КИБЕРУГРОЗЫ ПРОДЛИЛИ ТРЕНД / 3
«УМ» С РЕЗЕРВОМ ДЛЯ РАЗВИТИЯ / 4
НЕОДНОРОДНЫЙ ПРОЦЕСС / 6

Цифровая экономика

Четверг, 27 июня 2024
Тематическое приложение
к газете «Коммерсантъ» **№19**

Коммерсантъ
ONLINE

Guide

реклама 16+

Коммерсантъ в лучших местах Петербурга

РЕСТОРАНЫ

Бар-ресторан «География»	Рубинштейна ул., 5
Дворяне	Почтамтская ул., 1
«Кремль»	Выборгская наб., 55 (БЦ Gregory's Palace)
«Метаморфоз»	Литейный пр., 5/19
Панорамный ресторан «На Поляне»	Свердловская наб., 44 Д
Ресторан-гостиная «Штакеншнейдер»	Миллионная ул., 10
Ресторан русской кухни Siberika	Лейтенанта Шмидта наб., 43
Ресторан «Сыроварня»	Ковенский пер.,5
«Сказка Востока 1001 ночь»	Лесной пр., 48
«Таверна Гролле»	Большой пр. В. О., 20
«Шаляпин»	Тверская ул., 12/15
Cafe Claret	Марата ул., 11
Le Vernissage	Римского-Корсакова пр., 5–7
Marius	Марата ул., 11
SETTLERS	Наличная ул., 24/1 А
Stroganoff Steak House	Конногвардейский б-р, 4

КАФЕ

Пространство Freedom	Казанская ул., 7
Kroo cafe	Суворовский пр., 27 / 9-я Советская ул., 11

ГОСТИНИЦЫ

«А1 Отель Санкт-Петербург»	Кирпичный пер., 3
Бутик-отель Miris	Всеволода Вишневского ул., 1 А
Бутик-отель «Северный цветок»	Марата ул., 40
«Гранд Отель Мойка 22»	наб. реки Мойки, 22
«Гранд Отель Эмеральд»	Суворовский пр., 18
Екатерина	Миллионная ул., 10
«Лотте Отель Санкт-Петербург»	Антоненко пер., 2, стр. 1
Отель «Гельвеция»	Марата ул., 11
Отель «Индиго»	Чайковского ул., 17
Отель «Братья Карамазовы»	Социалистическая ул., 11 АВ
Отель «Коринтия Санкт-Петербург»	Невский пр., 57
Отель «Мартин»	Марата ул., 12
Отель «Невский Берег»	Невский пр., 122
Отель «Традиция»	Добролюбова пр., 2
Официальная гостиница «Эрмитаж»	Правды ул., 10
Талион Империал Отель	наб. реки Мойки, 59
Airportcity Plaza St. Petersburg	Стартовая ул., 6 А
Akyan Hotel	Восстания ул., 19
Author Boutique Hotel	Владимирский пр., 9
Cosmos St. Petersburg Olympia Garden Hotel	Батайский пер., 3 А
«Cronwell Inn Стремянная»	Стремянная ул., 18 А
Crowne Plaza St. Petersburg — Ligovsky	Лиговский пр., 61
DIPLOMAT Hotel	Дегтярный пер., 7 А
Grani Aparthotel	Большая Зеленина ул., 24
Four Seasons Hotel Lion Palace St. Petersburg	Вознесенский пр., 1
Majestic Boutique Hotel Deluxe	Садовая ул., 22/2
M-hotel	Садовая ул., 22 (вход с переулка Крылова, 2, со двора)
Novotel Санкт-Петербург Центр	Маяковского ул., 3, лит. А
Palace Bridge Hotel	Биржевой пер., 4 А
The Gamma Hotel	наб. Обводного кан., 130
Trezzini Palace Hotel	Университетская наб., 21
Welton Club Hotel & Apartments	Малая Разночинная ул., 11

