежа (ЭСП).

При этом более чем по 33 тысячам ЭСП банками было приостановлено его действие на основании выявленного риска и не принято обоснованного решения о возможности возобновления его использования. Сумма среднесреднедневных остатков на банковских счетах таких ЭСП составила почти 846 млн рублей.

Ландшафт киберугроз и итоги года

В ходе пленарного заседания своими наблюдениями по вопросу кибербезопасности поделились главный эксперт «Лаборатории Касперского» **Сергей Голованов** и руководитель

Департамента по противодействию мошенничеству компании «Инфосистемы Джет» **Алексей Сизов**.

Анализ статистики числа мошеннических операций в этом году показал, что если телефонные мошенники, как правило, находятся за рубежом, то **«мошенники в интернете – отечественные»**, сказал Сергей Голованов. По данным «Лаборатории Касперского», несмотря на все события, почти не изменились показатели, связанные с фродом на сайтах: кликфрод, незаконное копирование контента и прочее.

При этом объёмы телефонного мошенничества и число мошеннических объявлений после 24 февраля резко упало, а в случае с объявлениями до сих пор остаётся близким к нулю.

Тем временем Алексей Сизов обратил внимание, что **настройка систем антифрода** для борьбы с социальной инженерией двух-трёхлетней давности не перестала работать. В неё оказалось достаточно внести незначительные корректировки, чтобы они продолжили «ловить» потенциальные новые схемы.

«За последние 2 года требования по информационной безопасности, по логированию, по двухфакторной аутентификации стали настолько тривиальными, что их стали воспринимать как неизбежность. Компании, которые смогли сделать то же самое с точки зрения антифрода, за последний год практически не сталкивались с проблемами», – добавил он.

Эксперт также отметил, что попытка **«научить» клиентов банков** защищать свои данные оказалась провальной. Г-н Сизов уверен, что самым эффективным механизмом здесь были бы практические учения, которые, впрочем, сложно реализовать в случае с рядовыми пользователями.

Следующий форум AntiFraud Russia планируется на весну 2023 года. Чтобы обсудить подробности участия в мероприятии, свяжитесь с организаторами.



**АКАДЕМИЯ
ИНФОРМАЦИОННЫХ
СИСТЕМ**

www.infosystems.ru
www.vipforum.ru



Тренды развития бизнеса в России за последние полгода обсудили на TECH WEEK

В Сколково состоялась восьмая конференция об инновационных технологиях для бизнеса

Более 2300 представителей российских компаний объединила конференция об инновационных технологиях TECH WEEK. В масштабном событии приняли участие более 300 признанных экспертов бизнеса – спикеры, менторы, модераторы стали ведущими 14 тематических потоков. Программа одного из потоков проходила онлайн. В этом блоке выступили 20 лидеров мнений из России, Турции, Армении, Грузии, Казахстана, Киргизии, США, Швейцарии и Таиланда.

В выставке инновационных технологических цифровые решения для компаний представили 100 сервисов. Девелопер «Самолёт» презентовал несколько модулей своей цифровой системы: аналитика строительства и контроль.

«Миссия наших цифровых продуктов – сделать путь от выбора площадки для строительства до сдачи объекта в эксплуатацию максимально прозрачным, контролируемым и предсказуемым,

чтобы мы могли сэкономить ресурсы, время и сделать качественный продукт», – считают в компании.

В числе экспонентов также выступили компании по обеспечению кибербезопасности, автоматизации менеджмента, подбору и развитию персонала и разработчики других технологических инновационных решений.

Традиционно программу дополнили специальными мероприятиями для предпринимателей («Менторская гостиная», HR-консультации, Мастер-майнд, Практикум, Education day), программами нетворкинга для бизнес-знакомств (Speed networking, Random coffee, TECH-баня и AfterParty при участии солистки российского рейв-проекта Dead Blonde Арины Булановой).

«Мы проводим конференцию TECH WEEK каждые полгода. Событие зарекомендовало себя как неформальная площадка коммуникаций лидеров российского бизнеса и коллег из других стран. За несколько лет, что мы проводим TECH WEEK, нам удалось создать профессиональное бизнес-комьюнити – мероприятие помогает предпринимателям

адаптироваться к текущей новостной повестке, найти технические решения для бизнес-задач, нужных подрядчиков и партнёров, а также тестировать последние цифровые разработки и сервисы», – рассказала о программе продюсер события Наталья Бардина.

По словам директора по развитию бизнеса **Novo BI** Павла Сеницына, сегодня выигрывает бизнес, который умеет адаптироваться под повестку дня. Справиться с этой задачей помогают технологии. На TECH WEEK директор по планированию и управлению товарными запасами **ALIDI** Дмитрий Фризен поделился результатами работы с Novo Forecast Enterprise. За год использования цифровой системы оборотный капитал дистрибьютора снизился более чем на 1 млрд рублей. Помимо этого, за несколько лет компании удалось повысить точность прогнозов с 40% до 85%, а с марта 2022 точность спроса – не ниже 78%. Также **ALIDI** сэкономила 20% на фонде оплаты труда сотрудников отдела заказов и в несколько раз повысила эффективность их работы. Кроме того, цифровизация прогнозирования спроса



позволяет раз в сутки перестроить сценарий работы и операции по цепочке поставок.

Ещё один актуальный тренд – развитие метавселенной. По мнению основателя RTVI и основателя ЦИПР Ольги Пивень, мета сегодня открывает новый уровень коммуникации с аудиторией.

«Совершенно разные сферы – бизнес, госструктура, здравоохранение, медиа – интегрируются в пространство виртуальной реальности. Если ранее ключевыми инвесторами были энтузиасты, сейчас в мета вкладывают крупные игроки. В ближайшем будущем мета может стать самостоятельной площадкой для производства контента и его дистрибуции», – прокомментировала во время своего выступления Ольга Пивень.

В рамках деловой программы в тематическом потоке AI & BIG DATA выступил вице-президент по развитию бизнеса и GR **Westlink Group** Олег Попов. Он презентовал возможности отечественной разработки – интеллектуальной платформы Linkage Navigator, рассказал о прикладном применении

искусственного интеллекта в управлении бизнес-процессами организации, о том, как инсайты и сторителлинг, предоставляемые в режиме реального времени, способны улучшить показатели работы бизнеса.

«На TECH WEEK мы представили нашу разработку – Linkage Navigator. Это система для управления большими данными компании с использованием предиктивного анализа, машинного обучения и искусственного интеллекта. Система комплексно подходит к решению задач по повышению эффективности работы персонала. Платформа использует инструменты ИИ и машинного обучения поверх получаемых из разных источников неструктурированных данных, собирает их в единый Data lake и анализирует. Система предоставляет расширенную аналитику посредством онлайн-инсайтов (цифры, действия и пр.) и сторителлинга, что позволяет принимать оптимальные бизнес-решения на всех уровнях бизнеса», – отметил Олег Попов.

Основатель и CEO **«Цифровой HR-платформы»** Дмитрий Серебряков представил на TECH WEEK про-

ект, который глобально трансформирует процессы по взаимодействию с внештатным линейным персоналом в ряде отраслей бизнеса: ритейл, логистика, строительство, клининг, складские услуги, HoReCa и другие.

«Платформа полностью автоматизирует и оптимизирует все HR и финансовые процессы по взаимодействию с самозанятыми с применением алгоритмов искусственного интеллекта и машинного обучения. Сервис переводит на новый уровень не только работу отдельных подразделений – HR, бухгалтерии, службы безопасности, рекрутеров, но и всего бизнеса в целом: помогает ему укреплять свои позиции на рынке и расти даже в непростой экономической ситуации», – прокомментировал Дмитрий Серебряков.

В рамках EdTech-секции состоялась панельная дискуссия «Как меняется EdTech в сегменте ДПО». Лидеры рынка EdTech рассказали о том, как изменились их продуктовые и маркетинговые стратегии в 2022 году. Партнёром и организатором секции выступил образовательный холдинг **Ultimate Education**. Модератор: Павел



Мосейкин, CEO, со-основатель **XYZ School**. Спикеры: Марианна Снигирёва, CEO **Нетологии**; Артём Казаков, коммерческий директор **Skillbox**; Дарья Рыжкова, основательница **Smart Ranking**; Илья Курмышев, CEO **Яндекс Практикум**; Александр Шестопалов, директор по маркетингу **BBE Bang Bang Education**, Мария Данина, со-основательница **«Психодемии»**; Александр Журавлёв, со-основатель **Moscow Digital School**; Татьяна Дьяконова, CEO **Fashion Factory School**.

Вопреки пессимистичным прогнозам EdTech-рынок в третьем квартале снова показал положительную динамику. По мнению **Дарьи Рыжковой, основательницы Smart Ranking**, в целом сфера в третьем квартале восстановилась до показателей начала года. По мнению аналитиков, частичная мобилизация, кажется, не нанесла российскому эдтеху серьёзного урона и будет иметь незначительный эффект на показатели четвёртого квартала, который традиционно является лучшим периодом. Лучшую динамику на рынке в этом году показывает сегмент дополнительного профессионального образования: он аккумули-

ровал во втором квартале 38,5% выручки ТОП-100 компаний отрасли.

В потоке MANAGEMENT деловой программы Александра Герасимова, CEO FITMOST, рассказала, как перестроить стратегию в кризис на примере компании: *«В 2022 году мы переработали стратегию: изначально думали над федеральным масштабированием, но, оценив ситуацию, выбрали запуск проекта на международном рынке параллельно с развитием бизнеса в России. Мы меняемся, сохраняя наши ценности: это позволило нам пройти пандемию, это помогает нам сохранить устойчивость и сейчас».*

Гости TECH WEEK также приняли участие в специальных мероприятиях для бизнеса, получив комментарии по развитию от менторов, HR-консультантов, в рамках Практикума и Education day. В новом спецпроекте TECH-баня, впервые стартовавшем на летней конференции приняли участие 55 гостей.

В завершении каждого дня конференции в онлайн-потоке с гостями работали бизнес-психологи: Ирина Германова,

директор дополнительного профессионального образования работников социальной сферы Москвы; Светлана Хамаганова, executive-коуч, стресс-коуч Центра осознанного лидерства. А прямо на площадке конференции были организованы зоны отдыха и расслабления с гамаками и музыкальными инструментами: гонгом, поющими чашами, варганом. Компания Yamaguchi организовала зону восстановления с массажными креслами.

Гостьей Afterparty стала солистка российского рейв-проекта **Dead Blonde** Арина Буланова. Девушка получила популярность благодаря загруженным в TikTok другим пользователем песням «Мальчик на девятке» и «Бесприданное». Неформальное завершение конференции состоялось в клубе GIPSY на набережной Москвы.



techweek.moscow



XI торжественная церемония награждения «ComNews Awards 2022»

2 декабря 2022 г. в Москве состоялась торжественная церемония награждения лидеров рынка «ComNews Awards. Лучшие решения для цифровой экономики».

В этом году вручение ежегодной премии ComNews Awards состоялось в 11 раз.

Мероприятие поддержали отраслевые Союзы и Ассоциации: АНО «Цифровая экономика», АНО «Национальные приоритеты», Проект «Цифровая экономика», Национальная Ассоциация Участников Рынка Робототехники (НАУРР), Ассоциация «Цифровая энергетика», Ассоциация интернета вещей, Ассоциация профессионалов управления бизнес-процессами (ABPMР Russian Chapter), НП РУССОФТ, Союз участников рынка картофеля и овощей, Ассоциация по развитию цифровых технологий

транспорта «Цифровая Эра Транспорта», Ассоциация участников отрасли центров обработки данных (ЦОД), Ассоциация больших данных и Ассоциация разработчиков программных продуктов «Отечественный софт».

На конкурс было подано более 350 заявок, а после их тщательного изучения в шорт-лист вошли 70. Церемония состояла из четырёх смысловых блоков.

Первый блок номинаций посвящён проектам в ключевых отраслях экономики, или на вертикальных рынках. В этом блоке номинаций были выделены лучшие проекты в таких отраслях как: государственный сектор, транспорт и логистика, сельское хозяйство, финансы, здравоохранение, образование, топливно-энергетический комплекс, промышленность и экология.

Уход с рынка зарубежных игроков стал серьёзным вызовом для мно-

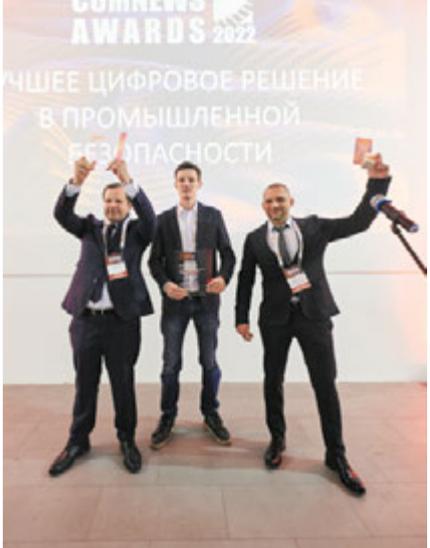
гих отраслей. С другой стороны, это открыло возможности для российских компаний занять освободившиеся ниши. Второй блок номинаций «Цифровая независимость» посвящён лучшим решениям и разработкам, которые уже сейчас помогают обеспечивать импортонезависимость России в условиях санкций.

Некоторое количество заявленных на конкурс проектов оказались шире, чем основной пул номинаций. При этом среди них были и уникальные решения, поэтому был добавлен третий блок – «Фокусные номинации».

В четвёртом блоке «Цифровые лидеры России» жюри отметило профессиональных специалистов и управленцев, которые решают задачи по реализации проектов в цифровизации ключевых отраслей экономики и общественной жизни.

#comnewsawards
#comnewsawards2022

ЛУЧШЕЕ ЦИФРОВОЕ РЕШЕНИЕ
В ПРОМЫШЛЕННОЙ
БЕЗОПАСНОСТИ



Цифровая трансформация в горной добыче, металлургии, энергетике и нефтегазовой отрасли – 2022

С 6 по 8 декабря 2022 года в Челябинске на площадке отеля «Рэдиссон Блу Челябинск» прошёл Седьмой международный форум «SEYMARTEC DIGITAL. Цифровая трансформация в горной добыче, металлургии, энергетике и нефтегазовой отрасли – 2022».

Мероприятие было открыто генеральным директором ООО «Сеймартек» Сеитовым Маратом Мухамбеткалиевичем.

«По традиции местом проведения стал Челябинск – город с большой производственной историей, являющийся местом сосредоточения крупнейших металлургических и добывающих предприятий.

Данное мероприятие является регулярным и проводится ежегодно. В 2021 году основной идеей мероприятия стал обмен производственным межотраслевым опытом. Нынешнее мероприятие проходит на фоне новых вызовов, а геополитические события оказывают самое прямое воздействие на нашу действительность. Сегодня многие программы технологического развития, заложенные в «далёких» 2010-х годах и 2021 году, претерпевают существенные изменения. При этом устойчивость российского промышленного бизнеса, пережившего не одну волну кризиса, не вызывает сомнений. Сегодня мы – компания «Сеймартек» – видим свою значительную роль в консолидации отрасли и возможности обеспечить существенные каналы для общения, что позволит не просто обмениваться мнением о дальнейших производственных задачах, но и быстрее реагировать на меняющуюся обстановку и быть адекватным в условиях неопределённости сегодняшнего дня.», – сообщил Марат и пожелал плодотворной работы участникам форума.

Мероприятие проходило 3 дня в 2-х параллельных залах, в которых выступило более 80 спикеров со всех уголков страны и ближнего зарубежья.

По традиции мероприятие открывалось общей стратегической сессией, лейтмотивом в которой, безусловно, стала тематика импортозамещения в промышленности. Компании «Евраз», «СУЭК», Datana, «Газпромнефть» и «Уралхим» выступили со своим видением в решении этих острейших на сегодняшний день вопросов.

В первый день мероприятия также работали следующие секции в программе:

- «Импортозамещение и цифровая стратегия холдингов. Обмен практиками работы с вызовами».
- Инструменты цифровой трансформации. Отечественные ИТ-платформы и CRM-системы.
- Облачные, серверные, инфраструктурные решения и системы
- Инструменты цифровой трансформации. Крупные проекты импортозамещения.
- Управление безопасностью, ремонтами и техническим состоянием.

Программа первого дня завершилась деловым ужином.

Во второй день работали следующие секции:

- Системы управления производством
- Цифровой двойник. Предиктивная аналитика, диагностика и прогнозирование.
- Технологии автоматизации процессов.
- MES, ERP, SCADA. Системы управления производственными процессами и ремонтами
- Автоматизированная информационная система «Безопасность производственной деятельности».

И последний – третий день полностью был посвящён тематике «Цифрового

ГОКа», модерировал программу Опалев Александр Сергеевич, заместитель директора по научной работе Горного института КНЦ РАН, к. т. н.

Компания выражает благодарность и остальным модераторам:

- Фимушину Андрею Викторовичу, руководителю направления, Дирекция по цифровизации производства, Группа «НЛМК»;
- Жаворонкину Олегу Валерьевичу, заместителю генерального директора компании «АТОЛЛис»;
- Артёму Сергеевичу Цыганку, руководителю департамента маркетинга и продаж «КОНСОМ ГРУПП»;
- Рамш Александру Станиславовичу, Управляющему партнёру компании DEX Consulting;
- Савину Андрею Валерьевичу, Директору по информационным технологиям Дивизиона Урал в ООО «ЕВРАЗ»;
- Паршикову Александру Юрьевичу, начальнику департамента технологической роботизации и трёхмерной печати, «Газпромнефть – ЦР»;
- Столярову Михаилу Михайловичу, руководителю группы проектов «НОРНИКЕЛЬ-Спутник»;
- Каплану Алексею Владимировичу, заместителю генерального директора, ООО «НТЦ-Геотехнология»;
- Наговицыну Олегу Владимировичу, заместителю директора по научной работе, ФИЦ «Кольский научный центр РАН».

Всего мероприятие посетило более 250 участников, заслушаны более 80 докладов.



СЕЙМАРТЕК

seymartec.ru





CDO/CDTO SUMMIT & AWARD

Осенняя сессия III Российского Саммита по цифровой трансформации организаций и Премия CDO/CDTO Award 2022

17 ноября 2022 года состоялась осенняя сессия III Российского Саммита по цифровой трансформации организаций, на которой были награждены лауреаты премии CDO/CDTO Award 2022.

Руководители по ИТ, цифровой трансформации и информационной безопасности Ростелекома, Росатома, X5 Group, Rostest Digital, ВШЭ и другие поделились мнениями о переходе на отечественное ПО и об актуальных трендах в области цифровизации.

Особым гостем Саммита стал известный российский учёный, специалист в области информационных технологий, системного анализа, искусствен-

ного интеллекта, кибербезопасности, вычислительных и телекоммуникационных систем, академик Российской академии наук Игорь Анатольевич Шеремет. Академик рассказал о ресурсно-технологической устойчивости и независимости социотехнических систем.

17 ноября в рамках Осенней сессии III Российского Саммита CDO/CDTO состоялась церемония вручения Премии в области цифровой трансформации организаций CDO/CDTO Award 2022.

В номинации «Лучшая DLP-система (Безопасность данных)» обладателем Гран-При стала компания «**Ростелеком-Солар**», система Solar Dozor.

В номинации «Лучший проект по импортозамещению» Гран-При члены

Жюри присудили **Госкорпорации «Росатом»**.

«Проектом года по цифровизации регионов» была названа разработка проектной команды **Rostest Digital** «Цифровая Экосистема ЦСМ Росстандарта».

Обладателем Гран-При в номинации «Лучший проект по укреплению информационной безопасности в госсекторе/регионах» стала «**Федеральная дирекция спортмероприятий**».

В номинации «Компания с лучшей Digital-культурой» Премия была вручена в нескольких отраслях: финансовые услуги, ритейл, телеком и финтех. Обладателями Гран-При в данной номинации стали: в отрасли финансовых услуг – **АО «НПФ «Открытие»**, в отрасли ритейла – **X5 Group**, в от-



расли телекома – **Ростелеком Информационные Технологии**, в отрасли финтеха – **Группа Qiwi**.

В номинации «Руководитель года по информационной безопасности» обладателями Гран-При стали: **Александр Владимирович Марков**, директор департамента информационной безопасности, X5 Group (в отрасли ритейла) и **Илья Владимирович Сулоев**, вице-президент, директор департамента информационной безопасности, ПАО Банк «ФК Открытие» (в банковском секторе);

Премия в номинации «CDO/CDTO года» была также вручена в двух отраслях. Титул «CDO/ CDTO года в банковском секторе» получил **Вадим Валерьевич Кулик**, заместитель президента-председателя правления, БАНК ВТБ (ПАО). Титул «ODO/

CDTO года в отрасли ИТ» получил **Игорь Васильевич Мнев**, руководитель «Центра продвижения цифровых сервисов и услуг» (Rostest Digital).

В номинации «CEO года цифровой компании» обладателями Гран-При стали **Андрей Михайлович Протопопов**, CEO группы QIWI (в отрасли финтеха) и **Сергей Юрьевич Беляков**, управляющий директор Ozon (в отрасли электронной коммерции).

Премия CDO/CDTO AWARD 2022 была вручена также Академику **Игорю Анатольевичу Шеремету** за вклад в технологическое развитие страны.

Поздравляем всех лауреатов Премии! Ждём всех в следующем году!

Организовано НИУ ВШЭ и компанией LBS International Conferences.

LBS INTERNATIONAL CONFERENCES



ОРГКОМИТЕТ III CDO/CDTO SUMMIT & AWARD 2022

Москва, Покровка, 43, стр. 2

Тел.: +7 (495) 926-78-70

cdosummit.ru

cdo@cdosummit.ru



Центральный российский форум по информационной безопасности «Инфофорум-2023»

7–8 февраля 2023 года в здании Правительства Москвы на Новом Арбате, 36 прошёл центральный отраслевой форум в сфере информационной безопасности Большой Национальный форум информационной безопасности «Инфофорум-2023».

Большой Инфофорум проводился уже в 25-й раз. В его работе в офлайн формате за 2 дня приняли участие более 1300 делегатов, зафиксировано более 3000 тысяч подключений к трансляции заседаний в режиме онлайн. Среди участников Инфофорума-2023 были руководители и представители регу-

лирующих органов отрасли информационной безопасности, федеральных и региональных органов власти, ведущих российских ИТ-компаний, образовательных и научных центров, промышленных корпораций, телеоператоров, известные эксперты.

Организаторы Инфофорума-2023: Комитет государственной Думы по безопасности и противодействию коррупции, Аппарат Совета Безопасности Российской Федерации, Ассоциация Национальный форум информационной безопасности «Инфофорум». Форум проходил при поддержке и участии ФСБ России, ФСТЭК России, Минцифры России, Минобороны России, Банка России, Минэкономразвития России и ряда других федеральных министерств и ведомств.