ИНТЕРЬЕРНЫЕ МАГАЗИНЫ

Салон «Сентябревъ»	Каменноостровский пр., 19

БИЗНЕС-ЦЕНТРЫ

Деловой центр NEVKA	Гельсингфорсская ул., 3, к. 11 Д, вход с Выборгской наб., 45–47
Коворкинг «Пушкин»	Торжковская ул., 5
«Оскар»	наб. реки Фонтанки, 13 А
Gregory`s Palace	Выборгская наб., 55
Gustaf	Средний пр. В. О., 36/40
Magnus	9-я линия В. О., 34

АВТОСАЛОНЫ

Автодом «Пулково»	Пулковское ш., 14 А
Петровский на Софийской	Софийская ул., 87
Gregory`s Cars	Выборгская наб., 55

АВИАКОМПАНИИ

ГТК «Россия»	
ЦБА «Пулково-3»	

РАЗНОЕ

Аэропорт Пулково	бизнес-салоны, VIP-зал
Генеральное консульство Индии в Санкт-Петербурге	Рылеева ул., д. 35
Генеральное консульство Республики Узбекистан в Санкт-Петербурге	4-я Красноармейская ул., 4, лит. А
Единый Центр Документов	Красного Текстильщика ул., 10/12
Поезда «Сапсан»	бизнес-класс

Узнайте подробную информацию о корпоративной подписке по телефону 8 800 600 0556 (звонок по России бесплатный) или электронной почте podpiska@kommersant.ru

www.kommersant.ru



ВАЛЕРИЙ ГРИБАНОВ,
РЕДАКТОР GUIDE
«ЦИФРОВАЯ ЭКОНОМИКА»

ДВИГАТЕЛИ ПРОГРЕССА С ПОБОЧНЫМ ЭФФЕКТОМ

Цифровизация в России идет даже быстрее, чем планировали в федеральном правительстве пять лет назад. По плану, к настоящему времени уровень Digital IQ (уровень цифрового развития) экономики РФ должен был достигнуть 64,2%, а в реальности сейчас составляет 74,4%. Жизнь обгоняет мечту: Россия сегодня входит в топ-10 стран по диджитализации государственных услуг.

Но с таким уровнем вовлеченности цифровых сервисов во все сферы жизни неизбежно возникает и угроза кибератак. И чем более цифровизирована экономика — тем опаснее для нее становятся киберугрозы. С ростом уровня диджитализации пропорционально повышается и число хакерских атак. Преступления связаны как с мошенническими практиками, так и с попытками воздействовать на объекты критической информационной инфраструктуры страны.

В таких условиях расходы на защиту от хакерских атак растут внушительными темпами: в прошлом году рынок кибербезопасности России увеличился более чем на треть и достиг двухсот с половиной миллиардов рублей.

Казалось бы, необходимость тратить большие средства на противодействие цифровым преступлениям бьет по экономике и тормозит ее развитие — сотни миллиардов рублей пригодились бы и для вложения в производства, строительства инфраструктуры и прочих объектов.

Но если поглядеть с расстояния, выходит, что и киберпреступники, и киберзащитники двигают прогресс. Необходимость постоянно находиться в тонусе, быть в вечном поиске решений для создания надежного щита порождает неожиданные побочные продукты, которые могут оказаться полезными и в других сферах. Это как с «Виагрой»: изначально искали лекарство от ангины, но побочный эффект принес гораздо большие прибыли.

↑
КОЛОНКА РЕДАКТОРА

КИБЕРУГРОЗЫ ПРОДЛИЛИ ТРЕНД

В РОССИИ ЗА 2023 ГОД КОЛИЧЕСТВО АТАК НА ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ (КИИ) УВЕЛИЧИЛОСЬ НА 16% И ДОСТИГЛО 65 ТЫСЯЧ. ВЛАДИМИР КОЛОДЧУК

Такие данные приводит Национальный координационный центр по компьютерным инцидентам (НКЦКИ). По его информации, одна из самых частых причин уязвимостей — использование иностранного программного обеспечения без технической поддержки и обновлений. Эксперты указывают, что основные прошлогодние тренды сохранились в первой половине 2024-го. Среди них — увеличение количества крупных хакерских атак и рост скорости несанкционированного проникновения в IT-инфраструктуру; развитие российскими вендорами новых продуктов, у которых ранее не было особых перспектив из-за доступности качественных западных аналогов; сосредоточение отечественных решений по обеспечению информационной безопасности (ИБ) в сегменте облачных сервисов.