В работе пленарного заседания и тематических заседаний Инфофорума-2023 приняли участие и выступили: **Эрнест Валеев** – депутат Государственной Думы, заместитель председателя комитета Государственной Думы по безопасности и противодействию коррупции; **Александр Шойтов** – заместитель Министра цифрового развития, связи и массовых коммуникаций Российской Федерации; **Евгений Хасин** – заместитель директора Департамента обеспечения кибербезопасности Минцифры России; **Сергей Катырин** – президент Торгово-промышленной палаты Российской Федерации; **Сергей Бойко** – начальник департамента проблем безопасности в информационной сфере аппарата Совета Безопасности Российской Федерации; **Николай Мурашов** – заместитель директора Нацио-

нального координационного центра по компьютерным инцидентам; **Андрей Крутских** – специальный представитель Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности МИД России; **Артём Шейкин** – член комитета Совета Федерации по конституционному законодательству и государственному строительству; **Игорь Панышин** – заместитель полномочного представителя Президента РФ в Центральном федеральном округе; **Алексей Мошков** – помощник полномочного представителя Президента РФ в Центральном федеральном округе; **Александр Горбатко** – заместитель руководителя Департамента информационных технологий города Москвы; **Вадим Уваров** – директор департамента информационной безопасности Банка России; **Денис Баранов** – генеральный директор Positive Technologies; **Андрей Бадалов** – вице-президент ПАО «Транснефть»; **Игорь Ляпунов** – вице-президент ПАО «Ростелеком» по информационной безопасности; **Александр Золотов** – первый заместитель генерального директора по управлению, эксплуатации и развитию сети ФГУП «Российская телевизионная и радиовещательная сеть»; **Илья Масух** – директор Центра компетенций по импортозамещению в сфере ИКТ; **Ренат Лашин** – исполнительный директор АРПП «Отечественный софт»; **Андрей Воробьёв** – директор Координационного центра доменов.RU/РФ и многие другие.

Инфофорум-2023 открылся Пленарным заседанием **«Информационная безопасность – стратегический национальный приоритет»**. Также в двухдневной программе Инфофорума-2023 состоялось: 10 тематических заседаний, более 100 выступлений, выставочная экспозиция «Кибер-ЭКСПО. Перспективные технологии информационной безопасности», работа студии Инфофорум ТВ: интервью, комментарии, фотозона.

7 февраля состоялась 20-я церемония награждения профессиональной премией в области информационной безопасности «Серебряный кинжал». Награды вручали: **Александр Шойтов** – заместитель Министра цифрового развития, связи и массовых коммуникаций Российской Федерации и **Эрнест Валеев** – депутат Государственной Думы Российской Федерации, заместитель председателя комитета Государственной Думы по безопасности и противодействию коррупции.

Лауреаты 2023 года

1. В номинации «За вклад в укрепление системы обеспечения информационной безопасности Российской Федерации»:

- **Шляхин Алексей Вячеславович** – главный советник департамента проблем безопасности в информационной сфере аппарата Совета Безопасности Российской Федерации;

- **Трушин Василий Викторович** – председатель Военно-научного комитета Вооружённых Сил Российской Федерации, заместитель начальника Генерального штаба Вооружённых Сил Российской Федерации;

- **Жиров Павел Валентинович** – начальник отдела управления Федеральной службы по техническому и экспортному контролю.

2. В номинации «За формирование и развитие знаний в области обеспечения информационной безопасности в Российской Федерации»:

- **Краснодарское высшее военное училище;**

- **Малюк Анатолий Александрович** – профессор Национального исследовательского ядерного университета «МИФИ».

3. В номинации «За вклад в развитие деятельности Национального форума информационной безопасности «Инфофорум»:

- **Фролов Дмитрий Борисович** – советник генерального директора ФГУП «Российская телевизионная и радиовещательная сеть» по информационной безопасности, доктор политических наук.

4. В номинации «Международное сотрудничество и информационная безопасность»:

- **Арсеньев Виктор Николаевич** – заместитель начальника Департамента Комитета национальной безопасности Республики Казахстан.

5. В номинации «Цифровая трансформация и информационная безопасность»:

- **Кунгурцев Артём Николаевич** – начальник Управления информационной безопасности Департамента информационных технологий города Москвы;

- **Шиловских Пётр Александрович** – министр информационного развития и связи Пермского края;

- **Ващенко Николай Александрович** – руководитель разработки системы «Периметр» ООО «Гарда Технологии»;

- **Акционерное общество «Апатит»** Группа «ФосАгро».

Также в рамках Большого Национального форума информационной безопасности «Инфофорум-2023» подписано соглашение между Департаментом информационных технологий и цифрового развития Ханты-Мансийского автономного округа – Югры и Ассоциацией «Инфофорум» по организации и проведению 6-й Международной конференции по информационной безопасности «Инфофорум – Югра» на площадке Международного ИТ-Форума с участием стран БРИКС и ШОС. Пройдёт она в Ханты-Мансийске 6–7 июня 2023 года.

ГЛАВНОЕ на Инфофоруме-2023 (из выступлений ключевых участников)

Как менялись кибератаки на российские стратегические объекты в 2022 году: основные факторы. Советник генерального директора компании Positive Technologies, доктор технических наук **Артём Сычёв** рассказал в ходе пленарного заседания о тенденциях в кибератаках за прошлый год.

«Три фактора, которые являются знаковыми: первый – это рост числа уязвимостей и использования их в атаках. Срок, который проходит от появления уязвимостей «первого дня» до применения инструментария, стал крайне коротким», – заметил Сычёв.

Он подчеркнул, что данные взяты на основе практики по клиентам компании на основе 50 серьёзных исследований и не являются «обобщением по всей России».

«Второй фактор – это нехватка кадров практически у 90% компаний, которые попали под атаки. Это гигантская проблема», – подчёркивает специалист. По его словам, кадры либо есть, но не обучены, либо их нет. Ещё одним фактором Сычёв назвал уход с российского рынка иностранных фирм и технической поддержки. Это привело к тому, что у части компаний образовались огромные дыры в системе информационной безопасности. Он также отметил, что злоумышленники атакуют по трём направлениям: государственные организации, ИТ-компании, промышленный сектор.

«По государственному сектору я бы обозначил два момента: продолжается активное использование шифровальщиков. Методы противодействия им немного иные, нежели методы по обычным компьютерным атакам: здесь важнее выявить и быстро локализовать распространение этой заразы, нежели ждать, когда инцидент достигнет определённого уровня», – считает эксперт.

Сычёв также коснулся темы утечек данных. По его мнению, в этих атаках используются методы социальной инженерии, когда напрямую воздействуют на работников компаний: «В любом случае мы должны говорить о повышении компьютерной грамотности».

Говоря о ситуации, которая ожидается в 2023 году, Сычёв заметил, что уход с рынка иностранных компаний породил тему импортозамещения, которая привела к определённой проблеме: «Если раньше наши операционные системы и программные комплексы, крупные информационные системы, производимые российскими разработчиками, были не очень интересны злоумышленникам, то теперь мы видим смещение вектора в сторону изучения «дыр» в этом программном обеспечении».

Кроме этого, злоумышленники активно используют инструменты социальной инженерии, в том числе обход двухфакторной идентификации, уточнил Сычёв.

В Совбезе назвали основные задачи по защите информационной инфраструктуры в 2023 году. Начальник департамента проблем безопасности в информационной сфере аппарата Совета безопасности **Сергей Бойко** на пленарной сессии мероприятия рассказал о задачах по защите информационной инфраструктуры в 2023 году и стоящих угрозах: «В условиях беспрецедентных по масштабу массированных компьютерных атак из-за рубежа в 2022 году приоритетной стала защита от деструктивного информационного технического воздействия на российские информационные ресурсы и прежде всего объекты критической информационной инфраструктуры».

По его словам, принятые уполномоченными органами власти и профильными структурами российских компаний меры позволили обеспечить противодействие этим угрозам. Бойко заметил, что приоритетным

должно стать повышение устойчивости и безопасности функционирования информационных ресурсов и защищённость объектов критической информационной инфраструктуры: «Это относится к сферам электроэнергетики, транспорта, банковской сфере, оборонной промышленности и другим областям. В практическом плане на данных направлениях предстоит воплотить в жизнь выработанные профильной межведомственной комиссией Совбеза дополнительные меры».

Он отнёс к ним обеспечение информационной безопасности при использовании открытого ПО, создание унифицированной среды разработки безопасного отечественного ПО. Коснулся Бойко и организаций оборонно-промышленного комплекса. По его мнению, в них важно «устранить технические каналы утечки информации».

Бойко отметил, что для защиты информации и противодействия атакам потребуется создать ведомственные отраслевые центры компетенций в области обеспечения информационной безопасности. Говоря о первоочередных задачах на 2023 год, чиновник назвал важным развитие взаимодействия государственных органов и организаций по повышению защищённости информационной инфраструктуры и устойчивости её функционирования и добавил: «Потребуется повысить эффективность ведомственной и отраслевой координации деятельности субъектов критической инфраструктуры по вопросам противодействия компьютерным атакам и защиты информации».

Спецоперация существенно повлияла на обстановку в российском информационном пространстве в 2022 году. Об этом на форуме заявил заместитель директора Национального координационного центра по компьютерным инцидентам **Николай Мурашов**: «Против России в информационном пространстве развёрнута беспрецедентная по своим масштабам киберкомпания, основными целями которой является выведение из строя информационной инфраструктуры, а также несанкционированный доступ к информационным системам организаций и предприятий различных отраслей критической информационной инфраструктуры РФ».

По его словам, от момента появления сведений об угрозе до их практической реализации иногда проходит

не более нескольких часов. Мурашов отметил доступность хакерского инструментария на специализированных ресурсах: «Имеют места недружелюбные действия международного киберсообщества, которое для реагирования на киберугрозы first приостановила работу с российскими центрами реагирования на компьютерные инциденты».

«В 2022 году фиксировались максимальные атаки на корневые DNS-серверы, а также отключение провайдеров от крупных магистральных каналов и встраивание вредоносного ПО в широко используемые элементы веб-страниц. Особенностью DDoS-атак последних месяцев стало по-настоящему большое количество их участников. В кратчайшие сроки были сформированы телеграм-каналы, в которых проводилась агитация обычных людей, инструктажи участников, координация и целеуказание, а также распространялись элементы проведения атак», – рассказал Мурашов.

Одним из трендов стали атаки с использованием шифровальщиков. А также и то, что злоумышленники выжирали платёжеспособные организации, у которых шифрование данных может нарушить бизнес-процессы.

«Увеличилось количество атак через цепочки поставщиков. Это и интеграторы, и производители средств защиты, поставщики услуг и другие деловые партнёры. Количество атак через подрядчиков за год, по имеющейся в нашем распоряжении информации, выросло в два раза», – заметил специалист.

Эксперты ИТ-отрасли, государственные деятели и представители профессионального общества обсудили вопросы импортозамещения, цифровой безопасности и противодействия информационным вбросам.

«В первую очередь речь идёт о разработке и замещении высокопроизводительных аппаратных и программно-аппаратных средств защиты информации: межсетевые экраны нового поколения, средства обнаружения и так далее», – отметил заместитель директора Департамента обеспечения кибербезопасности Минцифры России **Евгений Хасин** на обсуждении российской цифровой безопасности.

После ухода западных компаний поставщиков защитного ПО от российских разработчиков потребовались не-

замедлительные действия по созданию отечественных разработок для противодействия компьютерным атакам.

Обсуждая тему безопасности, директор Центра компетенций по импортозамещению в сфере информационно-коммуникационных технологий **Илья Массух** подчеркнул, что тенденция западного мира предоставлять бесплатные приложения несёт в себе очень большую опасность. Он также сообщил, что для достижения полной безопасности российские пользователи должны полностью переходить на отечественные разработки.

Важной темой стали меры противодействия фейкам и информационным вбросам. Заместитель генерального директора Российского фонда развития информационных технологий член оргкомитета «Инфофорума» **Илья Костунов** отметил, что развитие информационных технологий в разы затруднило выявление фейков. Он привёл в пример развитие нейросетей, когда любой человек может обработать любой фильм, сделав себя главным героем.

«За 2022 год почти 4 тыс. уникальных тематических фейковых линий было выявлено – это почти 10 млн копий в различных соцсетях, СМИ и мессенджерах. При этом совокупный охват этих копий фейков исчисляется уже десятках миллиардов просмотров», – согласился с Костуновым начальник отдела аналитического обеспечения АНО «Диалог Регионы» **Сергей Маклаков**. Он добавил, что тенденция распространения фейков в России сохранится и в 2023 году.

По мнению Маклакова, вопрос противодействия дезинформации должен прорабатываться как со стороны государства, так и самих онлайн-площадок. В качестве позитивного примера спикер привёл популярные российские ресурсы «Яндекс», «ВКонтакте» и «Одноклассники».

Киберэксперт предупредил о ложных утечках данных. Злоумышленники способны создать ложную утечку данных из имеющейся в Интернете информации, определить её источник невозможно, рассказал вице-президент ПАО «Ростелеком» по информационной безопасности **Игорь Ляпунов**. «Сейчас колоссального объёма данные уже утекли. И из них сфабриковать любую утечку очень просто, потому что нет какого-то магического способа определить, откуда утекло», – заявил он в рамках «Инфофо-

рума». По словам Ляпунова, структуру данных и названия полей, на которые специалисты обращают внимание в первую очередь, воссоздать легко.

Решения по защите информации должны быть доступны для малого бизнеса. Стоимость решений для обеспечения информационной безопасности на предприятиях малого и среднего бизнеса нужно дифференцировать. Об этом заявил глава Торгово-промышленной палаты РФ Сергей Катирин, выступая на пленарном заседании национального форума по информационной безопасности «Инфофорум-2023»: «Отечественные компании на протяжении ряда лет ориентировались на крупного государственного заказчика, а сегодня они вышли к заказчику с ограниченными ресурсами. И это необходимо учитывать, делать предложения понятными, а цены прозрачными и приемлемыми».

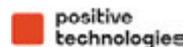
По его словам, нужно постоянно повышать уровень компетенций собственников и руководителей малого и среднего бизнеса в области информационной безопасности. Сегодня такую работу ведут банковские учреждения, производители и дистрибьюторы решений, общественные объединения.

«Наша палата на системной основе проводит вебинары и семинары для предпринимателей. Данная работа может и должна быть системной под эгидой Минцифры, Роскомнадзора с привлечением экспертов отрасли и крупнейших предпринимательских объединений. Могут быть разработаны общие рекомендации для малого и среднего бизнеса. Таким образом, мы получим больший значимый эффект», – отметил глава ТПП РФ.

Кроме того, целесообразно развивать такие направления, как господдержка российского ИТ-бизнеса, а также усиливать роль государства в повышении цифровой грамотности населения и укреплении доверия к «цифре», добавил Катирин.

Национальный форум по информационной безопасности «Инфофорум-2023» – одно из центральных отраслевых мероприятий в сфере информационной безопасности в России, которое проводится с 2001 года. Его аудиторию составляют специалисты, работающие во всех отраслях экономики, представляющие органы федеральной и региональной власти, местного самоуправления, науку, образование, бизнес.

Партнёры Инфофорума-2023



Генеральный партнёр



Золотой партнёр



Специальный партнёр



Серебряный партнёр



Серебряный партнёр



Серебряный партнёр



Серебряный партнёр



Серебряный партнёр



Серебряный партнёр



Серебряный партнёр



Официальный партнёр сессии

Компании-партнёры

«КСБ-СОФТ», «Код Безопасности», NGR Softlab, АО «НПО «Эшелон», «Айдеко», IBS Platformix, «Базальт СПО», CommuniGate Systems, «Киберпротект», «Бизнес Система Телеком», «Фродекс», ГК «Астра», Компания «ЗИКС», ЗАО «ОКБ САПР», «ЭЛВИС-ПЛЮС», «ДиалогНаука», ООО «ЦНТ «Импульс», Компания «Индид», МТУ-СИ, «Фактор-ТС», ООО «А-Реал Консалтинг», «Гринатом Простые Решения», «Конфидент», Компания «Актив», R-Vision, «АЛЬФАКОМ», «Гравитон», RDW Computers, ООО «Акстель-Безопасность», Digital Design, Staffcop, «СЕУСЛАБ», «ЭОС», Zecurion.

Компании-участники

«Астерит», «Открытая Мобильная Платформа», «Галэкс», GSgroup, Лаборатория Касперского, ООО «Айтуби».

25^й национальный форум информационной безопасности
ИНФОФОРУМ 2023

Подготовлено пресс-службой Инфофорума с использованием материалов и цитат ИА ТАСС, Редакции «ФедералПресс», Известия и других источников.

Исследование процессов импортозамещения в ИТ

Об исследовании

Цель:

- изучить процессы импортозамещения;
- выявить потребности целевых групп;
- выявить перспективные ниши для развития.



Задачи исследования:

- анализ поведения и мотивов основных целевых групп в период формирования суверенной экономики;
- определить степень удовлетворённости целевых групп уровнем зрелости российских технологий;
- выявить ключевые задачи и сложности бизнеса и государственных организаций при миграции на отечественные технологии;
- определить основные каналы информации об ИТ-рынке, которыми пользуются целевые группы.

Методология исследования:

- количественный опрос: ИТ-организации (361), государственные учреждения (154), коммерческие компании (167);
- глубинное интервью группы государственных и коммерческих компаний (11 респондентов);
- кабинетный анализ первичной и вторичной информации.

Целевые группы исследования:

ИТ-компании:

- системные интеграторы (47%);
- разработчики ПО (20%);
- реселлеры ИТ продуктов (13%);
- интернет-магазины/провайдеры облачных услуг/SEaaS (20%).

Государственные организации:

- бюджетные и казенные учреждения (90%);
- компании с частичным государственным участием (7%).

Коммерческий сектор:

- SMB (50,6%), крупный бизнес (35%);
- преимущественно промышленный сектор, производственные предприятия, консалтинговые и финансовые организации.

Основные результаты кратко / Основные процессы импортозамещения

Наблюдаются две тактики подхода к импортозамещению:

1

Госзаказчики

Ускоренно переходят на отечественные решения (**влияние административного ресурса**)

Первоочередные задачи:

- найти **аналоги** с подходящим функционалом
- **совместимость** ПО с текущей инфраструктурой
- найти **бюджеты** на переход

2

Коммерческие заказчики

Не планируют переход на отечественные решения в ближайшее время (**выжидательная позиция**)

Технический и психологический барьеры:

- психологический барьер к освоению новых программ;
- заказчикам приходится внедрять «сырые продукты» и **дорабатывать** на месте, что **увеличивает затраты**;
- аналогов нет: специализированные графические редакторы, hardware-решения.

Отношение к процессу импортозамещения в исследуемых сегментах

Рынок глазами ИТ-компаний

- **73%** интеграторов и реселлеров **активно ищут** и пополняют портфель российскими решениями;
- **57%** ИТ-компаний отметили потребность заказчиков в **ускоренном переходе** с западного ПО на российское;
- **37%** уже **планируют** заместить иностранное оборудование

Компании также стремятся:

- **восполнить** недостающую экспертизу по новым решениям (**17%**);
- **сертифицировать** сотрудников (**18%**);
- организовать центры **экспертизы** и демозоны для заказчиков (**11.9%**).

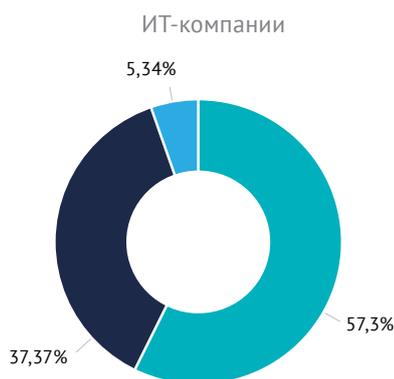
Рынок глазами заказчиков

- **44,7%** респондентов выбрали **тактику не спешить** и не замещаться в ближайшей перспективе;
- **27%** участников коммерческого сегмента предпочитают **ждать окончания срока лицензий установленного ПО**;
- **22%** **планируют заместиться** до того, как софт перестанет работать;
- основные **причины «выжидательной позиции»:** работоспособность уже установленного ПО, отсутствие альтернатив hardware, неудовлетворённость существующими отечественными решениями.

Рынок глазами государственных структур

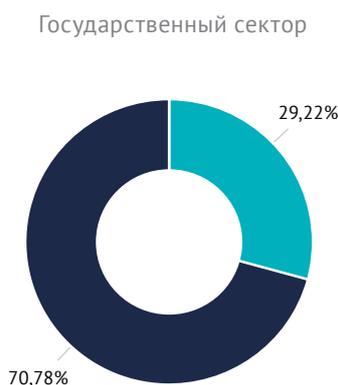
- **70%** участников опроса уже давно живёт в **парадигме перехода на отечественные решения** (процесс планомерно идёт с 2014 года);
- **29%** сталкивается с внедрением, эксплуатацией и **несовместимостью систем** с существующими решениями.

Испытывают ли ваши клиенты потребность в области импортозамещения ИТ-решений?



- Да, испытывают, планируют замещать западное ПО
- Планируют замещать западное оборудование
- Нет, не планируют ничего замещать

Испытывает ли ваша компания сложности в области импортозамещения ИТ-решений?



- Да, испытывает
- Нет, не испытывает

Испытывает ли ваша компания потребность в области импортозамещения ИТ-решений?



- Да, испытывает, будем замещать всё западное ПО до окончания срока
- Будем замещать только тогда, когда будут заканчиваться лицензии
- Нет, не планируем ничего замещать
- Будем замещать всё западное оборудование

«У нас нет необходимости в замещении. Мы не являемся госучреждением и не испытываем никакого административного давления». Представитель производственного предприятия

«Мы используем большой стэк продуктов. AstraLinux, МойОфис, Р7-Офис, Куберпротект, Код Безопасности, UserGate, Kaspersky, Элтекс. Ожидания оправдали». Представитель здравоохранения

«Могу положительно отозваться о всех продуктах российского производства в сфере информационной безопасности». Представитель образовательной организации

«Железо менять не планируем, идут плановые замены, из срочного ничего нет. Планируем менять только роутеры. Сейчас стоит вопрос только в лицензировании». Представитель консалтинговой компании

«Не испытываем проблем, потому что всё либо легко подбирается, либо не замещается в принципе». Представитель компании с частичным государственным участием

«В нашей области особых проблем нет, вся линейка у нас имеется. Есть проблема не заместить, а мигрировать на отечественное ПО». Представитель здравоохранения

Задачи и проблемы импортозамещения

Перед ИТ-рынком стоят три ключевые задачи:

1. Сохранить бесперебойность работы текущей инфраструктуры.
2. Обеспечить информационную безопасность.
3. Наладить работоспособность прикладного ПО.