ЕВГЕНИЙ ПАВЛЕНКО

ОБЪЕМ ОТЕЧЕСТВЕННОГО РЫНКА КИБЕРБЕЗОПАСНОСТИ СОСТАВИЛ В 2023 ГОДУ ОКОЛО 252 МЛРД РУБЛЕЙ, ЧТО НА 35% БОЛЬШЕ 193 МЛРД В 2022-М

ПЕРЕХОД НА ОТЕЧЕСТВЕННОЕ

Полгода назад правительство РФ установило сроки перехода на отечественный софт для госкорпораций и компаний с госучастием. Согласно методическим рекомендациям Минцифры от 12 января, российские операционные системы, офисные пакеты, системы виртуализации и антивирусные программы обязательны к использованию с 1 января 2025 года, а системы управления базами данных (СУБД) — с 1 января 2026-го. Ранее это относилось только к объектам критической информационной инфраструктуры.

Исходя из указа президента Владимира Путина от 30 марта 2022 года, госорганам и компаниям с госучастием с 1 января 2025-го запрещается применять на объектах КИИ иностранное программное обеспечение (ПО). Переход же на доверенные программно-аппаратные комплексы (ПАК) должен завершиться к 1 января 2030 года. Кроме того, как следует из постановления кабмина от 14 ноября 2023 года № 1912, субъекты КИИ не смогут использовать на значимых объектах недоверенные ПАК, если те приобретались после 1 сентября.

К субъектам КИИ относятся юрлица, которым на праве собственности, аренды или ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления в сферах здравоохранения, науки, транспорта, в топливно-энергетическом комплексе, банковском секторе и других значимых отраслях экономики.

По данным Центра компетенций по импортозамещению в сфере информационно-коммуникационных технологий, доля отечественного ПО в закупках госкомпаний в 2022 году составляла 87,1% в количественном выражении и 54,2% в денежном. При этом 89% всех контрактов общей стоимостью 1,9 млрд рублей приходилось на российскую СУБД Postgres Pro. До ухода с отечественного IT-рынка зарубежных компаний, в 2021 году в сегменте СУБД лидером была американская корпорация Oracle с портфелем в 84% от общего числа контрактов (около 4 млрд рублей).

«У субъектов КИИ осталось совсем немного времени для перехода на отечественные решения, и пока складывается ощущение, что от истории с импортозамещением выиграют только те из вендоров ИБ, кто успел включить свои продукты в Реестр отечественного оборудования и ПО, а также получил сертификаты регуляторов. При этом самим вендорам не хватает времени на развитие продуктов, заказчики же требуют качества и цен, сопоставимых с теми, которые предлагали ушедшие с рынка западные компании»,— говорит генеральный директор облачного провайдера НУБЕС (Nubes) Василий Степаненко.

В целом объем отечественного рынка кибербезопасности составил в 2023 году около 252 млрд рублей, что на 35% больше 193 млрд в 2022-м. Заметим, что общий объем по продуктам и услугам ИБ в 2022 году вырос менее чем на 4% в сравнении с показателями 2021-го.

Господин Степаненко поясняет, что выручка самых крупных ИБ-вендоров России за 2023 год составила около 110 млрд рублей, игроков поменьше — приблизительно 50 млрд. Продление ежегодных лицензий — около 32 млрд рублей. При этом интеграционные услуги на рынке ИБ, по словам эксперта, оценить сложно, так как зачастую это сервисное обслуживание, оказываемое из года в год без дополнительных продаж. Поэтому с учетом интеграции объем рынка кибербезопасности в России может быть значительно больше, чем 250 млрд рублей, уточняет спикер.

ТРЕНДЫ И ПРОБЛЕМЫ

Эксперт по информационной безопасности компании Axenix Евгений Качуров выделяет на российском рынке ИБ два важных тренда последнего полугодия.