Исследуемые целевые аудитории испытывают одинаковые сложности при импортозамещении. Однако их приоритетность в государственном секторе и бизнесе разная. Основная проблема для бюджетных организаций – несовместимость ПО с существующей инфраструктурой и ограниченность ИТ-бюджетов.

Для частных компаний ограниченность функционала у отечественных аналогов или отсутствие их в принципе является главным препятствием для импортозамещения. Такую разницу можно объяснить тем, что подведомственные организации начали процесс внедрения и использования российских технологий раньше, поэтому они сталкиваются с проблемой несовместимости, в то время как коммерческий сектор только присматривается к существующим инструментам.

В качестве проблемных зон в процессе импортозамещения респонденты отметили:

- несовместимость операционных систем с оборудованием;
- нестабильность работы установленных решений;
- недостаточный функционал в СХД;
- проблемы с сетевым оборудованием;
- внедрение офисных пакетов и миграцию; на коммуникационную платформу.

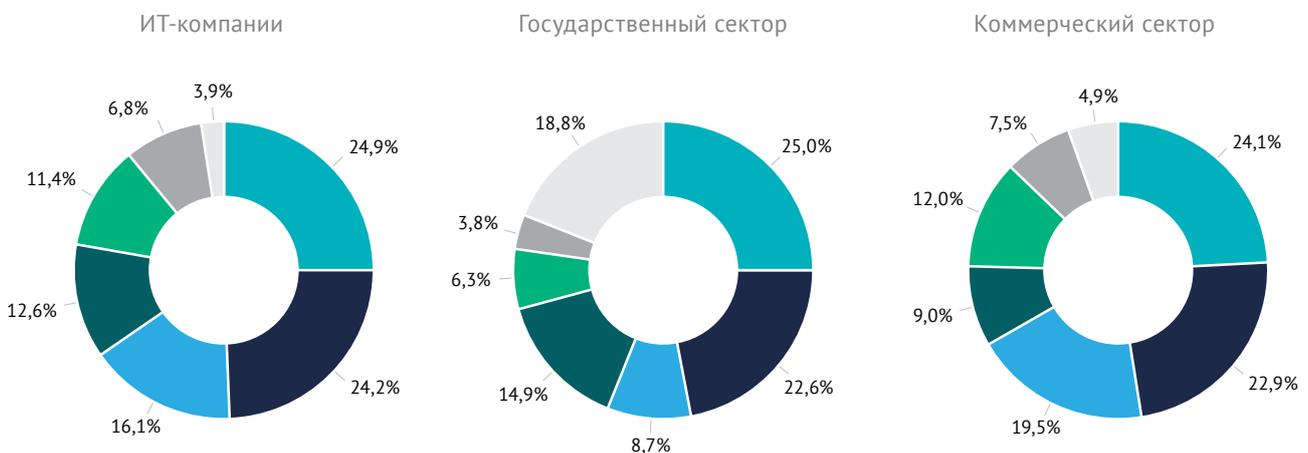
Среди остро необходимых направлений для замещения все участники выделили инфраструктурное и прикладное ПО, ИБ-решения, аппаратное обеспечение.

Причём голоса распределились практически одинаково среди всех исследуемых сегментов, за исключением госзаказчиков, для которых инфраструктурное ПО важнее на данный момент, чем ИБ.

Это может говорить о том, что вопрос с информационной безопасностью был решён в первую очередь, следуя законодательным требованиям.

Какие основные ИТ-задачи побуждают использовать российские ИТ-продукты?

- Обеспечить работоспособность текущей инфраструктуры
- Обеспечить информационную безопасность
- Обеспечить работоспособность прикладного ПО
- Обеспечить бесперебойное функционирование виртуализации
- Обеспечить дальнейшую автоматизацию
- Обеспечить дальнейшую безопасную разработку
- Другое



Сложности импортозамещения

Государственный сектор

- Несовместимость российского ПО/оборудования с текущей инфраструктурой является наиболее острой проблемой (**25,6%**). Сложности возникают с совместимостью ОС с новым оборудованием, а также ИБ-системами, внедрением ПО, офисными приложениями, аттестацией рабочих мест и виртуализацией.
- Ограниченность ИТ-бюджетов отмечает **23%** респондентов, что связано напрямую с отсутствием необходимого функционала в российских системах (**22,2%**), поэтому организациям приходится изыскивать дополнительные средства на доработку под конкретные нужды.
- Выполнение требований законодательства побуждает внедрять **«сырые» продукты** и дорабатывать их в процессе работы, что значительно увеличивает стоимость продукта.

Бизнес

- Отсутствие необходимого функционала выходит в данном сегменте на первое место (**28,7%**).
- **19%** респондентов основной проблемой I называют отсутствие бюджетов и недостаточное количество решений на рынке для закрытия конкретных задач.
- Проблема несовместимости является также важной для бизнеса, но пока не первоочередной – 15,7% респондентов, так как большая часть компаний не начали активно импортозамещаться.
- Определяется коммуникационный разрыв между ЛПР и ИТ/ИБ-подразделениями компаний. Руководители готовы ждать окончания существующих лицензий, в то время как специалисты предупреждают о немедленной замене, особенно это касается ИБ-систем.

ИТ-компании

- **27%** интеграторов и реселлеров отмечают, что отсутствие необходимого функционала у российского ПО является основной проблемой для миграции заказчиков, так же, как и совместимость с существующей инфраструктурой – **20,7%**.
- Отсутствие на рынке необходимых решений, которые могли бы заменить иностранное ПО, подтверждает **15,8%** респондентов.
- **16%** указали, что дополнительная плата за миграцию является сложностью для заказчиков, так как ИТ-бюджеты ограничены.

Что является главной сложностью для вас в импортозамещении?

- Не на что мигрировать, недостаточно решений на рынке
- Несовместимость российского ПО/оборудования с текущей инфраструктурой
- Отсутствие необходимого функционала в российских аналогах
- Ограниченность ИТ-бюджетов на ПО и оборудование
- Дополнительная плата за миграцию (перенос надстроек, макросов, политик и пр.)
- Другое



«У нас небольшое количество ПО. Для нас важно прокси, почтовое ПО, антивирусы. Хотим попробовать внедрить наш офис, посмотрим справится или не справится. Требуется дизайнерские программы для рекламы».

Представитель консалтинговой компании

«Сейчас мы нацелились на Астру, но опять же не видим, чтобы клиенты массово переходили на неё. На 1–2 года в выжидательной позиции. Но чего ждать – непонятно. Сложно убедить директора например, что необходимо 60 операционных систем».

Представитель консалтинговой компании

«Мы используем в основном Альт. Проблема заключается в работе принтеров Canon. Работает хорошо браузер, и то 50 на 50, hr без проблем устанавливается, со сканерами ещё не пробовали. Но драйверов просто не найти. Их либо вообще не существует в природе, либо работают не так, как нужно, в зависимости от модели принтера. Также есть проблемы аттестации рабочего места на некоторых машинах. Новые программы «сырые» и работают с ошибками, например, 1С».

Представитель подведомственной организации

«Покупать сейчас масштабные решения для нас сложность.

У директора цель – не растративать деньги. Возникают сложности в том, что требуется переучивать сотрудников. Сейчас мы ищем у себя технические резервы».

Представитель консалтинговой компании

«У нас проблема в несовместимости операционных систем с новым современным оборудованием, а точнее, с выполнением требований законодательства в части информационной безопасности. Либо операционка не поддерживает, либо средство, которое должно защищать, не поддерживает операционку. В принципе, вопрос решаемый. Вендор предлагает на замену свой же продукт, с которым надо будет использовать какие-то наложенные средства. Но это накладывает финансовые трудности, нам нужны дополнительные средства на переход на другую версию».

Представитель производственного предприятия

В чём, на ваш взгляд, наиболее остро ощущается необходимость в импортозамещении?

- Инфраструктурное и прикладное ПО
- Информационная безопасность
- Аппаратное обеспечение
- Облачные решения
- Другое



Источники информации о российских решениях

Несмотря на то, что целевые группы используют в большинстве случаев интернет, СМИ-презентации вендоров как основной источник информации, в глубинных интервью участники пояснили, что больше доверяют блогам, тематическим чатам и «сарафанному радио».

Использование неофициальных каналов говорит о том, что существует коммуникационный разрыв между разработчиками и заказчиками, которые сталкиваются с трудностями при эксплуатации решений, но не могут оперативно решить силами вендора. Также очевидно, что в интернете недостаточно информации о существующих решениях, поэтому представители компаний, технические и ИБ-специалисты стремятся восполнить её на других ресурсах.

- **38,8%** госзаказчиков предпочитает изучать информацию на официальных сайтах производителей и из профессиональных статей в СМИ. При этом **20%** считает презентации и рассылки от вендоров более надёжным источником информации, другие же (**21%**) доверяют только тематическим блогам или чатам с коллегами.
- Большинство представителей бизнеса (**36%**) также выбрало интернет и информацию от вендоров (**26%**) в качестве основного источника информации. Однако в глубинных интервью респонденты отмечали, что больше доверяют «сарафанному радио», блогам, где люди активно обмениваются опытом и делятся советами.
- ИТ-компании в меньшей степени доверяют интернету и СМИ (**22%**), преимущественно используют рассылки и презентации вендоров (**36%**), а также отраслевые блоги (**18%**) и сервисы по подбору решений (**16%**).

Цифровые финансовые инструменты: криптовалюты и перспективы их легализации

Глобализация мировой экономики и развитие ИТ-технологий в финансовой сфере сделали возможным возникновение нового вида денег – криптовалют – и их последующее стремительное распространение по всему миру. Так, первая криптовалюта (BTC, биткоин) была сгенерирована лишь десятилетие назад – 3 января 2009 г. Но уже сегодня операции с крипто-

валютами проводятся на биржах, в обменных пунктах и на многих ресурсах в Интернете. Однако национальное законодательство и само общество не успевают за активным развитием информационных технологий. Как следствие, проблема слишком быстрого роста криптоиндустрии выходит на первый план экономической повестки дня многих стран мира.

Криптовалюта – вид цифрового финансового актива, создаваемый и учитываемый в распределённом реестре цифровых транзакций участниками этого реестра в соответствии с правилами ведения реестра цифровых транзакций (Федеральный закон «О цифровых финансовых активах, цифровой валюте и изменениях отдельных законов Российской Федерации» от 31.07.2020 № 259-ФЗ) и учитываемый в распределённом реестре цифровых транзакций (рис. 1).

Рынок криптоплатежей – самая быстрорастущая отрасль. По прогнозам, с наибольшим среднегодовым темпом роста с 2019 до 2024 года рынок будет расти. У криптовалютных платежей есть несколько преимуществ:

- повышенная безопасность транзакций;
- защищённость от мошенничества;
- децентрализация;
- низкие комиссии;
- защита от возвратных платежей;
- быстрые международные трансферы.

По мнению аналитиков, самыми перспективными являются следующие виды токенов: Bitcoin (BTC), Ethereum (ETH), Litecoin (LTC), Cardano (ADA), Chainlink (LINK), XRP (Ripple), Bitcoin Cash (BCH), Tron (TRX).

В конце июля 2021 года исследователи института Гэллапа представили результаты анализа крипторынка, согласно которым с 2018 года число инвесторов самой капитализированной криптовалюты – бикоина – выросло в 3 раза. Исследователи пришли к выводу о том, что росту числа инвесторов биткоина и улучшению отношения потенциальных инвесторов к активу способствовал интерес к валюте со стороны таких компаний, как Tesla, Square и Morgan Stanley.



David Chaum, корпорация DigiCash – первая анонимная централизованная платёжная система.

Wei Dai – показывает идею собственной криптовалюты b-money, система прямых, анонимных и быстрых расчётов, децентрализованный реестр.

Satoshi Nakamoto (тайный создатель) – создание криптовалюты «биткоин» – одноранговая электронная денежная система.

Начало работы ПО версия **Биткоин 0.1**. Был сгенерирован первый блок монет и проведена первая транзакция – первый обмен биткоинов на реальные деньги. Пользователь **ArtForz** создаёт первую майнинговую ферму.

17 июля 2010 года была создана первая биржа цифровых валют **MtGox**.

В журнале Forbes вышла статья под названием **Crypto currency**, посвящённая биткоину, после этого термин «криптовалюта» стал общеупотребимым для описания подобных систем.

Рис. 1. История развития криптовалюты



Рис. 2. Потребляемое количество энергии (здесь укажите ед. измерения)
Источник: данные электронного сайта BBC News

Больше всего инвесторов интересуется биткоин (47%). На 2 месте по популярности среди криптоинвесторов оказалась вторая по капитализации криптовалюта – Ethereum (18%). На 3 месте по уровню интереса расположился стейблкоин Tether. На категорию «другие монеты» пришлось 17%.

Биткоин – ключевая криптовалюта, являющаяся наиболее ранней, безопасной, дорогой, стабильной и популярной во всём мире. Следует отметить, что в 2021 году министр финансов США или экономический советник Байдена, указали, что операции с биткоинами потребляют слишком много электроэнергии, поэтому сделки с ними крайне не эффективны. Интересный факт, что

биткоин потребляет такое же количество электроэнергии, как Нидерланды (рис. 2).

Главным фактором создания и продвижения криптовалюты было недовольство пользователей в государственном регулировании системы платежей. Существующие государственные платёжные системы не только контролируются различными регуляторами, но и являются зачастую не чувствительными к изменениям финансового рынка, поэтому потребовался аналог – независимая анонимная платёжная система прямых и быстрых расчётов с новой системой хранения данных и транзакций, такой технологией стала технология децентрализованного реестра или блокчейна.

Сегодня зарубежные специалисты выделили три основных подхода к пониманию сущности блокчейна.

1. Технически блокчейн есть база данных, выступающая как распределённый реестр с возможностью открытой проверки.
2. Определение с позиции бизнеса: это обменная сеть для перемещения транзакций, стоимости, активов между равными партнёрами без помощи посредников.
3. Определение с позиции юридической: это институт проверки транзакций без участия посредников.

По сути, блокчейн считается одной из разновидностей распределённого реестра со специфическими техническими устройствами. Именно они, в отличие от обычного распределённого реестра, формируют особые признаки: криптозащищённость, неизменяемость, наличие подписи в сообщении, формирование связанной цепочки блоков и консенсус при её создании. При таком способе хранения данных на многих компьютерах (нодах) ведётся онлайн-журнал с записями о каком-то активе и операциях с ним. Записи в блокчейне объединяются друг с другом в специальную структуру – блок. Этот блок содержит свой порядковый номер и результат обработки имеющихся в предыдущем блоке данных (особую хэш-функцию), с помощью которой можно проверить информацию (рис. 3).

На волне интереса к криптовалюте многие клиенты стали активно использовать технологию блокчейна. Сейчас, по данным экспертов, в мире насчитывается примерно 1000 модификаций блокчейнов, которые используются в самых различных сферах.

Но технология блокчейна не свободна от рисков, которые искажают его функционирование и требуют усилий по их преодолению. В связи с этим возрастают затраты по защите данных и технологии от неправомерного использования и взлома. Достаточно сказать, что, по данным WinterGreen, рынок программного обеспечения, услуг и аппаратных решений для защиты блокчейнов к 2024 году будет составлять 355 млрд долларов по сравнению с 259 млн долларов в 2017 году (www.if24.ru/tri-ugrozdlya-blokcejna). Речь идёт о выявлении способов взлома платформы, о разработке методов их нейтрали-

зации, о защищённости смарт-контрактов, о подготовке кадров специалистов ИТ, способных обеспечивать безопасность на уровне современных требований.

Положение криптовалюты в мире

Совокупная рыночная капитализация криптовалют увеличилась практически в 3 раза в течение только 2021 года. А годовая прибыль инвесторов выросла с 32,5 млрд до 162 млрд. Но после пика в ноябре 2021 года – тогда капитализация достигла \$2,9 трлн – к середине 2022 года она упала ниже \$1 трлн. Эксперты связывают это с тем, что значительное количество крупных инвесторов в этот момент ушли с криптовалютного рынка. Причинами этого оттока называют скачок инфляции в США и опасения, что повышение процент-

ных ставок центральными банками будет препятствовать росту криптовалютных активов. Но практически все эксперты прогнозируют новую волну роста.

К концу 2021 года во всём мире насчитывалось порядка 295 млн владельцев криптовалюты, что составило 3,83%. Ожидалось, что к концу 2022 года количество владельцев криптовалюты в мире достигнет 1 млрд (рис. 4).

Visa, MasterCard и PayPal внедряют криптовалюты в свои платёжные системы, а это становится катализатором освоения цифровых решений для остального финансового сектора. И не только финансового: в июле 2021 года социальная сеть Twitter решила пользователям отправлять донаты для своих креаторов в биткоинах.

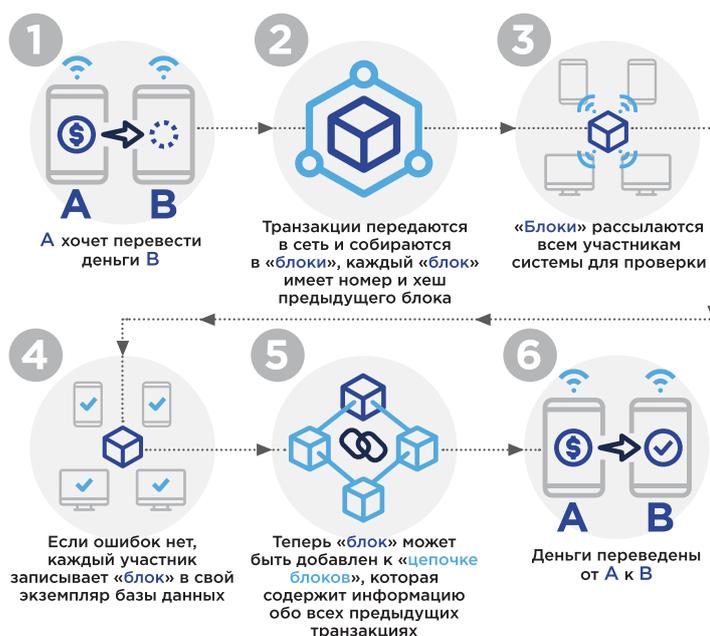


Рис. 3. Функционирование технологии блокчейн на примере криптовалюты



Рис. 4. Рост числа владельцев криптовалют в 2021 году
Источник: данные PLCUX

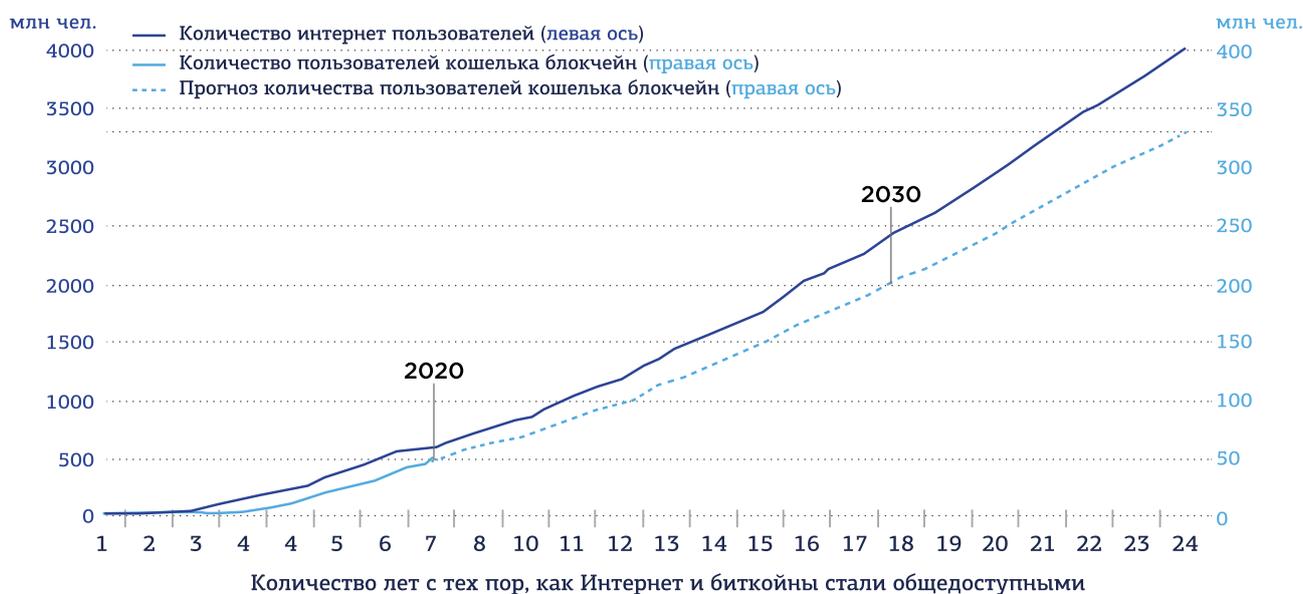


Рис. 5. Сравнение распространения криптовалют и интернета

Источник: данные PLCUX

Распространение криптовалют сравнивают с распространением интернета, которое лишь растёт в скорости. По этой аналогии, криптовалюты только начали период бурного развития (рис. 5).

На современном этапе прослеживается ряд тенденций регулирования

криптовалюты за рубежом: во многих странах (Алжир, Бангладеш, Египет, Ирак, Непал, Китай, Катар, Тунис) использование криптовалюты запрещено в связи с тем, что эта сфера экономики находится в «серой зоне» и единственным средством платежа является национальная валюта; в некоторых странах торговля крип-

товалютой запрещена, в других – разрешена исключительно на криптовалютных биржах; в качестве средства инвестирования криптовалюта зачастую запрещена (табл. 1).

Так, Азиатско-Тихоокеанский регион, в том числе RoAPAC (Сингапур, Малайзия, Таиланд, Индия, Австралия

Таблица 1. Методы регулирования криптовалюты в разных странах

Страна	Методы регулирования
Южная Корея	Чтобы пользоваться криптовалютой, каждый трейдер должен инициировать себя с помощью создания счёта в банке.
Индия	Индия легализовала использование криптовалюты в качестве биржевого товара. Весной 2022 года одобрен «Закон о финансах», предполагающий взимание налога в размере 30% с любого дохода, полученного от криптовалютных транзакций, и второй налог в размере 1% у источника дохода со всех транзакций (TDS).
Китай	Запрещает ICO и торговлю на международных биржах.
Евросоюз	Обмен криптовалюты на нац. валюту не будет подвергаться НДС; идентификация криптовалютных бирж обязательна.
США	Криптовалютой пользоваться можно, только используя лицензию (разработчики ПО и купля-продажа товаров и услуг); налогом облагаются; не признаются платёжным средством.
Швейцария	Швейцария одна из первых стран разрешила использовать криптовалюту в качестве платёжного средства. В последние два года местное управление по надзору за финансовыми рынками (FINMA) выдало лицензии 2 цифровым банкам, одной бирже и первому в стране инвестиционному фонду. С 2016 года принимаются коммунальные платежи в BTC. Цифровые монеты можно купить в банкоматах и железнодорожных кассах по всей стране. Коинами платят за покупки в универмагах (бренд Lehner Versand) и в торговых сетях. Криптовалютные компании облагаются налогом на богатство. Профессиональные трейдеры вносят сборы за приток капитала. Криптовалюта соотносится с фиатными деньгами, для которых не предусмотрен НДС. Осенью 2022 года FINMA ужесточит правила проведения операций с криптовалютами для усиления действий по борьбе с отмыванием денег. В соответствии

	с новыми правилами гражданам страны придётся подтверждать личность при проведении операций с криптовалютными активами на сумму более 1000 швейцарских франков (около \$ 1000) в месяц.
Великобритания	Разработан законопроект о финансовых услугах и рынках, согласно которому криптовалюты должны быть включены в систему регулирования финансовых активов. То есть криптовалюта будет признана самостоятельным финансовым активом (криптоактивом). В декабре 2022 года британские власти приняли решение о разработке нового комплекса мер по регулированию индустрии криптовалют, включающий ограничения на продажу криптовалют иностранным компаниям, инструкции на случай краха криптофирм, введётся запрет на работу неавторизованных крипто-провайдеров, а также рекламные ограничения.
Саудовская Аравия	Саудовская Аравия ещё не выпустила никаких официальных нормативных актов, касающихся криптовалют, но правительство заняло благосклонную позицию в отношении цифровых активов и технологии блокчейн. В 2022 году появилась регуляторная песочница от денежно-кредитного управления (SAMA) – аналога центробанка, а также образовательные программы по блокчейну. Разрешён майнинг.
ОАЭ	Введена упрощённая схема получения лицензии для криптобизнесов. В Дубае действует закон «О регулировании виртуальных активов», нацеленный на создание правовой базы для защиты инвесторов и разработки общепризнанных международных стандартов для индустрии виртуальных активов. В стране нет подоходного, корпоративного и других налогов, компаниям необходимо платить лишь НДС в 5%.
Франция	Нет запрета на пользование криптовалютой, но вскоре будет введено их налогообложение и требование по раскрытию всех сделок (убирается анонимность).
Германия	Биткоины признаны средством взаиморасчётов; криптовалюта облагается налогами; легальны только операции с частными лицами.
Турция	Криптовалюта разрешена, но ведутся наблюдения над пользователями, чтобы в дальнейшем разработать эффективную правовую базу.
Сингапур	Криптовалюта считается финансовым активом, но рынок не регулируется; сделки облагаются НДС; криптовалютным биржам разрешено работать только по лицензиям.
Япония	Высокий налог на прибыль от криптовалюты (55%). Парламент в 2022 году принял законопроект, разъясняющий правовой статус стейблкоинов и определяющий их как цифровые деньги (вступит в силу через год). В настоящее время вводятся новые правила, ужесточающие борьбу с отмыванием незаконно полученных средств с помощью цифровых активов. Местные криптовалютные биржи обяжут передавать информацию о клиентах, включая их имена и адреса, при перемещении криптовалют между платформами. Меры предоставят властям дополнительные возможности для мониторинга денежных переводов лиц, занимающихся нелегальной деятельностью.
Бразилия	29 ноября 2022 года Палатой представителей после семи лет дебатов был одобрен законопроект, который будет регулировать криптовалютный рынок в Бразилии. Регулятором выступит Центральный банк страны. Законопроект предусматривает выпуск лицензии поставщика виртуальных услуг, которую должны запрашивать биржи и другие криптокомпании. Новые правила будут применять к юридическим лицам, которые обменивают цифровые монеты, переводят их и финансово взаимодействуют с эмитентами и поставщиками виртуальных активов. Это не делает биткоин или другую криптовалюту законным платёжным средством в стране, но признаёт их в качестве цифрового представления стоимости, которое можно использовать как платёжный инструмент и инвестиционный актив.
Сальвадор	В июне 2021 года Сальвадор первой приняла Bitcoin в качестве официального платёжного средства. С 2021 года с принятием закона Bitcoin Law в стране многие цены указываются в биткоинах, налоги можно платить биткоином, обмен долларов на эту криптовалюту не облагается налогом. Внедрён национальный криптокошелёк Chivo, обеспечивающий транзакции без комиссии. В 2022 году Сальвадор создал Национальный офис (ONBTC) по биткоином, который занимается контролем всех инициатив, имеющих отношение к данной криптовалюте. На данный момент в стране рассматривается «Закон о выпуске цифровых активов», который будет регулировать деятельность компаний и эмитентов услуг цифровых активов в стране.

и Новая Зеландия) находятся на первом месте по объёму криптовалютного рынка в мире и примут на себя наибольшую долю всего криптовалютного рынка в течение периода до 2024 года. Уровень осведомлённости и знаний о криптовалютах наиболее высоки в Японии. Государственное регулирование в Японии очень лояльно к криптовалюте. Развивающиеся экономики также вносят серьёзный вклад в развитие криптовалют. По данным Chainalysis, на страны RoAPAC в 2021 году пришлось 43% всей активности на рынке, а три первых места по объёму транзакций заняли Вьетнам, Пакистан и Индия.

Европа занимает второе место после Азиатско-Тихоокеанского региона по объёму криптовалютного рынка. В Европе также растёт осведомлённость о криптовалютах. Эксперты Европейского центрального банка отмечают, что интерес к криптовалютам в регионе быстро растёт и что до 10% жителей региона уже купили цифровые валюты.

В Европе также развивается регулирование криптовалютного рынка. В марте 2022 года был принят законопроект о включении поставщиков кошельков и платформ по обмену виртуальных валют в Директиву по борьбе с отмытием денег (AMLD). В рамках этого постановления поставщики кошельков и платформ для обмена виртуальных валют будут обязаны выполнять требования по борьбе с отмытием денег и предоставлять данные, необходимые для выявления, предотвращения и подготовки отчётности по отмытию денег и финансированию террористических организаций. Виртуальные валюты определяются как цифровое представление ценности, которое не выпускается Центральным банком или государственным органом и необязательно

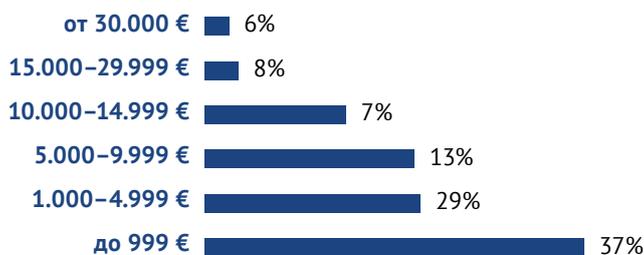


Рис. 6. Состояние европейского криптовалютного рынка (по критерию стоимости владения крипто-активами)

Источник: www.gminsights.com

связано с фиатной валютой, но принимается физическими и юридическими лицами в качестве средства оплаты, которое можно хранить, переводить или обменивать онлайн (рис. 6).

По данным специалистов криптобиржи Gemini, 2022 год стал прорывом для многих цифровых валют. Криптовалюты перестали быть малоизвестными и понятными только экспертам. Особенно большую роль в популяризации криптовалют сыграли социальные сети, где цифровые активы стали темой оживлённого обсуждения, а посты известных предпринимателей напрямую влияют на цены криптовалют. Вместе с осведомлённостью о криптовалютах растёт и число инвесторов. Около 10% населения Земли с доступом к интернету владеют криптовалютами. Ожидается, что в будущем эта цифра будет только расти.

Большой интерес вызывают и новые способы инвестиций в криптовалюты. Теперь, чтобы получить прибыль, обязательно продавать и покупать монеты. Интерес инвесторов вызывают DeFi – децентрализованные финансы. На данный момент в этих сервисах работают 40 миллиардов долларов. А в октябре 2021 года в США был одобрен первый биткойн-ETF. Фонд объединяет криптовалюты и биржи

акций и позволяет инвесторам вложиться в биткойн через традиционных брокеров. На состояние рынка криптовалют также влияют глобальные проблемы. Так, и регуляторы, и большое число пользователей обеспокоены высоким энергопотреблением проектов на блокчейне, а также возможностью использовать криптовалюты для финансирования преступности. Для решения данных проблем планируется переход на новые формы организации сетей, что значительно сократит потребление энергии, а новые правила контроля криптовалют помогут ограничить опасные транзакции.

Рынок криптовалюты в России

В настоящее время Россия является одним из ключевых игроков на рынке криптовалют (табл. 2).

Согласно исследованию Банка России «Криптовалюты: тренды, риски, меры» от 20 января 2022 г., российские граждане покупают криптовалюту, используя различные способы, в том числе и за наличные деньги; основные цели её приобретения физическими и юридическими лицами: спекуляция, инвестиции, уход от требований ПОД/ФТ, трансграничные переводы.

К эмитированным частным образом активам, в соответствии с докладом

Таблица 2. Рейтинг стран по числу пользователей на криптобиржах

№	Binance	Huobi	Coinbase	Kraken Exchange	Bithumb	Butfinex
1	Турция	Китай	США	США	Республика Корея	Россия
2	Россия	Украина	Соединённое Королевство	Германия	Россия	Тайвань
3	Соединённое Королевство	Вьетнам	Испания	Франция	Турция	Германия
4	Бразилия	США	Германия	Соединённое Королевство	США	Украина
5	Аргентина	Россия	Франция	Нидерланды	Польша	Бразилия

Источник: доклад Банка России «Криптовалюты: тренды, риски, меры»

Банка России, можно отнести следующие группы финансовых активов:

- 1) электронные деньги (eMoney) – этот финансовый актив, выпущенный частным эмитентом, выступает в качестве альтернативы наличным деньгам;
- 2) необеспеченные криптовалюты;
- 3) стейблкоины – криптоактив, представляющий собой аналог фонда денежного рынка или иного имущественного комплекса, при выпуске которого может использоваться непрозрачная система, не обладающая правовыми основами;
- 4) токенизированные активы – криптоактивы, применяемые в целях закрепления за их владельцами определённых прав: аналоги акций, долговых ценных бумаг, права на получение определённого товара или услуги.

Вне зависимости от вида криптовалюты её долгосрочный потенциал может быть ограничен в связи со стремительным ростом рыночной стоимости. Формирование стоимости на рынке определяется её спекулятивным спросом в расчёте на дальнейшее увеличение курса.

По независимым исследованиям объём рынка криптовалюты в России на январь 2022 года оценивается в 16,5 трлн рублей, или 214 млрд долларов США, что эквивалентно примерно 12% от общей мировой стоимости криптоактивов. По данным сингапурского платёжного шлюза TripleA, более 17 млн россиян, или около 12% всего населения, владеют той или иной криптовалютой. По словам источников агентства, возраст около 60% криптоинвесторов составляет от 25 до 44 лет. Банк России приводит данные, согласно которым объём операций с криптовалютами в РФ по итогам прошлого года составил 5 млрд долларов США.

Согласно данным МВФ, в 2021 году Россия наряду с несколькими другими находилась в числе лидеров по количеству посещений сайтов таких криптобирж, как Binance (2-е место), Huobi (5-е место), Bithumb (2-е место), Bitfinex (1-е место). Российские граждане являются активными пользователями интернет-платформ, осуществляющих торговлю криптовалютами. Кроме того, Россия находится в числе лидеров по объёму мировых майнинговых мощностей. Согласно данным, позволяющим оценить объём трафика

с территории Российской Федерации, доля российских пользователей на различных криптобиржах варьируется в пределах от 7 до 14,5%. Помимо иностранных криптовалютных бирж, в России распространена покупка криптовалюты через криптообменники (в т.ч. telegram-боты, терминалы) в Интернете. В августе 2021 года Россия вышла на 3-е место по объёму майнинга биткоина: на её долю приходится 11,23% вычислительных мощностей, используемых для майнинга биткоина (в начале 2021 года доля России составляла 6,9%).

При этом Россия лидирует в мире по доле теневых криптовалютных операций с долей в размере 41,1% по итогам 2021 года по данным Chain Technologies. Второе место на глобальном рынке теневых криптоопераций занимает Украина (доля – 6,54%), третье – Великобритания (2,8%) и Германия (1,87%). Доля «неизвестных стран» составила 24,6%, «других» – 23,1%. Специалисты объясняют это популярностью в России запрещённых сервисов, таких как Hydra, а также простотой проводимых операций, лёгкостью регистрации доменов, слабостью правового регулирования и отслеживания.

Проблемы законодательного регулирования криптовалюты в России

В Концепции законодательного регулирования механизмов организации оборота цифровых валют от 8 февраля 2022 года, отмечается, что в настоящее время в России отсутствует должное законодательное регулирование такого высокорискованного финансового инструмента, как цифровая валюта (криптовалюта). Вступивший в силу с 1 января 2021 года Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» даёт только общие ориентиры для регулирования отношений, возникающих при обороте цифровых финансовых активов и цифровой валюты, и указывает на иные федеральные законы, которые должны быть приняты в развитие норм основного закона. В частности, речь идёт об отдельных нормативных правовых актах, которые должны упорядочить организацию выпуска и обращения цифровой валюты в России (ч. 4 ст. 14 Закона № 259-ФЗ).

Но, несмотря на то, что криптовалюта в РФ на законодательном уровне не является средством платежа, вместе с тем она не находится под запретом и не ограничивается право на владение ею. И, по статистике, обозначенной в Концепции, за последние годы наблюдается существенный рост объёмов денежных средств россиян, вкладываемых в криптовалюты. По экспертным оценкам, гражданами РФ открыто более 12 млн криптовалютных кошельков, а объём средств на них составляет порядка 2 трлн руб.

В отношении правового регулирования криптовалюты на территории России существуют значительные разногласия между Минфином России и Банком России.

Так, министерство выступает за запрет использования цифровых валют в качестве средства платежа на территории РФ, рассматривая криптовалюту исключительно в качестве инструмента для инвестиций и предполагая возможность осуществления операций с покупкой или продажей криптовалюты только при условии проведения идентификации клиента. Позиция ведомства по этому вопросу отражена в разработанном им законопроекте «О цифровой валюте». В рамках проектов законов «О цифровой валюте» и «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О цифровой валюте» Министерством финансов Российской Федерации предложено внедрение следующих изменений:

- законодательное закрепление определения цифрового майнинга как деятельности, направленной на получение криптовалюты;
- введение механизма предоставления информации налоговым органам, действующим на территории Российской Федерации;
- создание условий для проведения операций с покупкой и продажей криптовалюты при идентификации клиента;
- сохранение запрета на использование криптовалют в качестве средства платежа на территории Российской Федерации.

Помимо предложенных мер, Министерство финансов Российской Федерации настаивает на введении онлайн-тестирования перед покупкой криптовалюты для российских гра-

ждан: при успешном прохождении теста можно будет вкладывать до 600 тысяч рублей в год, без теста – 50 тысяч рублей, при этом квалифицированным инвесторам и юридическим лицам будет разрешено совершать операции без ограничений.

В свою очередь, Банк России уверен, что распространение криптовалют создаёт существенные угрозы для благосостояния населения, стабильности финансовой системы и угрозы, связанные с обслуживанием криптовалютами нелегальной деятельности. В частности, речь идёт о рисках для граждан: из-за высокой волатильности курса и распространённости мошенничества в торговле криптовалютами имеются риски утраты существенной части вложенных средств, а при торговле с использованием заёмных средств – риски остаться должником. Распространение криптовалют приводит и к выводу сбережений граждан за периметр российского финансового сектора и, как следствие, сокращению его возможностей по финансированию реального сектора и снижению потенциального роста экономики, что уменьшает количество рабочих мест и потенциал роста доходов граждан (табл. 3).

В начале декабря 2022 года стало известно, что ЦБ готов разрешить майнерам продавать криптовалюту только на иностранных биржах. В законопроекте № 237585–8 о регули-

ровании майнинга, который группа депутатов внесла в Госдуму в ноябре, майнерам предлагалось два варианта продажи добытой цифровой валюты: через иностранные системы без соблюдения норм закона о валютном регулировании и через площадку, которая будет создана в России в рамках экспериментального правового режима. В обоих случаях о сделках надо уведомлять ФНС. В настоящее время Банк России поддерживает законопроект о легализации майнинга, но считает, что полученная в результате майнинга цифровая валюта должна продаваться только на иностранных биржах и только нерезидентам.

В соответствии с обсуждаемым законопроектом, майнеры смогут с 1 января 2023 года продавать добытую цифровую валюту как на зарубежных площадках, так и в России в рамках закона об экспериментальных цифровых режимах. Законопроект вводит определения «майнинг цифровой валюты» и «майнинг-пулов». Законопроект также вводит запрет на рекламу (или предложение в той или иной форме) цифровых валют, но при этом делает исключение для майнинга цифровой валюты.

В частности, ограничение рекламы торговли криптовалютой на криптобирже может стать одним из способов повышения защиты потребителей, которые не знакомы с рынком криптовалют. В Сингапуре, несмо-

тря на в целом положительное отношение к криптовалютам со стороны властей, финансовый регулятор в начале 2022 года опубликовал руководство, содержащее ограничение рекламы криптовалют.

Руководство содержит:

- общее указание на то, что торговля криптовалютами не подходит для широкой общественности;
- запрет на создание впечатления о том, что вложения в криптовалюты не столь рискованны;
- запрет рекламы криптовалют в местах общественного пользования (общественном транспорте, публичных мероприятиях, рекламных вывесках и т.п.);
- запрет рекламы криптовалют на сайтах третьих лиц, в социальных сетях, привлечение блогеров и т.д.

С учётом того, что дискуссия по регулированию майнинга в контексте электроэнергетики и экологии в России пока лишь начинается, стоит обратиться к текущим предложениям в иностранных правовых системах. В некоторых из них оптимизации майнинг-деятельности добиваются посредством установления дополнительных ограничений (например, Китай, Иран), а в других – посредством предоставления льгот в случае осуществления определённой бизнес-модели (например, Бразилия, Квебек).

Таблица 3. Сравнение концепций развития законодательного регулирования криптовалют в РФ

Банк России	Правительство РФ
<p>Установить ответственность за нарушение законодательного запрета на использование криптовалют в качестве средства платежа за товары, работы и услуги, продаваемые и покупаемые юридическими и физическими лицами – резидентами РФ.</p> <p>Ввести запрет на организацию выпуска и (или) выпуск, организацию обращения криптовалюты (в т.ч. криптобиржами, криптообменниками, P2P-платформами) на территории РФ и установить ответственность за нарушение данного запрета.</p> <p>Ввести запрет на вложения финансовых организаций в криптовалюты и связанные с ними финансовые инструменты, а также на использование российских финансовых посредников и российской финансовой инфраструктуры для осуществления операций с криптовалютами и установить ответственность за нарушение данного запрета.</p>	<p>Против запрета криптовалют в России, но поддерживает идею регулирования рынка.</p> <p>Проводить операции с криптовалютой в периметре банковской инфраструктуры – это поможет контролировать операции и идентифицировать всех участников.</p> <p>Сделать организаторами системы обмена цифровых валют банки с универсальными лицензиями, которые будут контролировать операции, выявлять незаконные, идентифицировать клиентов и т.д.</p> <p>Использовать сервис «Прозрачный блокчейн» для отслеживания операций в криптовалютой и выявления незаконных транзакций.</p> <p>Создать операторов обмена цифровых валют по модели р2р-обменника (между физлицами) или по модели биржи.</p> <p>Разделить функции надзора между ЦБ, Минфином, Росфинмониторингом, ФНС, Минцифры и Генпрокуратурой.</p> <p>Определить ключевые параметры майнинга криптовалют</p>

Так, в Китае, помимо тотального запрета на использование криптовалюты, власти также вводят повышенные тарифы на электроэнергию для майнинговых предприятий. В ноябре 2021 года Национальная комиссия по развитию и реформам Китая объявила о необходимости оптимизации деятельности государственных промышленных предприятий, участвующих в майнинге. Хозяйствующие субъекты, которые сейчас используют субсидированную электроэнергию для майнинга криптовалют, в будущем могут столкнуться с более высокими тарифами на электроэнергию. Комиссия намерена изучить возможность взимания «карательных» тарифов в рамках превентивных мер. Вслед за общенациональным регулятором в декабре 2021 года Комиссия по развитию и реформам провинции Хайнань опубликовала документ, который установил повышенный тариф на электроэнергию для предприятий по добыче криптовалюты в размере 0,8 юаня за киловатт-час, в то время как стандартная цена на электроэнергию составляет около 0,6 юаня за киловатт-час. Бразильский Конгресс рассматривает предложение по освобождению от пошлин на ввоз оборудования для майнинга криптовалют, а также от налогов на майнинговую деятельность, если используются возобновляемые источники энергии. В Нидерландах, если майнинг осуществляется в значительных масштабах и требует существенного количества энергии, такая деятельность нуждается в обеспечении дополнительной безопасности. Кроме того, в случае превышения нормы выбросов в окружающую среду для осуществления майнинга криптовалют могут потребоваться соответствующие разрешения, например, экологическое разрешение.

Минэкономразвития России, в свою очередь, указывает на целесообразность разрешить майнинг криптовалют в регионах, имеющих устойчивый профицит генерации электроэнергии. Также рассматривается перспектива установления порогового значения использования электроэнергии для её потребления физическими лицами (социальной нормы потребления). В итоге майнеры, потребляющие большие объёмы электроэнергии и превышающие установленную норму, будут платить по повышенному тарифу. Основной проблемой в текущей повестке яв-

ляется поиск баланса между стимулированием эффективной майнинговой деятельности и оптимизацией уровня потребления электроэнергии.

В целом к значительным недочётам правового регулирования криптовалюты следует отнести: законодательную неопределённость в понятии «криптовалюта»; двоякость применения (одни суды говорят, что криптовалюта является имуществом, другие – что не является, ссылаясь на её обезличенность и отсутствие как вещи в натуре); невозможность возмещения ущерба из-за того, что нельзя наложить арест на криптовалюту; уголовно-правовые риски инвесторов и самих криптобизнесменов (все участники сделки с криптоактивами могут пострадать от интересов правоохранителей).