Первый — резкий взлет количества крупных хакерских атак и сопутствующий ему рост скорости, с которой злоумышленники проникают в IT-инфраструктуру жертвы. Тенденция, по словам эксперта, обусловлена появлением у хакеров новых навыков, увеличением финансирования (реализация масштабной атаки требует огромных средств), а также тем, что отечественные программные продукты, которыми заказчики замещают зарубежные, часто недостаточно исследованы на уязвимости.

Снизить риск крупным компаниям помогает тщательная проверка IT-контура, в том числе с помощью пентестов, усиление средств защиты и использование услуг SOC, отмечает господин Качуров.

Более революционным он называет второй сохраняющийся с прошлого года тренд — фейковые коммуникации с помощью искусственного интеллекта (ИИ). По словам представителя Axenix, злоумышленники так умело применяют ИИ-технологии, что, например, «могут подделать голосовое сообщение или видеозвонок, таким образом заставив жертву перевести им деньги или выдать персональные данные».

«Для защиты от этой угрозы пользователям мессенджеров и соцсетей нужно проявлять максимальную бдительность, стараться замечать признаки аномального поведения коллег и друзей»,— говорит эксперт.

В свою очередь, господин Степаненко относит к основным тенденциям ИБ в первом полугодии развитие российскими вендорами новых продуктов, лишенных ранее особых перспектив из-за доступности качественных западных аналогов. В этой группе решения класса NGFW, WAF, сканеры уязвимостей и прочее.

«На отечественном рынке тем временем продолжают осваиваться азиатские ИБ-вендоры. Их продуктов нет в квадрантах Gartner, и они пока не вкладывают огромные деньги в рекламу на территории РФ, но это крупнейшие вендоры ИБ в Китае и Индии, которым явно интересен рынок России»,— отмечает спикер.

Еще одним трендом 2023–2024 годов он считает сосредоточение отечественных вендоров на разработке и выпуске полноценных облачных версий своих продуктов. Долгое время SECaaS («ИБ как услуга») заключался лишь в помесячной оплате, а мультитенантность решений оставалась в бэклогах.

Из проблем на рынке ИБ эксперт выделяет бездумное использование решений с открытым исходным кодом.

«На рынке появляются IT-стартапы, которые пытаются решить задачи ИБ на базе opensource-разработок. Среди таких задач, например, защита контейнерных сред (kubernetes); безопасность новых почтовых систем; обеспечение бэкапа и так далее. При этом многие угрозы являются следствием бездумного использования opensource-решений. Теперь потенциальный нарушитель — это разработчик, выкладывающий в opensource свой код, но в какой-то момент начинающий встраивать в него зловредный функционал для пользователей из конкретных стран, для носителей языков и так далее»,— уточняет господин Степаненко.

По мнению ведущего инженера CorpSoft24 Михаила Сергеева, предотвращение кибератак требует комплексного подхода с использованием целого ряда инструментов и методов. Тем самым компания создаст надежную систему защиты от угроз и минимизирует риск утраты и компрометации данных.

К полезным инструментам специалист относит антивирусное ПО («Касперский», Dr Web); системы обнаружения и предотвращения вторжений (Snort, Suricata, Palo Alto Networks); межсетевые экраны (pfSense, Windows Firewall); многофакторную аутентификацию (Google Authenticator, Microsoft Authenticator, Яндекс Ключ) и сегментацию сети (разделение ее на сегменты для ограничения распространения угроз).

Господин Сергеев рекомендует не забывать и о резервном копировании и шифровании данных, а также об обучении сотрудников основам кибербезопасности. ■

«УМ» С РЕЗЕРВОМ ДЛЯ РАЗВИТИЯ

В ПОСЛЕДНЕЕ ВРЕМЯ НЕКОТОРЫЕ ДЕВЕЛОПЕРЫ ДЕКЛАРИРУЮТ ОТКАЗ ОТ «ИЗЛИШНЕЙ» ЦИФРОВИЗАЦИИ ЖИЛЬЯ, ПОЛАГАЯ, ЧТО ПОТЕНЦИАЛЬНЫЕ ПОКУПАТЕЛИ СЛИШКОМ ПРЕСЫТИЛИСЬ ВХОЖДЕНИЕМ ИНТЕЛЛЕКТУАЛЬНЫХ УСТРОЙСТВ В ИХ ЖИЗНЬ. НАСКОЛЬКО ОПРАВДАННО ТАКОЕ СДЕРЖИВАНИЕ, РАЗБИРАЛСЯ КОРРЕСПОНДЕНТ GUIDE. КИРИЛЛ КОСОВ