Первостепенные направления развития законодательства в сфере оборота криптовалют обозначены в Концепции. Причём там идёт речь не только о внесении поправок в уже действующий Закон № 259-ФЗ, но не исключается и разработка нового федерального закона. Кроме того, предусмотрено рассмотрение и доработка следующих законопроектов:

- о декларировании сведений по операциям с использованием цифровой валюты в сумме более 600 тыс. руб. и установлении налоговой ответственности за непредставление в налоговые органы информации об обороте средств и об остатке цифровой валюты, за неуплату налога по операциям с использованием цифровой валюты;
- о введении административной ответственности за организацию незаконного оборота цифровых финансовых активов и нарушение правил совершения сделок с ними, а также за организацию незаконного приёма цифровой валюты в качестве встречного предоставления: рассмотрение дел об административных правонарушениях, а также составление протоколов в сфере незаконного оборота цифровых финансовых активов в рамках законопроекта отнесено к компетенции Банка России, а в сфере незаконного оборота цифровой валюты – к компетенции ФНС России;
- об установлении ответственности за уклонение от обязанности де-

кларирования сведений об операциях, связанных с использованием цифровой валюты, и отнесении использования цифровой валюты при совершении преступления к обстоятельству, отягчающему наказание;

- об обязанности субъектов противодействия отмыванию денежных средств и финансированию терроризма направлять в Росфинмониторинг информацию об операциях с цифровыми валютами.

Отсутствие единых регуляторных стандартов и связанная с этим неопределённость являются одними из основных сдерживающих факторов для всеобщего принятия криптовалюты. Технология распределённого реестра по-прежнему вызывает ряд вопросов у регулирующих органов и политиков на национальном и международном уровне. Из-за проблем со стандартизацией и функциональной совместимостью нормативный статус криптовалюты остаётся неопределённым, и это является основным сдерживающим фактором для роста. Так, в 2021 году Китай запретил оборот криптовалют, из-за чего все жители страны были обязаны в короткие сроки вывести все средства с криптобирж. Пожалуй, главной проблемой, которая повсеместно мешает регулирующим органам дать криптовалютам легальный статус, остаётся беспокойство по поводу безопасности, конфиденциальности и контроля. Тот факт, что криптовалютные транзакции и данные платежей отражаются в блокчейн-сети, не только гарантирует сохранность и достоверность информации об этих транзакциях, но и создаёт риски хакерских атак и взломов. Также серьёзной проблемой внедрения криптовалютных платежей является вопрос конфиденциальности в распределённом публичном реестре. Но эксперты уверены, что принятие общих правил сделает как использование криптовалют, так и инвестиции в них намного безопаснее. Особенно полезными стандартами станут для долгосрочных инвестиций.



Пресс-центр Группы «ДЕЛОВОЙ ПРОФИЛЬ»

+7 (495) 740 16 01

Pashkevich@delprof.ru

CIS TV

ИТ-НОВОСТИ

Новостной ИТ-канал
о цифровых и информационных
технологиях в России



 YouTube

CIS – Современные Инфосистемы
www.cis.ru

Главная ценность СИГМА.Академии – знания наших экспертов

В ИТ-компании «СИГМА» есть внутреннее подразделение, нацеленное на работу со студентами и привлечение молодых специалистов, – СИГМА.Академия. Руководитель Академии Александр Ерошкин рассказал о проекте, работе со стажёрами и тенденциях в сфере ИТ-образования.

Над чем сейчас работает СИГМА.Академия, что стоит в приоритете?

Как и всегда, Академия сейчас нацелена на приём стажёров. Основная наша задача – найти, подготовить и принять к себе самых толковых ребят. Работа продолжается круглый год, к нам по-

стоянно поступают заявки от производственных департаментов. Запрос на стажёров есть в разных городах присутствия СИГМЫ.

Сейчас у нас параллельно ведутся несколько курсов:

- «Управление ИТ-проектом»;
- «Управление требованиями»;
- «Проектирование дизайна».

Также важной задачей является организация обучения наших специалистов – сотрудников СИГМЫ. Мы предоставляем возможность дополнительного профессионального образования и получения дипломов по повышению квалификации по 13 направлениям.

Какое направление Академии чаще всего выбирают студенты? Как Вы думаете, почему?



Александр Ерошкин
Руководитель Академии

Самые популярные направления – «Разработка и Внедрение» и «Системная и бизнес-аналитика». Разработку и внедрение хотят изучать, потому

что это одно из самых перспективных направлений на сегодняшний день. Особенно если пишешь код вручную, умеешь программировать и разбираешься в сфере приложений. И в разработке чаще встречаются интересные и технически сложные задачи.

Направление «Системная и бизнес-аналитика» популярно среди студентов, потому что содержит в себе технические знания и коммуникативные навыки. Аналитики общаются с заказчиком, собирают требования, пишут технические задания и являются «переводчиком» с языка заказчика на технический язык, который будет понятен разработчику. В аналитике очень важно сочетание таких качеств, как точность, аккуратность и навыки коммуникации.

Меняется ли программа обучения в связи с какими-то новыми трендами в сфере ИТ?

Постоянно меняются и сами курсы, и их содержание. Каждый год учебные программы дорабатываются в связи с изменившимися обстоятельствами. В прошлые годы, например, мы во многом опирались на зарубежное программное обеспечение по управлению и разработке проектов. Сейчас упор идёт на отечественное ПО.

Что бы Вы посоветовали студентам при выборе направления в Академии?

В вузе студент должен определить, какие предметы нравятся ему больше всего. Это поможет выбрать действительно интересное ему направление. Следующий шаг: перед тем, как идти на курсы, стоит изучить направление – его особенности и профессиональные обязанности. Но полностью понять специфику получится уже в ходе стажировки. В это время студент узнаёт, что его ждёт, подходит ли ему это направление, завязывает первые рабочие связи в мире ИТ и по-настоящему погружается в профессию.

Расскажите подробнее о специалистах, которые преподают в СИГМА Академии. Как подбираете нужных людей? Что самое важное при выборе преподавателя?

Основной пул преподавателей – эксперты нашей компании. Ведь самая главная ценность в образовании от Академии – практические знания экспертов, которые ежедневно сталкиваются с теми или иными задачами в работе. Основное требова-

ние – наличие желания поделиться своими знаниями. Мы постоянно объявляем о наборе на курсы, и к нам в инициативном порядке обращаются эксперты. Большое спасибо им за вклад в работу нашего подразделения! Другая часть преподавателей – штатные сотрудники Академии.

Привлекаете ли Вы экспертов из других ИТ-компаний для проведения дополнительных лекций или мастер-классов?

На сегодняшний день такой практики нет. Мы акцентируем внимание на том, что делимся опытом «СИГМА». Наш основной вектор – специализированные курсы, по окончании которых человек приобретает квалификацию.

Какие тенденции в сфере ИТ-образования Вы можете выделить на данный момент?

ИТ-образование отталкивается от базовых аксиом:

1. ИТ-рынок развивается очень быстро, и вузы не успевают готовить такое количество специалистов, которые требуются компаниям.
2. Технологии – языки программирования, фреймворки – тоже очень быстро меняются, и образовательный стандарт никогда за ними не успеет. Академическое образование инертно. Но тенденция такова, что университеты всё же идут в сторону большей гибкости. Для студентов открываются больше специальностей, дополнительных спецкурсов, преподаются предметы по выбору.
3. Ещё одна тенденция – огромное количество коммерческих курсов, которые быстро, за пару месяцев, обещают дать какие-то основы в сфере ИТ. Я считаю, если учиться с нуля, нужно поступать в университет. Никакие курсы не дадут базы. А если выбирать самообразование, должна быть огромная самодисциплина на годы вперёд.

Есть ли у Академии явные конкуренты?

Конечно, СИГМА Академия появилась далеко не первой. Компания «Ланит» более 20 лет осуществляет учебную деятельность в рамках своей академии. Есть крупная школа у «Сбербанка». «Лукойл» хоть и не относится напрямую к ИТ-сфере, является хорошим примером коммерческой компании, которая осуществляет образовательную дея-

тельность. Однако ни одна из данных академий не сфокусирована на специфике энергетики, а в этой отрасли есть большая потребность в ИТ-кадрах. Поэтому здесь у «СИГМА» есть неоспоримое преимущество.

Какие партнёрские программы есть у Академии?

Основные целевые организации, с которыми мы сотрудничаем, – университеты с ИТ-направлениями. Это СПбГЭТУ «ЛЭТИ», СПбГУ, СПбПУ Петра Великого, НИТУ «МИСИС», ОмГТУ и не только.

Есть ли у Вас любимый проект, созданный студентом?

У нас ведётся групповая разработка, в рамках Академии есть несколько открытых проектов, которые мы даём студентам в работу. Какой-то один выделить сложно. Если говорить о пройденном пути, есть ряд студентов, которые отлично себя проявили.

Можете рассказать об истории успеха студента, прошедшего стажировку в Академии?

Как я ранее упомянул, таких примеров немало. Артём Великанов – талантливый парень, предельно мотивированный, устроился к нам на летнюю практику после 3-го курса в качестве младшего разработчика. Он много работал, выполнял серьёзный объём задач и вскоре благодаря своему усердию стал подниматься по карьерной лестнице. На сегодняшний день Артём является тимлидом в Департаменте разработки бизнес-приложений. Также сразу несколько аналитиков, прошедших стажировку в «СИГМЕ», замечательно себя проявили и стали на постоянной основе работать в Департаменте биллинговых решений.

Сотрудник Академии Александра Лончина изначально пришла в качестве преподавателя практики. Увидев уровень её знаний и работы, я пригласил Александру в компанию. Сейчас она сама разрабатывает курсы.

Автор интервью: Екатерина Васюткина.



Компания «СИГМА»

www.sigma-it.ru

Учебный курс по продукту JMS 3.7

Цель данного курса – познакомить слушателей с системой управления жизненным циклом ключей и смарт-карт JaCarta Management System версии 3.7 от компании «Аладдин Р. Д.».

Задачами курса являются:

- сделать обзор ключевых носителей, производимых компанией «Аладдин Р.Д.»;
- познакомить слушателей с жизненным циклом ключевых носителей;
- показать процесс развёртывания JMS;
- познакомить слушателей с ключевыми настройками JMS;
- разобрать основные сценарии работы JMS;
- познакомить слушателей с процессом технического сопровождения JMS после внедрения.

Объединяя опыт



СОБИНТЕГРА

«Современная Интеграция»

- Проектирование
- Внедрение
- Разработка документаций
- Сопровождение

CIS Современные Информационные Системы

«Современные Инфосистемы»

- Разработка авторских курсов
- Проведение курсов
- Чтение авторских курсов

Курс по JaCarta Management System

- Разработан опытными тренерами
- В соавторстве с инженерами-практиками
- На основе реальных кейсов
- Полнота учебного материала
- Содержательные лабораторные работы
- Разбор практический кейсов
- Лайфхаки от практиков

Содержание курса

1. Введение в курс «Система управления жизненным циклом ключей и смарт-карт JaCarta Management System 3.7».
2. Обзор ключевых носителей.
3. Жизненный цикл ключевого носителя.
4. Архитектура и варианты развёртывания JMS.
5. Развёртывание JMS.

*Лабораторная работа №1.
Развёртывание сервера JMS.*

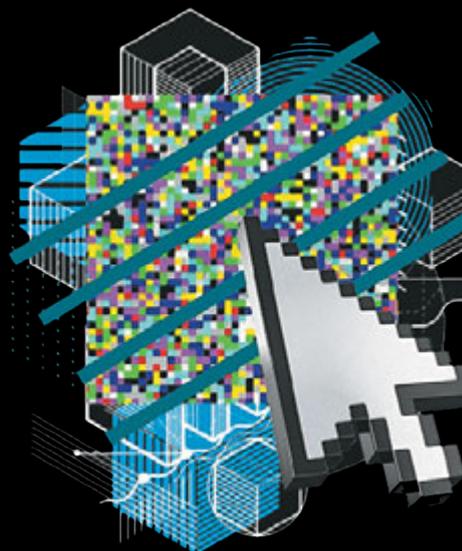
6. Интерфейс сервера JMS.
7. Интерфейс консоли управления JMS.
*Лабораторная работа №2.
Настройка JMS для выпуска цифрового сертификата с Microsoft CA.*
8. JMS клиент.
9. Типовые задачи сопровождения.



Учебный комплект

В учебный комплект входят следующие материалы:

- данное учебное пособие;
- ключ JaCarta PKI в формфакторе XL;
- ключ JaCarta PKI в форм-факторе Nano



Требования к слушателям курса

Слушатели курса должны обладать следующими знаниями и навыками:

- знание Windows Server 2012 или выше на уровне продвинутого пользователя, что включает понимание принципов:
 - работы домена Windows (Active Directory);
 - работы центра сертификации Microsoft (MSCA);
- построения инфраструктуры открытого ключа (Public Key Infrastructure – PKI);
- знание Windows 10 на уровне пользователя;
- знание и понимание принципов работы MS SQL Server 2014.



Контакты и запись

По завершению обучения вам выдадут именную сертификат о прослушивании курса по JaCarta Management System.

С вопросами и предложениями можно обратиться, написав на электронный адрес education@cis.ru.

Лицензия департамента образования и науки города Москвы № 041137 от 30 ноября 2020 года.



education@cis.ru

www.cis.ru

Блиц-опрос среди ИТ-специалистов

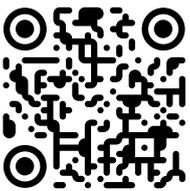
Редакция ИТ-журнала CIS провела ежегодный блиц-опрос среди ИТ-директоров и руководителей в этой сфере. Цель опроса – узнать мнение экспертов о перспективах развития сферы информационных технологий в 2023 году в России.

ActiveCloud



Сергей Крутилин
Генеральный директор ActiveCloud в России

Active CLOUD



activecloud.com

Какая область ИТ будет наиболее интересной и знаковой в 2023 году в стране?

Не вызывает никаких сомнений: потребность в облаках растёт сегодня и продолжит расти в 2023 году. Происходит это параллельно росту проблем, связанных с заменой «железа» и ПО. Например, стоимость серверного оборудования, начиная с февраля 2022 года, неуклонно повышается, и та цена, которую все имеют сейчас, – ещё не предел. У всех сегментов бизнеса, включая крупнейших компаний из рейтинга Forbes 200, есть свои объёмы и сроки поставок. Дистрибьюторы стараются не давать гарантий в датах поставки. Как следствие, компании вынуждены рассматривать альтернативы закупкам в собственность, и в этом вопросе граница между малыми и крупными предприятиями размывается. Облака – самый очевидный путь к поддержанию необходимого уровня SLA-работы бизнес-процессов для любой организации.

Рост потребности в облачном консалтинге – второй тренд, который укрепился в 2022 и наверняка перейдёт в 2023 год. Рынок испытывает острый дефицит кадровых ресурсов для реализации инфраструктурных проектов. Нехватка внутренней экс-

пертизы приводит к тому, что заказчику нужна не просто облачная инфраструктура, состоящая из виртуальных машин, дискового пространства и облачных сервисов. Нужны те, кто поможет мигрировать в облако, объединить локальную инфраструктуру с облачной, поддержит выстроенные сервисы в дальнейшем. Этот ресурс есть у облачных провайдеров, и мы готовы им делиться.

Третий момент – облачные провайдеры всё чаще получают запросы на комплексные проекты, продают сразу облачную инфраструктуру «под ключ» и облачный консалтинг, и эта тенденция тоже сохранится. Поскольку ресурсы ИТ на стороне клиентов сокращаются, независимо от того, реализуется проект локально в облаке или в гибридной инфраструктуре, заказчикам целесообразнее привлекать подрядчиков в рамках «одного окна».

В какой области ИТ в этом году следует ожидать интересных открытий и достижений?

Российские вендоры получили отличный шанс на собственное развитие под текущие потребности клиентов в РФ, которые раньше использовали иностранные решения. С одной стороны, это даст возможность компаниям в РФ избавиться от зависимости в иностранных решениях, с другой – даст безграничные возможности российским разработчикам на развитие.

В чём сильные стороны российских ИТ-компаний и специалистов на мировой арене?

Российские ИТ-компании нацелены на модель – «один сотрудник может многое», в то время как иностранные коллеги используют модель – «один сотрудник выполняет только одну задачу». Взаимозаменяемость персонала в ИТ-компаниях России – наше кардинальное отличие от западных компаний. Это стандарт де-факто, и это очень ценится иностранными заказчиками, которые понимают, что поставленную задачу российские ИТ-компании решат в сжатые сроки и с минимальным бюджетом по сравнению с локальными игроками.

Для развития каких технологий и проектов в России имеется благодатная почва?

Сейчас нет каких-либо ограничений. По сути, есть возможность для развития абсолютно любой технологии в отсутствие уже сформированных решений от иностранных компаний. Раньше во многих областях были монополисты, развивать те или иные решения не имело особого смысла. Сейчас же, когда монополисты определённых ИТ-сегментов ушли с нашего рынка, у многих российских разработчиков появилась уникальная возможность развития, которой у них раньше не было.

На какие аспекты развития технологий (ИТ, ИБ) сейчас следует сделать акцент государству?

Нужна консолидация и координация дальнейшего развития. У всех участников рынка (ИТ-компаний, государства, потребителей решений) должна быть общая дорожная карта развития отрасли. Например, если в 2024 году станет обязательным офисный формат ODF для всех типов компаний (коммерческие, образовательные, государственные), то, безусловно, это даст импульс в сторону перехода на этот формат все-

ми участниками рынка и выработки общих подходов вокруг экосистемы продуктов, которые данный формат будут развивать или поддерживать.

В каких сферах бизнеса по вашему мнению в стране ИТ-технологии развиты достаточно высоко, а в каких оставляют желать лучшего? В чём причина?

Ритейл, а в частности онлайн-бизнес, сейчас имеет наиболее развитый стек технологий. Наряду с высокотехнологичными облачными провайдерами, онлайн-бизнес вынужден быть постоянно в тренде, что побуждает эту отрасль всегда быть на пике технологий. Сейчас можно заказать товар или услугу множеством способов: через соцсети, в приложении, по телефону, на сайте, в офлайн-магазине или на термине – все эти каналы сбыта необходимо как-то консолидировать, а для этого без современных технологий не обойтись.

На что будет делать ставку ваша компания для дальнейшего развития в 2023 году?

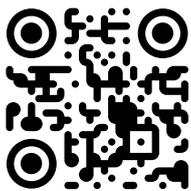
В 2023 году компания ActiveCloud будет помогать клиентам развивать их бизнес путём снижения затрат на серверное оборудование и предоставлять аналоги иностранных решений в облаке для оперативного запуска новых цифровых сервисов, которые развивают наши клиенты.

На данный момент, есть уверенность, что рынок Cloud в 2023 году продолжит активный рост. В условиях дефицита оборудования и компетенций тренд перехода на российские облака уверенно набирает силу. Все сложности преодолимы, если стремиться к развитию, быть проактивными и искать силу в консолидации.

Group-IB



Валерий Баулин
Генеральный директор Group-IB в России и СНГ



group-ib.com

Какая область ИТ будет наиболее интересной и знаковой в 2023 году в стране?

Разумеется, на наш взгляд, наиболее востребованной и интересной отраслью в текущем году будет информационная безопасность. Почему именно она? Ответ простой: в 2022 году российские компании столкнулись с небывалой волной кибератак как со стороны прогосударственных хакеров и хактивистов, так и киберкриминала. На порядок выросло количество атак программ-вымогателей, рассылок вредоносных программ, DDoS, утечек баз данных, фишинга и скама. Это «киберцунами» бушевало на фоне ухода из России зарубежных вендоров, и многие их решения защиты без технической поддержки превратились в кирпич.

В 2023 году, я уверен, и Group-IB, и всю сферу информационной безопасности ждёт ещё больше работы. Прошлый год чётко показал многим заказчикам, что огромное количество используемых ими решений бесполезны, поскольку не укомплектованы технологиями сканирования даркнета, не сопоставляют атаку и атакующего, не имеют предикативной аналитики и не позволяют строить собственную картину киберугроз для каждой отдельно взятой компании. Поэтому вырос спрос на системы Threat Intelligence (Киберразведка) и решений MXDR для предотвращения сложных целевых атак, проактивного поиска недетектируемых угроз и реагирования на выявленные инциденты. Этот рынок переживает по факту «второе рождение».

В какой области ИТ в этом году следует ожидать интересных открытий и достижений?

Думаю, что мы увидим прорывные решения из сферы машинного обучения и искусственного интеллекта (далее – ИИ) применительно к информационной безопасности. Мы уже давно используем эти наработ-

ки в решениях Group-IB Fraud Protection и Group-IB Digital Disk Protection. Наш опыт показывает, что ИИ может предотвращать киберпреступления ещё на этапе их подготовки: искать и анализировать огромные массивы самой разнообразной информации (цифровые отпечатки устройств, графические данные, технические индикаторы и т.д.), выявляя скрытую активность, связи и предупреждая наших клиентов о готовящихся преступлениях. Если говорить о достижениях в условиях ухода зарубежных вендоров, то у российских вендоров есть шансы частично заместить некоторые иностранные решения или запустить продукты, не имеющие аналогов на международных рынках.

В чём сильные стороны российских ИТ-компаний и специалистов на мировой арене?

Одна из сильных сторон российских ИТ-компаний – специалисты. Наши разработчики создают уникальные решения и технологии, которые успешно могут конкурировать на глобальных рынках. И в этом нельзя отрицать значение нашего академического образования. Хотя в нашей сфере есть мнение, что кибербезопасности не учат: исключительно практика даст необходимые знания и навыки для изучения киберкриминала, реагирования на инциденты, цифровой криминалистики. Мы меняем этот подход, и в 2022 году открыли на базе ИТ-центра МАИ Лабораторию информационной безопасности Group-IB. Это шаг к тому, что буквально со студенческой скамьи высококвалифицированные специалисты смогут работать с самыми современными решениями для детектирования и предотвращения кибератак. Мы рассчитываем, что такие Лаборатории в дальнейшем будут открыты на базе всех ключевых ведущих российских вузов. Кроме МАИ, совместная магистерская программа действует сейчас в МФТИ, а тренеры Group-IB читают лекции и ведут практические занятия в МГТУ им. Н.Э. Баумана, Высшей школе экономики и других ВУЗах.

Для развития каких технологий и проектов в России имеется благодатная почва? Какие факторы наиболее влияют на это?

Исходя из опыта, сейчас в России растёт спрос на наши облачные «лёгкие» решения Group-IB Attack Surface Management (полный контроль внешней поверхности атаки) и Group-IB Business Email Protection (локальная и облачная защита электронной почты от сложных киберугроз), которые не требуют от региональных компаний больших бюджетов. Всё более востребованными также становятся сервисы аудита и пентеста, особенно Read Teaming, реагирования на инциденты Incident Response.

У российских вендоров есть возможности создавать решения и продукты не хуже, чем у «чемпионов» международного кибербезопасности, а в некоторых сегментах и лучше. В этих условиях отечественные разработчики, интеграторы ИБ-решений стали кооперироваться, договариваться, вместе развивать партнёрский рынок и создавать безопасную инфраструктуру. Коллаборация даёт преимущество, когда рынку нужна реальная эффективность продуктов.

На какие аспекты развития технологий (ИТ, ИБ) сейчас следует сделать акцент государству?

Именно сейчас закладываются правила игры и регуляторика, по которым российская ИТ-отрасль и особенно сфера информационной безопасности будет существовать ближайшие годы. Должен быть закреплён переход от «бумажной» безопасности к практической, а иностранные вендоры замещены российскими. Появление любой нормотворческой инициативы в области ИБ фокусирует внимание общества на вопросах безопасности цифровой среды, и это позитивно влияет на рынок в целом.

Но всё-таки переводение нормативных требований в практическую реализацию – зона ответственности компаний, а не регулятора. И тут в первую очередь от компаний

требуется уход от слепого выполнения требований регулятора, переформатирование существующих требований законодательства в практические шаги, позволяющие выявлять атаки, своевременно реагировать и восстанавливать инфраструктуру после инцидентов, количество которых с учётом меняющегося ландшафта угроз будет только расти.

На что будет делать ставку ваша компания для дальнейшего развития в 2023 году?

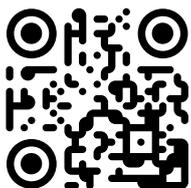
Наша миссия не менялась с момента основания компании в 2003 году – это борьба с киберпреступностью. Мы предотвращаем потенциальные атаки и реагируем на реальные инциденты, чтобы создать благоприятные условия для наших клиентов и помочь их бизнесу развиваться. Нам не важна география, происхождение злоумышленников или объект атаки – мы боремся с киберпреступностью во всех её проявлениях. Мы постоянно совершенствуем наши технологии, продукты и услуги, чтобы проактивно бороться с киберпреступниками. Мы вкладываемся в создание центров исследований и привлечение талантов. Поддерживая нас, наши клиенты также помогают развитию безопасной киберкультуры в России и СНГ.

Цель Group-IB – обеспечить надёжный уровень защиты любому типу бизнеса по всей стране. Абсолютно любая компания, организация, предприятие может стать жертвой проправительственных хакерских групп, хактивистов, финансово мотивированных киберпреступников. Для этого мы будем продолжать активно развивать сотрудничество с партнёрами в российских регионах, где, кстати, проявляется очень большой интерес к отечественным услугам и сервисам кибербезопасности.

NordClan



Каштанкин Илья Александрович
Директор
ООО «Норд Клан»



nordclan.com

Какая область ИТ будет наиболее интересной и знаковой в 2023 году в стране?

После того, как рынок покинули зарубежные вендоры, сохранится тренд на импортозамещение. Если раньше этот процесс был хаотичным и компании стремились заместить ПО, необходимое для ежедневной работы, то теперь процесс станет более стабильным и ориентированным на информационную безопасность.

Продолжится цифровизация типовых бизнес-процессов. Раньше разработкой собственного ПО интересовались в основном крупные компании, сейчас от коробочных решений в сторону собственных продуктов уходят всё больше представителей среднего и малого бизнеса.

Однако самой интересной областью станет развитие ИИ-технологий и их внедрение в повседневную жизнь. Лидеры цифровизации финтех, ритейл и телеком уже добавили умные технологии в банковские приложения и алгоритмы поиска товаров. Скорее всего, их примеру последуют другие сегменты экономики.

В какой области ИТ в этом году следует ожидать интересных открытий и достижений?

Из-за роста интереса к цифровизации бизнес-процессов можно будет наблюдать за появлением интересных решений в области автоматизации рабочих мест или использования виртуальных решений для удалённого формата работы.

Несмотря на то, что после потрясений последних лет ИТ-отрасль будет сосредоточена больше на планомерном процессе импортозамещения привычных цифровых решений, будем надеяться, что мы увидим новый функционал на основе искусственного интеллекта и нейросетей.

Также, учитывая интерес к внедрению технологий в медицинский сектор и рост инвестиций в медтех-отрасль, есть вероятность выпуска на рынок новых цифровых решений. Возможно, мы увидим продукты с использованием технологий машинного обучения или речевых роботов, например в области диагностирования заболеваний или консультации пациентов.

В чём сильные стороны российских ИТ-компаний и специалистов на мировой арене?

Российские ИТ-компании после событий 2020–2022 гг. закалились и стали намного быстрее приспосабливаться к изменениям внешней среды.

В некоторых отраслях (например, финтех) экспертиза российских разработчиков опережает многих цифровых лидеров по всему миру. Уровень цифрового банковского сервиса у нас один из лучших в мире.

Следующая интересная отрасль – промышленность. Опыт ИТ-компаний на стыке технических и промышленных знаний заинтересует многие зарубежные компании, учитывая общемировой тренд «новой индустриализации».

Для развития каких технологий и проектов в России имеется благодатная почва? Какие факторы наиболее влияют на это?

Назрел вопрос замены импортных платформенных решений, которые стали недоступны из-за санкций. Логично, что сейчас идёт процесс развития собственных российских платформ, которые станут лидерами по использованию отечественным бизнесом. Глобально с этой задачей могут справиться вендоры и интеграторы, способные работать совместно над созданием крупных цифровых экосистем.

Особенно интересны свободные слоты в области офисного ПО, промышленной автоматизации, решений для торговли и логистики. Это связано с уходом с рынка основных иностранных ИТ-поставщиков. Сейчас есть возможность легко занять ниши, которые раньше нужно было завоёвывать годами. Вероятно, в 2023 году мы услышим новые громкие имена в ИТ-сфере.

Продолжат своё развитие мобильные технологии. В предыдущем тренде супераппов лидерство поделили крупные игроки рынка, теперь интерес может сместиться в сторону приложений для умного дома.

По прогнозам аналитиков, рынок умных устройств для дома в России вырастет вдвое – до \$ 2,7 млрд к 2025 году. Бытовые устройства, управляемые с телефона, уже не новость, однако теперь могут понадобиться решения, которые объединят их в удобную экосистему.

На какие аспекты развития технологий (ИТ, ИБ) сейчас следует сделать акцент государству?

Отметим повышение суверенитета в области ключевых цифровых технологий. Об этом говорит тот факт, что в бюджете России на 2023 год заложено более 1,7 трлн рублей на технологическую независимость.

В условиях активного развития импортозамещающих цифровых продуктов стоит позаботиться о безопасности данных. Учитывая популярность облачных сервисов, необходим качественный сервис в области кибербезопасности.

Защита цифровых данных – это общемировой тренд. Это подтверждает исследование компании «Ростелеком» о глобальных трендах цифровизации: «Совокупный объём инвестиций в технологии обезличивания данных в 2021 году вырос на 193%».

Также с 1 января 2025 года государственным органам будет запрещено использовать иностранное ПО на объектах критической инфраструктуры. Возможно, стоит разработать меры поддержки для компаний, которые участвуют в госзаказах на разработку цифровых систем.

В каких сферах бизнеса, по вашему мнению, в стране ИТ-технологии развиты достаточно высоко, а в каких оставляют желать лучшего? В чём причина?

Традиционно лидерство удерживают финтех, ритейл и телеком. В основном из-за того, что население страны ежедневно использует цифровые решения из этих сегментов. К то-

му же пандемия вызвала бум в онлайн-торговле, и даже с окончанием изоляции люди продолжили использовать удобные инструменты для покупок и доставки.

Из слабо развитых областей отметим отсутствие широкого производства электронных компонентов – от этого страдают производственные ИТ-мощности. Из-за ухода иностранных игроков сегмент освободился. И, хотя у российских производителей есть шанс усилить эту сферу собственными разработками, большинство компаний переориентировались на закупки в дружественных странах. Скорее всего, этот сегмент не будет развиваться, пока не будут разработаны меры стимулирования отрасли со стороны государства.

Также сейчас весь мир продолжает идти к Индустрии 4.0. В России не все производственные компании достаточно развили цифровую грамотность, чтобы активно внедрять цифровые решения. Отчасти это связано с дополнительными инвестициями в переобучение персонала на работу в новых цифровых системах, и не всем компаниям пока очевидно, насколько экономически выгодна подобная трансформация.

На что будет делать ставку ваша компания для дальнейшего развития в 2023 году?

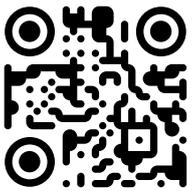
Компания «Норд Клан» продолжит развитие своей линейки продуктов и услуг. Поддержим тренд импортозамещения: 3 наших собственных продукта уже зарегистрированы в реестре отечественного ПО. Сфокусируемся на масштабировании успешного направления компьютерного зрения и нейросетей. А также продолжим поставлять все более качественный сервис в области разработки ПО и мобильных приложений.

Axoft



Сергей Игнатов
Директор
по развитию
продуктовых
направлений
компании Axoft

AXOFT



axoftglobal.ru

Какая область ИТ будет наиболее интересной и знаковой в 2023 году в стране?

На мой взгляд, перерождение отечественной промышленности продолжит стимулировать дальнейшее развитие и внедрение технологий в области цифровизации предприятия: автоматизация проектирования и производства, управление проектной деятельностью и жизненным циклом изделий, а также системы защиты АСУ ТП.

Что касается сетевой безопасности, то, уверен, мы увидим ряд новых сильных решений, которые заменят ушедших разработчиков. Кроме того, направление безопасной разработки эксплуатации приложений (DevSecOps) получит дополнительный толчок как со стороны государства, так и со стороны новых игроков на рынке.

Для развития каких технологий и проектов в России имеется благодатная почва? Какие факторы наиболее влияют на это?

На данный момент мы наблюдаем несколько позитивных тенденций на ИТ-рынке, которые могут послужить катализатором для технологического рывка:

- Цифровизация, ускоренная миграция на российские решения и дефицит квалифицированных кадров подталкивает компании к применению гиперавтоматизации в ИТ, информационной безопасности, бизнесе и производственных процессах (RPA, Low/No Code, BPM, AIOps, OSS/BSS, SOAR, BAS). Технологии с применением ИИ позволяют выстраивать сервисы самообслуживания на предприятиях и снижать нагрузку на специалистов.
- Искусственный интеллект (AI), машинное обучение (ML), Big Data, сенсорика, компьютерное зрение (CV), система обработки естественного языка (NLP) – всё меньше предлагаются как точечная и заказная разработка и становятся встроенными в тиражируемые продукты для аналитики, управления и принятия решений (Decision Intelligence). Отечественные разработчики стремятся использовать данные технологии, и в этом их активно поддерживает государство.
- Большое разнообразие производителей с фрагментарными продуктами, которые оста-

лись после ушедших экосистемных иностранных корпораций, формируют потребность в развитии зонтичных систем мониторинга и управления (оркестрации) физическими и облачными инфраструктурами. В это же время технологии контейнеризации и Cloud-Native Platforms позволяют выстраивать максимально гибкую гибридную среду для приложений и микросервисов на предприятиях.

Безусловно, благотворными факторами для дальнейшего развития технологий продолжит являться всяческая поддержка от государства для стартапов, малого и среднего бизнеса. И, конечно, всеобщее стремление всех участников ИТ-рынка достичь мирового уровня цифровой зрелости российской промышленности.

На какие аспекты развития технологий (ИТ, ИБ) сейчас следует сделать акцент государству?

На данный момент не все решения ушедших вендоров замещены. В первую очередь, следует обратить внимание на развитие отечественных продуктов в части классов ИБ-решений, по которым существуют жёсткие требования регуляторов. Согласно указу № 250 «О дополнительных мерах по обеспечению информационной безопасности РФ», все объекты КИИ обязаны перейти на отечественный софт с 1 января 2025 года. Это подразумевает, что организации должны использовать российское ПО в полном объёме на всех этапах. Но аналогов по ряду решений, которые попадают под данное постановление, ещё нет.

В части ИТ стоит сделать фокус на количестве отечественных операционных систем, сейчас их уже более 40. Минкомсвязи РФ планирует определить перечень основных ОС, с которыми каждый вендор должен будет протестировать своё ПО на совместимость. Пока (в большинстве случаев) такие мероприятия не проводятся.

На что будет делать ставку ваша компания для дальнейшего развития в 2023 году?

Основные направления, на развитии которых мы сосредоточимся в 2023 году, включают следующие технологические практики: цифровизация производства, управление данными, вычислительная и сетевая инфраструктура, DevSecOps, бизнес-продуктивность, автоматизация ИТ- и ИБ-процессов.

Аурига

Какая область ИТ будет наиболее интересной и знаковой в 2023 году в стране?

По моему мнению, наиболее перспективной в 2023 году в России должны стать разработка и внедрение интеграционных решений. В настоящее время происходит вынужденный поиск потенциальных замен информационных систем во всех отраслях. Из-за ухода западных вендоров, почти полностью контролировавших этот рынок, многие ИС перестали работать, и компаниям требуется аварийный переход на новые продукты. Это напоминает разбитое зеркало, которое необходимо быстро склеить, чтобы сохранить работоспособность. Позднее в России будет создаваться полная технологическая цепочка от инструментов разработки через мелкие библиотеки к крупным фреймворкам и законченным отечественным решениями. Это потребует не только времени, но и осознанного финансирования и выращивания кадров.

В какой области ИТ в этом году следует ожидать интересных открытий и достижений?

Сейчас не время для прорывных достижений. Задача номер один – обеспечить работоспособность тех продуктов, которые уже развёрнуты. Открытия, несомненно, появятся позднее, когда наберётся достаточное количество новых отечественных разработок и компании введут их в стабильную эксплуатацию.

В чём сильные стороны российских ИТ-компаний и специалистов на мировой арене?

«Аурига» работает на рынке высоких технологий больше 30 лет. Мы были фактически одной из первых российских компаний-разработчиков, вышедших на рынок софтверных услуг на Западе. За эти годы мы выполнили сотни и сотни технологически сложных комплексных проектов. Мы на своём опыте убедились в надёжности российских инженерных традиций. Наши инженеры практичны, прекрасно образованы в математике и физике и поэтому особенно сильны в создании решений для управления реальными физическими объектами.

Для развития каких технологий и проектов в России имеется благодатная почва? Какие факторы наиболее влияют на это?

Я считаю, что наиболее благоприятный момент сейчас сложился для развития систем управления технологическим процессом про-

изводства. Современный завод не может работать без комплексных информационных систем ведь без отлаженного производственного процесса нет готовой продукции.

Кроме этого, системы в системообразующих областях – финансы, госуправление и связь, нуждаются в обновлении и переходе на решения, которые надо разрабатывать уже сейчас. Это вопрос выживания нашего государства.

Основной фактор развития этих проектов – необходимость быстрого перехода на импортонезависимые продукты, поскольку западные поставщики с рынка ушли.

На какие аспекты развития технологий (ИТ, ИБ) сейчас следует сделать акцент государству?

Государству сейчас необходимо сделать акцент на поддержку развития сферы инструментального ПО – ассемблеров, отладчиков, редакторов графических интерфейсов, текстовых редакторов, библиотек подпрограмм. Без отечественных решений и в условиях отсутствия поддержки западных продуктов фактически вся отрасль не сможет функционировать долго, разработчикам не на чём будет работать.

В каких сферах бизнеса, по вашему мнению, в стране ИТ-технологии развиты достаточно высоко, а в каких оставляют желать лучшего? В чём причина?

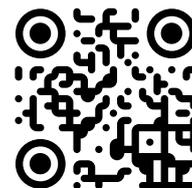
Прикладное ПО, особенно в банковской сфере, сфере коммуникаций, информационной безопасности и автоматизации/цифровизации процессов у нас достаточно хорошо развито. Встраиваемое, и особенно инструментальное ПО, сильно отстают. Причина в том, что на разработку и совершенствование последних требуются годы, надёжная экосистема технологических сателлитов и, главное, рынок сбыта, не ограниченный территорией одной страны.

На что будет делать ставку ваша компания для дальнейшего развития в 2023 году?

«Аурига» продолжит работать в области создания ПО для вновь воссоздаваемого оборудования на альтернативной номенклатуре изделий, необходимых для обеспечения промышленной, медицинской и прочей критически важной инфраструктуры.



Вячеслав Ванюлин
Генеральный директор ООО «Аурига»



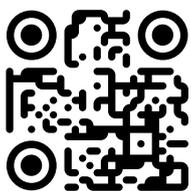
auriga.com

Ctrl2GO



Виктор Соловьёв
Директор
по продуктам
Ctrl2GO Solutions

ctrl²go!



ctrl2go.solutions

Какая область ИТ будет наиболее интересной и знаковой в 2023 году в стране?

Возможно, это будет финтех, крипто, в первую очередь связанная с внешнеэкономической деятельностью. Ситуативный отклик на возникшие трудности с расчётами по ВЭД уже назрел и должен начать решаться. Тем более сами банки являются интересантами в этом движении.

В какой области ИТ в этом году следует ожидать интересных открытий и достижений?

Развитие новых серьёзных сервисов требует ряда лет, думаю, в 2023 мы не увидим чего-то принципиально нового. 2023 год – год возможностей для российских сервисов, которые ранее не могли активно развиваться из-за массового присутствия на рынке более зрелых западных решений. Ключевой вопрос в том, как компании распорядятся этим временем, чтобы заработать денег или реинвестировать в развитие, сократив отставание на международном рынке. Таких областей очень много. Например, это сервисы мониторинга и диагностики промышленного оборудования, предиктивной аналитики, которыми занимается группа Ctrl²GO и некоторые другие компании в РФ.

В чём сильные стороны российских ИТ-компаний и специалистов на мировой арене?

У нас хорошая математическая база, сохранившаяся ещё с Советского Союза, у нас талантливый и изобретательный народ – творческий. Поэтому считаю, что у наших компаний и специалистов широкий потенциал на мировом рынке.

Для развития каких технологий и проектов в России имеется благодатная почва? Какие факторы наиболее влияют на это?

По моим прогнозам, в ближайшее время мы увидим, что ИТ-сектор будет становиться всё более государственным. В приоритете будут проекты, направленные на поддержку и развитие ВПК. Если говорить о роли в этом ИТ, то это всё, что связано с ИТ-обеспечением БПЛА, включая дронов различного назначения.

Возможно, в промышленность будет внедряться робототехника для ускорения работ и роста объёмов производств, и здесь роль ИТ будет

одной из определяющих, начиная с проектирования (САПР) и заканчивая программированием таких роботов на конечных производствах.

Возможно, мы также увидим и попытки импортозаместить западные ОС (Windows/MacOS), создать отечественную ОС. Думаю, будет несколько подобных мегапроектов.

На какие аспекты развития технологий (ИТ, ИБ) сейчас следует сделать акцент государству?

Думаю, не будет какого-то единого аспекта или области. Будет масса сервисов из разных областей, которым надо дать возможность вырасти за ближайшее время. Не заработать денег, а вырасти. А сервисы растут хорошо в конкурентной среде, поэтому в ходе мероприятий по поддержке ИТ нельзя допустить, чтобы «подросло» всего по одной штуке в каждой области.

В каких сферах бизнеса, по вашему мнению, в стране ИТ-технологии развиты достаточно высоко, а в каких оставляют желать лучшего? В чём причина?

У нас традиционно неплохо развиты корпоративные ИТ-системы и гораздо слабее – B2C-сервисы, особенно коробочные. Связано это с тем, что в корпоративном сегменте очень много специфики, кастомизации, консалтинга. «Приземление» западных аналогов на российский ИТ-ландшафт бывает и затруднительным, и дорогим. Поэтому были неплохие условия для формирования отечественных аналогов, которые хорошо чувствовали и учитывали локальные потребности, отличались большей гибкостью, адаптивностью. С B2C-коробками ситуация ровно обратная: мы сразу получили высококачественные сервисы, и конкурировать с ними российским решениям было трудно. К тому же требуется высокая культура инвестирования, чтобы запускать подобные сервисы на конкурентных рынках, да и привычка потребителя «по-честному» платить за коробку тоже стала формироваться лишь недавно.

На что будет делать ставку ваша компания для дальнейшего развития в 2023 году?

Группа Ctrl²GO постарается использовать это время для того, чтобы привлечь инвестиции (в том числе грантовое финансирование) для серьёзного рывка в развитии наших продуктов. В будущем это принесёт дивиденды в виде возможности потягаться на международных рынках с западными лидерами отрасли.

Национальная платформа

Какая область ИТ будет наиболее интересной и знаковой в 2023 году в стране?

Во-первых, системное ПО. Всё, что нужно для построения технологически независимой ИТ-инфраструктуры: российские ОС, системы виртуализации, СХД, системы резервного копирования, системы мониторинга и автоматизации служб Service Desk. Это – ИТ-фундамент для всего остального.

Во-вторых, информационная безопасность, особенно корпоративная. Потому что любая крупная система, надёжно не защищённая, в нынешних условиях будет взломана в течение очень короткого срока. А все ИБ-системы сейчас построены на западном ПО, и его надо заменять.

В какой области ИТ в этом году следует ожидать интересных открытий и достижений?

В мире активно развиваются такие области, как большие языковые модели (LLM) в машинном обучении. Полагаю, что вложения в эти технологии могут давать в дальнейшем большую отдачу в практическом применении.

В чём сильные стороны российских ИТ-компаний и специалистов на мировой арене?

Раньше был неплохой нишевый уровень в достаточно большом количестве сегментов (виртуализация, ИБ, прикладное применение систем с алгоритмами машинного обучения), но сейчас на мировом рынке российских по юрисдикции компаний осталось мало. Большая часть отдела международного бизнеса от российского.

Если говорить о сильных сторонах российских специалистов, то это – хорошая базовая подготовка, относительная низкая стоимость и небольшая разница в деловой и технологической культуре с Европой и США. Например, дочерние компании «Дойче Телеком» держали большой штат в России, именно потому, что стоимость специалистов была сравнительно невысока, уровень квалификации достаточен и с нашим специалистами коммуникационно легче работать, чем с индийскими, т.к. разница деловой и профессиональной культуры не такая значительная. Дополнительным стимулом к применению российских офшорных разработчиков теми же европейцами является меньшая разница поясного времени с Европой в сравнении с Индией.

На какие аспекты развития технологий (ИТ, ИБ) сейчас следует сделать акцент государству?

В первом вопросе мы уже отметили, что ИБ и системное ПО – это основные направления, на которые надо обращать внимание государству. Без этого не выжить.

Есть критичное ПО, которое крайне важно для машиностроения, например PLM-системы или технологии создания цифровых двойников, но нет уверенности, что государство здесь может что-то сделать в разумные сроки. Попытки есть, но до серьёзного продвижения требуется ещё много усилий. Другой вопрос, что российские компании использовали небольшую часть возможностей подобного ПО от мировых лидеров рынка. Возможно, платформы для замещения данных систем в используемой нашими предприятиями части удастся создать в ближайшие 3–5 лет при продолжении целенаправленных усилий в этом направлении.

В каких сферах бизнеса, по вашему мнению, в стране ИТ-технологии развиты достаточно высоко, а в каких оставляют желать лучшего? В чём причина?

Можно отметить, что на хорошем уровне находится применение ИТ в госуслугах, телекоме, банках, ритейле, нефтегазовом комплексе. Государственные информсистемы хорошо работают, грамотно построены, масштабируемые, надёжные. Очень неплохая ситуация с разработкой бизнес-приложений: ERP, CRM, банковское ПО.

На что будет делать ставку ваша компания для дальнейшего развития в 2023 году?

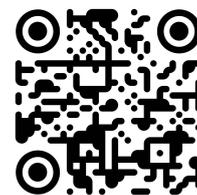
Мы планируем дальнейшее развитие ERP-платформы «Ma-3» по трём векторам: наращивание функциональности, создание отраслевых решений, развитие партнёрской сети, в том числе развитие партнёрских отношений с вузами для формирования пула специалистов по внедрению «Ma-3».



Михаил Аксёнов
Операционный директор компании «Национальная платформа» (входит в НКК)



Национальная платформа



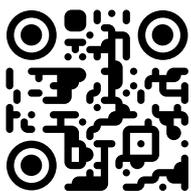
www.national-platform.ru

СИНТО



**Игорь Германович
Веселов**

Заместитель
генерального
директора
по развитию
компании
«СИНТО»



sinto.pro

Какая область ИТ будет наиболее интересной и знаковой в 2023 году в стране?

Абсолютно все игроки ИТ-рынка вынуждены заниматься импортозамещением. Замещение иностранных производителей как железа, так и софта (а также комплексных проектов софт + железо + сеть + безопасность) идёт семимильными шагами, российские производители являются основными выгодоприобретателями.

В какой области ИТ в этом году следует ожидать интересных открытий и достижений?

Следует признать, что по всем направлениям в ИТ постепенно, год от года, будет накапливаться технологическое отставание от мирового ИТ-рынка. Оно, к сожалению, неизбежно.

Сейчас есть интересные решения российских разработчиков по информационной безопасности, рывок в разработке системного и прикладного программного обеспечения. Предполагаю, что будут активно продолжать развиваться проекты с нейронными сетями, будет рост предоставления услуг по технической поддержке оборудования (замена технической поддержки вендоров, которые ушли с рынка). А также тема параллельного импорта и развития альтернативных каналов поставок станет актуальна.

В чём сильные стороны российских ИТ-компаний и специалистов на мировой арене?

Написание программного кода (кодинг), то есть в области программирования российские специалисты, безусловно, обладают сильными компетенциями.

Для развития каких технологий и проектов в России имеется благодатная почва? Какие факторы наиболее влияют на это?

Задача минимум – это создание различных условий и возможностей для развития производств компонентов для ИТ. В части производства печатных плат, SMD-установщиков процесс пошёл, многие крупные игроки инвестируют в создание таких производств. Этому способствовала политика Правительства РФ,

требования по импортозамещению, создание реестра Минпромторга. Но это производство на основе импортной элементной базы.

Мировая ИТ-отрасль остро ощутила на себе проблемы с элементной базой (чипами) в последние годы. Способствовали тому всем известные события, пандемия и другие геополитические процессы, которые сейчас происходят в мире.

Поэтому мне кажется, что задача максимум – это развитие фотолитографии, локализация производства микроэлектроники в России пусть и не по самым современным техпроцессам. Это крайне необходимо для сокращения пропасти в технологическом отставании нашей страны. Считаю, что поиск каналов для закупки пусть не самых современных технологических линий полного цикла для производства на территории России микросхем (чипов) даже по устаревшим для мировой ИТ-отрасли технологиям **90 нм** – это то, на чём следует сосредоточиться. Кроме технологического оборудования необходимы схемотехники, дизайнеры, инженеры-технологи, сырье и материалы. Необходимо почти с нуля создавать производство собственной элементной базы, это даст нам толчок для развития и самостоятельность, независимость во многих ИТ-направлениях от колебаний мирового рынка и зарубежных производителей.

Это огромные инвестиции, есть ли возможность их привлечь – это отдельный вопрос.

На какие аспекты развития технологий (ИТ, ИБ) сейчас следует сделать акцент государству?

Одновременно с созданием условий для производства чипов, печатных плат на территории России необходимо оказать поддержку профильным ВУЗам для увеличения подготовки специалистов по специальностям «Инженер-технолог по производству интегральных схем» и смежным специальностям.

В каких сферах бизнеса, по вашему мнению, в стране ИТ-технологии развиты достаточно высоко, а в каких оставляют желать лучшего? В чём причина?

Финансовый сектор, государственные электронные услуги и электронный документо-

оборот, нефтяная и газовая промышленность, ритейл и другие активно применяют ИТ-технологии. Слабее в плане ИТ многие образовательные учреждения, медицинские (преимущественно региональные) и т.д., всё зависит от уровня бюджетирования (например, госструктур) и вложений в ИТ той или иной коммерческой компании. Безусловно, у кого-то, например банков, этих возможностей больше, у кого-то они практически отсутствуют. Важный аспект – понимание руководителя, топ-менеджмента в необходимости внедрения ИТ-технологий в процессы своих предприятий и желание это делать, разбираться в рынке и технологиях, понимать, как их можно применить, смотреть на перспективу.

На что будет делать ставку ваша компания для дальнейшего развития в 2023 году?

Первый и главный наш ресурс – это люди. Развиваем новые компетенции, обучаемся, перестраиваемся под изменения рынка. Активно работаем с альтернативными каналами поставки, ищем новых партнёров, изучаем азиатский рынок, ближнее зарубежье, делаем успехи в этом направлении. Смотрим и делаем шаги в направлении сервисной поддержки взамен ушедших вендоров. Развиваем OEM (в частности, серверное оборудование), делаем акценты на ИБ, виртуализации, комплексных проектах по переходу на импортозамещающие решения.

eXpress

Какая область ИТ будет наиболее интересной и знаковой в 2023 году в стране?

Сегодня абсолютно вся область ИТ является интересной и знаковой, везде одна и та же ситуация: «импортозамещение поневоле».

В какой области ИТ в этом году следует ожидать интересных открытий и достижений?

Главный вопрос – дефицит микроэлектроники, российских чипов: сможет ли страна дать массовое локальное производство.

В чём сильные стороны российских ИТ-компаний и специалистов на мировой арене?

Западные рынки для российских компаний очевидно закрыты, зато для Востока будет очень сильный value proposition: качественная альтернатива Западу – решение для заказчиков «не класть все яйца в одну корзину».

Для развитие каких технологий и проектов в России имеется благодатная почва? Какие факторы наиболее влияют на это?

Благодатная почва в России сейчас для всех проектов, особенно в тех рыночных нишах, где доминировал Запад: там есть клиентский спрос и нет продуктов. Первый, кто сделает продукт, устраивающий клиентов, сорвёт банк.

На какие аспекты развития технологий (ИТ, ИБ) сейчас следует сделать акцент государству?

Внимание государства нужно направить на развитие кадров, а не технологий, в первую очередь, на сохранение разработчиков в стране или хотя бы их доступность. А потребность в технологиях определит рынок, это следует из предыдущего пункта.

В каких сферах бизнеса по вашему мнению в стране ИТ-технологии развиты достаточно высоко, а в каких оставляют желать лучшего? В чём причина?

С софтом всё относительно хорошо, с «железом» – гораздо хуже. «Железо» более капиталоемкое: большая зависимость от лицензируемых западных технологий, значительно выше способность Запада применять санкции. Тем не менее и по «железу» вопрос в той или иной степени, очевидно, будет решён.

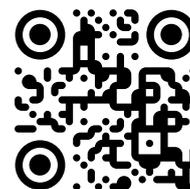
На что будет делать ставку ваша компания для дальнейшего развития в 2023 году?

На рост функционала и качества наших продуктов. В этом плане для нас ничего не изменилось.

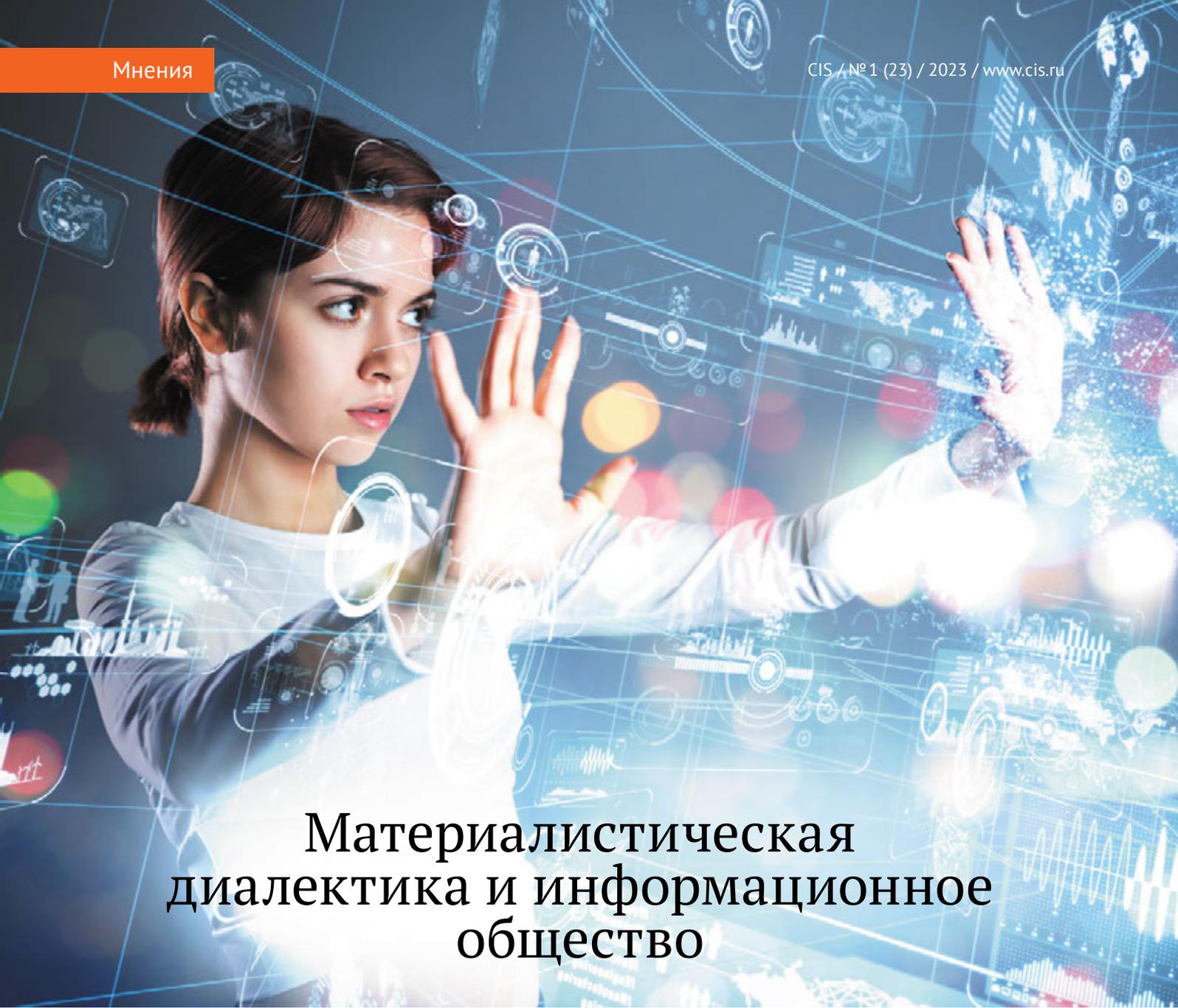


Андрей Вращкий
CEO платформы корпоративных коммуникаций и мобильности eXpress

eXpress



express.ms



Материалистическая диалектика и информационное общество

Наука и практика современного информационного общества показывают, что механизм взаимодействия материальных и духовных процессов продолжают усложняться. Это порождает множество подходов к концепции идеального и материального, предлагаются разные теоретические принципы осмысления нынешнего этапа общественного развития.

Много публикаций посвящается современным особенностям материализма и диалектического материализма в частности. Идёт большой поток критики в адрес философской науки, начи-

ная с корректности постановки основного вопроса философии и заканчивая сомнениями в части состоятельности диалектического материализма как теории. Можно сказать, что в современной философии фактически складывается кризис в понимании материи и её взаимодействия с сознанием. С одной стороны, это связано с известными социально-политическими причинами и отказом России от традиционного марксистского диалектико-материалистического мировоззрения с попыткой заменить его другими концепциями, с другой – с более глубокими объективными процессами, связанными с развитием науки: квантовой механики, биотехнологии, искусственного интеллекта и информационных технологий.

Преодоление данного кризиса требует уточнения понятий материального и идеального, сопоставления их с новыми для научного познания



Анатолий Орлюк
КЭН, доцент РУТ (МИИТ)

явлениями, в которых взаимодействие материи и сознания приобретает сложные формы.

В этой связи возникает закономерный вопрос: насколько оправданы и обос-

нованы были наши обращения к диалектическому материализму в статье «Причинность, случайность и принцип дополнительности» (см. CIS № 22021 г.), где предпринималась попытка рассмотреть эти категории через призму материалистической диалектики.

В статье мы обращали внимание на противоречие в диалектическом материализме (далее – ДМ), и предлагалось в определённом смысле совместить материализм и идеализм, тем самым снять проблему. В другой статье – «Ещё раз о причинности в философии и естествознании» (см. CIS № 22022 г.) тоже апеллировали к ДМ по вопросу о причинности. Эти отдельные примеры понуждают ещё раз вернуться к уточнению и критическому анализу основных положений материализма.

Касаясь основного вопроса философии о соотношении материального и духовного, представляется очевидным, что, если речь идёт о первичности материи или сознания, тут не может быть места для дискуссии: она, скорее, допустима о бытии и сознании, но утверждение идеалистов о том, что без сознания нет материи, противоречит логике и здравому смыслу (правда, учёные физики критикуют его, по-видимому, из-за ассоциации с классической механикой). Допустим, речь о Марсе, где нет людей и отсутствует сознание, но он как объект существует. Думается, великие философы – Гегель, Кант – это понимали, но над ними довлела политика, вера, и они прибегали к надуманным схемам: «абсолютная идея», «вещь в себе», чтобы завуалировать религиозную сущность своих учений. Хотя это несло в себе определённый научный смысл, а не только политическую подоплёку, особенно если учесть постоянное отставание науки от практики, когда наука не могла объяснить многие явления и люди вынужденно обращались к вере.

Вместе с тем развитие науки, особенно физики, появление квантовой механики (далее – КМ) привело к отходу от позитивистских принципов, когда материя является объективной реальностью данной нам в ощущениях, поскольку в настоящее время известно, что материальность означает не только вещественность, взяв хотя бы поле. Но не только: многие физические объекты недоступны чувственному опыту, они введены в науку как теоретические мысленные конструкции (модель ДНК, объекты квантовой физики – без этого

продвижение научных исследований невозможно). Объекты такого рода, с одной стороны, существуют объективно, а с другой – они невещественны, подобно идеям Платона.

Возможно два варианта истолкования рассматриваемой специфики квантово-механического описания реальности: микрореальности не существует до акта измерения – она создаётся этим актом, или существование микрореальности до акта измерения не отрицается, хотя и считается непознаваемой для человека. Но специалисты в области КМ не ограничиваются микрореальностью.

Был проведён эксперимент: два человека в нужных условиях могут наблюдать одно и то же событие, но с разным результатом, при этом оба будут правы, из чего можно сделать вывод об отсутствии объективной реальности. Материя не обладает субстанцией, первоосновой, тем самым разрушаются основы материалистических представлений. Означают ли все эти эксперименты необходимость решительного отказа от материализма? Отнюдь! Не касаясь вопросов чистоты экспериментов и других сопутствующих проблем, их результаты не есть окончательно установленный научный факт, и, может быть, со временем данные эксперименты получат другую трактовку, не противоречащую материализму: процесс познания бесконечен. Вместе с тем они дают пищу для переосмысления наших знаний и в определённой мере позволяют сблизить позиции материализма и идеализма в проблеме познания мира.

В контексте современных подходов к материальному и идеальному огромное значение имеет изучение феномена сознания и не только с философской точки зрения. Выявление сущности сознания является сложнейшей научной проблемой. Всестороннее изучение сознания вызвано также интенсификацией работ по искусственному интеллекту (далее – ИИ). Острота проблемы в том, что здесь сознание играет ключевую роль и вызывает повышенный интерес у специалистов по разработке ИИ. Овладение его секретами открывает дорогу к созданию ИИ.

В литературе можно увидеть самые разнообразные подходы и теории: сознание не является продуктом работы мозга, не сознание подчинено мозгу, а наоборот, сознание материально и другое. Очень модна теория панпси-

хоза – представление о всеобщей одушевлённости природы, когда каждый атом обладает сознанием и т.п. Да, если допустить, что сознание возможно без мозга, то атом может обладать сознанием. Наличие такого множества мнений и, соответственно, критики материалистического подхода означать его близость к истине, с одной стороны, а с другой – сложность и необходимость глубокого изучения данного феномена. О его сложности и малой степени изученности свидетельствует хотя бы тот факт, что многие учёные говорят о квантовой природе сознания, они выдвигают ряд гипотез, в основе которых предположение, что сознание невозможно понять и объяснить на основе классической физики, но это может быть сделано с привлечением постулатов КМ.

Возвращаясь к материальному и духовному, подчеркнём, что материя первична и существует вне зависимости от сознания, но всё-таки допустимо и уместно вести дискуссию о соотношении бытия и сознания, когда общественное бытие определяет общественное сознание. Дискутировать уместно о механизме формирования сознания и, что особенно важно, о влиянии его на бытие. Разумеется, сознание отражает бытие, но это не значит, что бытие всецело и однозначно определяет сознание, – оно создаёт основные предпосылки его формирования.

Механизм формирования сознания весьма сложен. Одним из главных его составляющих являются СМИ, которые, находясь в руках власти, могут формировать общественное сознание в своих интересах. Не менее важна в этом вопросе существующая система образования. Большое влияние на формирование сознания оказывает наука, искусство, литература – они могут его активизировать или подавлять. То есть, на сознание, кроме бытия как такового, влияет много других факторов, и, если учесть теорию о том, что оно никак не формируется, а даётся от природы, можно сделать вывод об отсутствии тождества бытия и сознания. Акцент в дискуссии о первичности бытия и влиянии сознания на бытие проистекает из того, что в классическом материализме всячески принижалась роль сознания, подчёркивалась его вторичность и пассивность. Такой догматизм имел самые негативные последствия для теории и практики. В чём это выражалось? Например, в последние годы советской

власти наблюдался приоритет материальных ценностей над духовными, что вытекало из данной догмы. Хотя это не свойственно социалистической системе, но инициировалось и поощрялось партийной элитой, которая всячески пользовалась материальными привилегиями, что никак не согласовывалось с декларируемыми высокими идеями. Разумеется, такое положение отрицательно отражалось в сознании, но партия это игнорировала, опять же исходя из вторичности сознания и убеждённости в его пассивности.

Каковы последствия этих заблуждений – социально-экономический тупик в нашем обществе. Справедливости ради укажем, что не только следствие догматизма в теории, были и другие причины неоправданного отхода от социалистической идеи. Практической иллюстрацией такого изъяна в теории было выдвижение партией тезиса о необходимости создания материально-технической базы нового общества. На самом же деле необходимо было решать единую задачу: главное не только материальная база, а в первую очередь формирование нового сознания. Ошибочным было предположение, что это получится само собой.

Продолжая вопрос диалектического единства бытия и сознания, допустим, что в обществе, где соседствует роскошь и нищета, общественное сознание на начальной стадии не отвергает такую действительность, но это вовсе не значит, что в его глубине не зарождаются ростки нового, противоречащего данному бытию. Отметим, что возможны текущие временные противоречия или несоответствия связаны с тем, что сознание может отставать от бытия и наоборот. Здесь речь может идти о противоречиях роста, которые свойственны для диалектического единства. Они вызваны в основном существующим механизмом формирования сознания. Но в процессе развития могут иметь место глубокие противоречия, которые нарушают единство. В этой связи необходимо отдельно коснуться общественного и индивидуального сознания.

Даже исходя из вторичности общественного сознания и рассматривая сознание отдельного индивида и его интеллектуальные способности, которые настолько развиты, что тот может увидеть рамки своей ограниченности и выйти за них, понятно, что его сознание становится первичным, и человек

в состоянии изменить бытие. Вопрос в том, что такое возможно, если только данное индивидуальное сознание станет общественным, превратится в массовое. И тут важно следующее: способствует ли существующий механизм формирования общественного сознания такому переходу, с одной стороны, и отношение власти к новым идеям – с другой, ибо её невосприимчивость может оказать решающее воздействие на общественное сознание. Тогда идея, овладевая массами, станет первичной, уже не бытие будет определяющим – оно станет вторичным. Людей в обществе с прогрессивными идеями меньше, поэтому общественное сознание более консервативно, откуда и зарождается его инертность, вторичность.

В своей статье (см. CIS № 12022 г.) мы писали о том, как можно построить разумную экономику, при этом исходили не из существующей действительности, а искали новые идеи, модели, даже привлекая неординарные подходы на основе КМ, подчёркивая отставание бытия. Вот один из примеров влияния на общественное сознание с целью превращения его в реальную силу, способную изменить бытие.

Почему столь подробно? Приведённые соображения целесообразно учесть при окончательной разработке упомянутой теории в рамках материализма и не только в контексте материального – духовное, но и для понимания собственно феномена сознания. Данная теория могла бы стать одной из научных предпосылок для создания ИИ на платформе материалистической диалектики, ИИ в свою очередь будет оказывать соответствующее влияние на общественное сознание.

Преодоление выше упомянутого кризиса требует уточнения понятий «материальное» и «идеальное», сопоставления их с новыми для научного познания явлениями, в которых взаимодействие материи и сознания приобретает наиболее сложные формы такие, как информация, компьютерная программа, цифровая модель. В среде специалистов нет единого мнения относительно их материальности или идеальности, особенно острая дискуссия ведётся относительно информации.

Рассмотрение можно начать со знаний – знаний законов природы и общества. В природе всё взаимосвязано и взаимообусловлено, и объективно существуют законы, описывающие эти связи, которые материальны,

но на данном этапе люди могут все их не знать. Например, как влияет хозяйственная деятельность человека на климат или как последний – на численность населения на Земле. Понятно, что приближенные оценки возможны, но точные, как это следовало бы из существующих законов, нет. Познание природы и есть выявление этих законов через сознание, то есть новые знания относятся к миру идеального, а уже принятые и используемые знания материальны. Но знания и информация тесно связаны, так как информация несёт в себе признак скрытых закономерностей, предтеча знаний как идея, которая превращается в знание. Информация – это необычное отклонение, которое требует реакции или действия. И это отклонение носит случайный характер. В этом смысле можно определить информацию как отражение свершившейся случайности. Почему случайности? Не потому, что отсутствуют причинно-следственные связи, а из-за неполноты данных, мы не знаем всех фактов или событий, которые связывают и обуславливают наблюдаемое явление.

Наконец не во всех случаях имеется стройная научная теория, которая способна объяснить эту взаимосвязь, и полученная информация не вписывается в рамки существующих законов. Как видно из этого, самой по себе информации в природе нет – это продукт работы сознания. В такой трактовке информация относится именно к миру идеального, а попытки доказать материальность информации – как ещё один пример принижения роли сознания.

Наверное, возможны и другие интерпретации, и для большей убеждённости, хотел бы отослать читателей к статье в журнале БИТ («Что такое информация», № 1 февраль 2018 г.), где автором этих строк предпринята попытка осмысления такой сложной категории.

Что касается компьютерных программ, то, если они зарождаются и существуют в сознании программиста, – это идеальное, но, как только он начинает переносить программу на компьютер и запускать её, это как раз и есть реализация идеи, которая становится материальной.

Ровно то же можно отнести и к цифровой модели, если это идея в сознании автора – мир идеального, но, как только начинается реальное построение такой модели, она превращается

в материальный объект. Может возникнуть вопрос: для науки такое деление важно, а какое практическое значение? Оказывается, большое. Если с программами сегодня всё ясно: они нематериальные активы, но вместе с тем являются объектом хозяйственного оборота, что вполне логично, то, что касается информации и попытками её долговременного хранения, принятия на баланс и т.п., окончательной ясности нет, что свидетельствует о непонимании смысла информации и показывает абсурдность попыток её материализации.

Огромное значение в современных условиях имеют также оценки и отношение к ДМ как учению о развитии и познании мира. В литературе много критики ДМ, начиная от догматизма, примитивности и заканчивая нелепыми выводами об абсурдности данной теории, о чём нет смысла спорить.

Что касается догматизма, то есть вопросы, и один из главных: законы диалектики – это законы природы, мышления и истории или только законы мышления и истории? С точки зрения Гегеля, это законы мышления. Энгельс же критикует его за «вымученность и ужасность» такой конструкции, которая вытекает не из законов природы, а из законов мышления. В основе философии Гегеля лежит тождество бытия и мышления. И тогда, казалось бы, нет проблем. Но такое идеалистическое отождествление бытия и мышления сводится к мыслительному процессу. По Гегелю, бытие представляет собой воплощение понятий «мышление», «идея», то есть, по-другому говоря, они первичны. Поэтому трудно критиковать Гегеля за такую конструкцию: для объективного идеалиста она вполне приемлема.

Дальнейшее развитие естественных наук показало, что переворот Энгельса не корректен. Имеется много явлений и закономерностей в природе, которые не вписываются в законы диалектики, как законы природы, хотя есть и такие. Из этого следует, что законы диалектики не являются всеобщими. Можно только восхищаться глубиной абстракций Гегеля, отдавать должное Марксу, который сумел увидеть связь законов Гегеля с социально-политическими явлениями и выявить с их помощью законы истории и политической экономики. Но законы мышления, формальной логики существенно отличаются от законов природы, которые действуют сами по себе. Законы логики зависят от людей, то есть субъективны, а законы природы – объективны.

Догматизм заключается в том, что партийная философия не занималась изучением этого вопроса ни в свете КМ, ни других современных наук, а развитие предполагает обязательную оценку и переосмысление новых явлений. ДМ, как и всякая теория, требует обновления. Но проблема не только в этом. О каком обновлении могла идти речь, если даже существующие законы догматически трактовались партийной наукой или игнорировались на практике. Взять пример из политической экономики: рынок и планирование – парные категории, при правильном понимании и творческом подходе из законов диалектики следует, что в социалистическом обществе есть место для рыночных отношений, план и рынок – в борьбе и единстве, взаимно дополняются и развиваются. Практика показала, что абсолютизация планирования приводила к «чёрному рынку» и прочим негативным явлениям, которые и стали причиной отхода от социализма, равно как отсутствие планирования тормозит развитие и приводит к огромным потерям ресурсов (об этом свидетельствует практика сегодняшнего дня). Адепты рынка не говорят о планировании, они призывают к регуляторам и другим государственным институтам, которые зададут отправные точки для рынка. Но это и есть планирование.

Таким образом, можно сказать, что ДМ является теоретической основой для изучения и понимания истории, социально-политических явлений, а диалектические законы мышления – хороший инструмент оценки фактов и явлений повседневной жизни, но в меньшей степени имеют отношение к естественным наукам и опору на них, в частности современную физику. Заметим, что сегодня в учебниках по философии, как и 200 лет тому назад, утверждается, что законы диалектики – это законы природы, истории и мышления.

Некоторые учёные говорят о необходимости освобождения естественных наук от оков материализма. Такая гипотеза наводит на мысль о потребности современных физиков-теоретиков, например, в свободе фантазии, генерации идей, выходящих за рамки существующих теорий, за рамки здравого смысла. Но материализм должен оставаться в качестве ориентира или допустимого предела, а когда ими овладеют невероятные, безумные идеи и вера в сверхъестественные силы, материалистическая теория вернёт их на истинный путь или по меньшей мере заставит ещё раз учесть её

положения и проверить истинность невероятных идей.

Можно сделать вывод, что ДМ, несмотря на своё идеалистическое происхождение, является последовательно научно-материалистической теорией как метод изучения человеческого общества и мышления. Всякие измышления о его несостоятельности как теории и непригодности для практики решительно отвергаются. Альтернативы ДМ нет, и отказ от него означал бы возврат в средневековье. Кроме того, ДМ подтверждает жизнеспособность социалистической идеи как естественного и единственного пути развития человечества, являясь её теоретической основой.

Особо следует отметить, что оставаясь на позициях ДМ, возможно создать полноценный ИИ, так как ИИ относится к материальному миру и любая другая платформа ведёт к заблуждениям, погружает в область мистических сил и мракобесия, а это мешает получению дружественного и полезного помощника человеку.

В заключение отметим, что в эпоху информационного общества становится ясно: отношение материи и сознания не исчерпываются упрощёнными понятиями первичности и вторичности. Каждая исторически возникшая форма объективной реальности связана с сознанием по-своему, и философский анализ современного общества требует раскрытия специфики этих способов связи материального и духовного. Между материальным и идеальным наблюдаются тенденции к сближению как между двумя диалектическими противоположностями, которые дополняют друг друга, что способствует развитию научной и философской мысли.

Именно при таком подходе возможно необходимое обновление и творческое развитие материалистической философии, что позволит преодолеть наблюдающийся кризис в этой науке в современном информационном обществе. Будет создана одна из предпосылок для включения материалистической диалектики в идеологический базис нашего общества. Подчеркнём, что данная работа потребует огромных усилий со стороны учёных философов, особенно академической философской науки, которая пока бездействует, хотя обязана быть в авангарде.

Чипирование человека

Плюсы и минусы
биочипов



Наличие чипа под кожей может стать отличным подспорьем в повседневной жизни. С его помощью человек сможет подтверждать свою личность, оплачивать покупки в магазине или следить за уровнем глюкозы в крови. Однако подобные удобства способны нанести существенный урон в сфере конфиденциальности и безопасности человека.

Что такое чип?

Биочип – разновидность чипа, имплантируемого под кожу, представляет собой электронный компонент, помещаемый в живую ткань животных или человека. Он, как правило, состоит из четырёх основных частей: спиральной антенны, конденсатора и микрочипа. Четвёртый элемент представляет собой биосовместимую капсулу, в которую заключены три вышеуказанных элемента.

Подобные типы биочипов не имеют внутреннего источника питания – они реагируют только на радиосигнал, посылаемый сканером. Чип получает сигнал, активирует и отправляет ответ с информацией (которая в нём закодирована) на сканер. Стоит отметить, что чипы обычно ограничены расстоянием: сканер должен быть относительно близко, чтобы иметь возможность взаимодействовать с носителем информации.

Первое чипирование человека

Первым человеком, имплантировавшим подкожный микротрансмисмиттер, был британский учёный Кевин Уорвик. В 1998 году его тело было «модернизировано» с помощью небольшого устройства – имплантата, который позволял британцу выполнять несколько простых действий: включение и выключение света, переключение программы передач на ТВ и пр. После девяти дней использования чип был удалён из тела Уорвика. Но изобретатель остался доволен результатами эксперимента – он доказал, что связь с имплантатом возможна. Этот эксперимент заложил основу для темы чипирования, которая сейчас волнует умы тысяч людей на планете.

Преимущества биочипов

Перейдём к современности. Как именно имплантированный под кожу биочип может помочь людям в повседневной жизни?

Имплантат, правильно подключённый к нашему банковскому счёту, мог бы работать по тому же принципу, что и платёжная карта. Он может хранить наши точные данные, всю информацию, которая есть в наших удостоверениях личности. Проблема с потерей кошелька, бумажных или пластиковых удостоверений ушла бы в прошлое: вся самая важная информация всё время «под рукой».

Подкожные чипы уже используются компаниями, которые ценят свою безопасность. Например, организация Three Square Market (США, штат Висконсин) уже прочипировала 80 своих сотрудников. Биочипы размером с рисовое зёрнышко были оснащены RFID-модулем и имплантированы в руку. Имплантаты должны были предоставить доступ к отдельным отделам в компании, облегчить покупку продуктов в столовой и использовать компьютеры и копировальные аппараты по назначению.

Чипирование сотрудников получило распространение и в шведских компаниях. Это положительно сказалось на безопасности внутри организаций и снизило риски утечки данных.

Подкожный кусочек кремния мог бы быть полезен врачам: имплантат может хранить всю необходимую личную медицинскую информацию пациента. По крайней мере, данный подход сэкономял бы время и упразднил бы многие бюрократические проволочки. Особенно в экстренных ситуациях: ДТП, стихийные бедствия и пр.

Реальная опасность чипирования

Интернет «гудит» о всевозможных теориях заговора, связанных с имплантатами и биочипами: якобы люди пытаются пронумеровать, лишиться личного пространства, частной жизни, осуществить контроль доступа к финансам и т.п. Так в чём дело и на что стоит обратить внимание?

Беспроводная кража информации

Это связано с проблемой личных данных, содержащихся в памяти чипа. На данный момент информация никак не защищается и может быть украде-

на посторонними лицами при наличии соответствующего оборудования и знаний. Номер кредитной карты, телефон, адрес, биометрия, прочие персональные данные – всё это способно оказаться в руках преступников, которые могут использовать информацию против её носителя.

Побочные эффекты для здоровья

Можно с уверенностью предположить, что долгосрочные потенциальные побочные эффекты до сих пор неизвестны. Эксперименты по имплантации микрочипов не были протестированы долгосрочно. Науче известны исследования на грызунах, указывающие на связь между применением чипа и развитием рака. Этот случай, безусловно, является верхушкой айсберга с точки зрения безопасности жизни и здоровья человека. Разработка технологий чипирования потребует интенсивных исследований с целью развеять любые сомнения и заполнить пробелы в вопросе побочных эффектов.

Ещё одна проблема – биочип не закреплён под кожей. Может произойти ситуация, когда устройство просто пропадёт с места его вживления. Подобный случай способен привести как минимум к медицинским осложнениям (тромбоз).

Чипирование – вопрос времени для каждого из нас?

Тема чипирования ворвалась в сознание людей и закрепилась достаточно прочно. Можно смело предположить, что разработка этой технологии станет со временем чем-то популярным, как это было в случае с компьютерами, мобильными телефонами и т.д. Людям свойственно всё подвергать сомнению, и простая человеческая осторожность всегда сопутствовала технологическим новшествам. Время расставит всё на свои места, поэтому вопрос пока остаётся открытым.



SOVINTEGRA

«SOVINTEGRA» – инновационный проект, объединивший первоклассных специалистов с колоссальным опытом работы (более 15 лет) в области информационных технологий. Выбрав нашу компанию, вы получаете знания и умения команды профессионалов, не переплачивая за громкое имя фирмы.

sovintegra.ru

Гороскоп для ИТ-компаний на весну 2023 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 компании.



Овен

21 марта – 20 апреля

Весной 2023 года компании Овны могут начать массу новых направлений. Это благоприятный период для любых начинаний, поэтому если есть план развития и свежие бизнес-идеи, то можно смело начинать их реализовывать. Период обещает быть ярким и насыщенным событиями. Некогда будет скучать и думать о неприятностях.

Рекомендуется направить все мощности на повышение благосостояния и партнёрских отношений – на этом поприще есть шанс добиться максимальных успехов.



Телец

21 апреля – 21 мая

Тельцам в это время года следует переключиться с решения финансовых вопросов на устройство комфорта и благополучия внутри компании и сотрудников. Кроме того, звезды настоятельно рекомендуют избегать всяческих авантур, ведь они могут привести хаос в устоявшийся порядок и стабильно протекающие бизнес-процессы.

Научитесь сдерживать порывы во всех проявлениях. Немного остудив темперамент и амбиции, можно найти и принять массу взвешенных и разумных бизнес-решений.



Близнецы

22 мая – 21 июня

Компании Близнецы всегда находят верные пути для решения тех или иных проблем. Весна 2023 года не станет исключением из этого правила. У компаний есть шанс стать ещё эффективнее и богаче, если руководство приложит для этого достаточно усилий.

Прекратите заниматься провальными проектами и действовать по привычке – оглянитесь вокруг: как много перспективных направлений ждут вашего участия. Что ждёт компанию на рынке – решать смелым и находчивым руководителям!



Рак

22 июня – 22 июля

Весна 2023 года для компаний Раков станет удачным временем для налаживания партнёрских отношений. Сейчас получится быть достаточно лояльными и эффективными, чтобы завести множество полезных знакомств, деловых связей и заказчиков. Кроме того, малому бизнесу знака начало весны сулит массу приятных бонусов в развитии.

Следует перестать жить старыми принципами, ценностями и проектами, ведь не ровен час, когда финансовое положение может значительно ухудшиться. Именно поэтому в это время года важно сбалансировано распределить ресурсы компании, чтобы успеть выполнить все намеченные задачи.



Лев

23 июля – 22 августа

Весной Львов ждёт несколько праздничных событий. В это время компании смогут проводить множество незапланированных, но необременительных и ярких мероприятий, эффективных для дальнейшего роста.

Если ранее были сделаны некоторые инвестиции или успешно закрыты важные проекты, то сейчас можно спокойно пожинать плоды трудов без лишних усилий.

Однако совсем расслабляться не следует – высокое финансовое положение рискует пойти на убыль, если не поддерживать текущие бизнес-процессы в стабильном состоянии. Именно поэтому весной Львам, как никогда, важно чередовать период активной работы на рынке и отдых. Не предавайтесь излишним иллюзиям, что всё само собой устроится, – держите руку на пульсе, и тогда вам улыбнётся удача.



Дева

23 августа – 22 сентября

В начале весны компаниям Девам предстоят не только радостные события, но и настоящие испытания. Не стоит унывать, ведь

отступление от задуманного плана развития лишь усугубит ситуацию. Лучше спокойно оцените свои возможности и ресурсы.

Если самостоятельно компания не может решить возникшие проблемы, следует обратиться к надёжным партнёрам или опытным советникам за помощью. Не переживайте по мелочам, ведь уже к середине месяца всё решится в пользу вашего бизнеса.

Это не значит, что нужно сидеть сложа руки, наоборот, чем раньше компания начнёт решительно действовать, тем быстрее стабилизирует своё положение.



Весы

23 сентября – 22 октября

Сейчас планеты влияют на бизнес таким образом, что всё, за что ни взяться и ни запланировать, столкнётся с серьёзными препятствиями. Компания получит вызов, на который обязана достойно ответить, – вселенная проверяет бизнес на прочность, и это ни в коем случае не стоит воспринимать как трагедию: можно получить достойное вознаграждение за упорство и преодоленные препятствия.

Зная о нестабильности бизнес-процессов в организации, постарайтесь минимизировать резкие переходы от кардинальных направлений в развитии. И если сотрудники с пониманием отнесутся к таким переменам внутри компании, то на рынке это не будет воспринято лояльно, даже может стать источником значительных трудностей.



Скорпион

23 октября – 22 ноября

Если компания относится к тем Скорпионам, которые с нетерпением ждали весны, то оптимизм и надежда на повышение благополучия станут основными мотиваторами развития. Гороскоп оправдывает ожидания представителей знака в полной мере: многих ждёт успех как в финансовом вопросе, так и в развитии внутренних процессов.

Скорпионам важно быстрее начать смотреть на бизнес реалистично и оптимистично. В таком случае компании будут довольны своим положением, станут эффективнее и финансово благополучнее, удивляя своих партнёров и конкурентов.



Стрелец

23 ноября – 21 декабря

Весной 2023 года Стрельцов ждёт немало серьёзных потрясений, ярких проектов и незабываемых встреч. Все события будут

положительными, а компании смогут добиться внушительных успехов не только в области внутреннего развития, но и приобретут вес на рынке.

Привилегии не будут сыпаться на с неба, нужно помнить, что всего придётся добиваться решительностью и продуманными шагами.



Козерог

22 декабря – 20 января

Активные и ответственные компании Козероги будут чувствовать себя прекрасно. В тоже время представители знака, которые не стесняются злых умыслов против конкурентов или необдуманных действий с заказчиками, могут получить по заслугам. Именно поэтому лучше всего пересмотреть ценности компании, отношение к сотрудничеству и взаимодействиям в любых направлениях.

Нестабильность бизнес-процессов может выразиться в ряде нарушений и дисбалансе в производстве. Именно поэтому Козерогам следует подумать о качественном улучшении отношений с партнёрами и заказчиками, а также финансовом положении.



Водолей

21 января – 19 февраля

Компаниям Водолеем будет сопутствовать успех во многих направлениях бизнеса. Знаковыми станут перемены во внутреннем устройстве организаций. Необходимо внимательно следить за стратегией компании на рынке и не оттолкнуть заказчиков и партнёров излишней настойчивостью и упорством.

В этом периоде хорошо повлияет на компанию смена внутренних процессов или устройства. Возможно, стоит взяться за ремонт офиса, который так долго планировался, или внести в корпоративный кодекс новые правила, пересмотреть бонусы.

В целом это замечательное время для компаний, занятых полезным и востребованным производством.



Рыбы

20 февраля – 20 марта

Этот период обещает быть спокойным и даже немного скучным для компаний Рыб. Стоит воспользоваться свободным временем и начать развивать новые направления или разрабатывать интересные продукты. Благоприятное влияние окажет обучение или повышение квалификации персонала, а также обмен опытом.

Стабильность на рынке поможет комфортному протеканию бизнес-процессов внутри компании и успешному движению вперёд.

Календарь мероприятий

1 марта 2023

Онлайн-трансляция • Митап
Online IT HR meetup 11.55

1–25 марта 2023

Санкт-Петербург • Онлайн-трансляция • Курс
Курс IT-Recruiter

2–5 марта 2023

Иркутск • Конференция
Интенсив Код ИБ ПРОФИ Байкал

2 марта 2023

Краснодар • Лекция
Семинар Труконф о видеоконференцсвязи и совместной работе в Краснодаре

3 марта 2023

Москва • Онлайн-трансляция • Конференция
14я ежегодная международная научно-практическая конференция «Инвестиции. Инновации. Информационные Технологии». Тема этого года: «Управление ИТ: особенности текущего периода».

3 марта 2023

Воронеж • Лекция
Семинар Труконф о видеоконференцсвязи и совместной работе в Воронеже

4 марта 2023–20 мая 2023

Онлайн-трансляция • Курс
Основы программирования на C++. Уровень 1

6 марта 2023–6 апреля 2023

Онлайн-трансляция • Курс
Основы программирования на Java. Уровень 1

13–14 марта 2023

Москва • Онлайн-трансляция • Конференция
DevOpsConf

14 марта 2023

Москва • Онлайн-трансляция • Конференция
HR IT DAY | IT-talantы: как привлекать, развивать и удерживать

14 марта 2023–20 апреля 2023

Онлайн-трансляция • Курс
SQL. Основы работы с БД

14 марта 2023–13 апреля 2023

Онлайн-трансляция • Курс
Алгоритмы для разработчиков

15 марта 2023–28 июня 2023

Онлайн-трансляция • Курс
Data Scientist

15 марта 2023

Онлайн-трансляция • Митап
Golang meetup (Online)

18 марта 2023

Омск • Хакатон
OmWars CTF

22–23 марта 2023

Москва • Конференция
GO DIGITAL

22 марта 2023

Онлайн-трансляция • Митап
Online IT HR meetup 12.56

23 марта 2023

Москва • Онлайн-трансляция • Конференция
Ежегодная конференция «Цифровая медицина «23»

28 марта 2023–29 июля 2023

Санкт-Петербург • Онлайн-трансляция • Курс
UX | UI дизайнер

29 марта 2023

Онлайн-трансляция • Митап
Python meetup (Online)

30 марта 2023

Москва • Онлайн-трансляция • Форум
BIG DATA&AI 2023

31 марта 2023

Москва • Конференция
День гостиничного ИТ

3 апреля 2023–8 июня 2023

Санкт-Петербург • Онлайн-трансляция • Курс
Автоматизация тестирования ПО (Java). Basic

4 апреля 2023–9 июня 2023

Онлайн-трансляция • Курс
Основы программирования на Python. Уровень 1

Сканворд



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



1		3		2	
		Овощная «плантация»	1	Философ Жан-Жак	Птица с красным хохолком
		Сленговое название конкурента евро	Сумма после подсчета	Валюта Гаити	
Аппарат для писем по телефону	Машинное масло	Краснокоричневая краска	8	Щель между деталями	Для ловли рыбы
Баранко-видная фигура	Герой поэмы Пушкина «Цы-ганы»	Ветер-брат Боррея, Зефира и Нота	Собака из фразы наоборот	Подсадная птица	Дебаты по поводу цены
2	Жорж... автор «Кармен»	4	Лежанка авосечной вязки	Древнеримская медная монета	3
«Отец...» (О. Бальзак)	Майский жук	Способ отвлечься от реальности	«Район» интернета	Село, ушедшее в горы	Поглоща-тель харчей
Городошная чурка	Геологическая разведка	Были бы кости, а оно нарастет	Перемывание чужих костей	Польский танец	Африканская река рекордной длины
Все артисты как коллектив	Автокросх с речным названием	Английская земельная мера	Пропуск, пробел в тексте	Самое северное дерево в мире	Фитиль для прикуривания (устар.)
	Денежка Папуа-Новой Гвинеи	7	4	Роль Ляли Жемчужной	3

1 2 3 4 5 6 7 8

Ключевое слово



ИТ-КОНКУРС КРАСОТЫ BEAUTY & DIGITAL

Приглашаем девушек работающих в ИТ-сфере
принять участие во всероссийском ежегодном
ИТ-конкурсе красоты «Beauty&DiglTal» 2023

CIS - Современные Информационные Системы
www.cissmiss.ru