Строительные компании еще с пандемии взяли на вооружение цифровую трансформацию бизнеса. Если сначала цифровизация воспринималась застройщиками как возможность увеличить объемы продаж за счет дистанционного заключения сделки с клиентом без привязки к определенной локации, то сейчас для многих объектов это уже конкурентное сервисное преимущество.

Девелоперы начинают позиционировать жилье как в той или иной степени цифровизованное. «Однако стремление некоторых компаний перегрузить свои проекты цифровизацией не нашло отклика у массового покупателя»,— считает коммерческий директор Plus Development Елена Тарасова. По ее подсчетам, «полностью цифровизованные» проекты интересны лишь отдельным целевым группам. «Например, это молодежь от 25 до 35 лет, „продвинутый IT-сегмент“»,— говорит эксперт.

Другие целевые группы опция «Умный дом», реализуемая застройщиком, привлекает не слишком. Кому-то это кажется неоправданным удорожанием проекта, кто-то просто не склонен разбираться в технических нюансах.

Поэтому сегодня более успешной представляется «разумная цифровизация»: когда участник девелоперского рынка реализует в своем проекте необходимый минимум и создает возможности для последующего подключения тех или иных систем по желанию жильцов многоквартирного дома.



АЛЕКСАНДР КОРЖОВ

ЭКСПЕРТЫ УТВЕРЖДАЮТ: ПОТРЕБИТЕЛИ НЕ ПРЕСЫТИЛИСЬ ГАДЖЕТАМИ, А, СКОРЕЕ, НАУЧИЛИСЬ ИМИ ПОЛЬЗОВАТЬСЯ И ОЧЕНЬ ХОРОШО ПОНИМАЮТ, КАКИЕ НУЖНЫ, А КАКИЕ ИЗБЫТОЧНЫ

ВСЕ ДЛЯ УДОБСТВА Генеральный директор агентства недвижимости «КВС» Анжелика Альшаева рассказала, что ГК «КВС» разработала приложение, которое позволяет собственникам квартир управлять недвижимостью прямо с экрана мобильного телефона. «С помощью приложения „КВС для жизни“ клиент может круглосуточно поддерживать связь с управляющей компанией, вызывать на дом мастеров — сантехников и электриков, — а также оценивать выполненные работы»,— подчеркнула госпожа Альшаева.

Коммерческий директор группы «Аквилон» в Санкт-Петербурге и Ленобласти Наталия Коротаевская отмечает, что системы умного дома уже неотъемлемая часть современных жилых комплексов. «Но это не просто интересная фишка, это часть системы безопасности, комфорта и экономии денежных средств жителей и их времени. Поэтому пресыщение гаджетами, возможно, стоит понимать в плане переизбытка предложения по ряду функций, которые не так уж и важны именно для качества жизни»,— обратила внимание она.

С этим согласен управляющий партнер девелоперской компании Stenoy Илья Фролов. Он считает, что часто отказ от цифровизации жилья объясняется не тем, что клиенты пресытились гаджетами, а широким распространением бесполезных и даже вредных умных устройств, которые в лучшем случае просто создают нагрузку на проект, а в худшем (это очень распространено в новых жилых домах) — проблемы проживающим. «Так, сбой в работе лифтов вызывает пробки на 20–40 минут и не позволяет комфортно пользоваться жильем, умное освещение часто раздражает резидентов, а электрофицированные распашные двери с датчиками приближения на высоком трафике выходят из строя и их становится практически невозможно открыть вручную»,— перечисляет слабые места эксперт.

Госпожа Коротаевская добавила, что ее компания разработала систему inHOME с предустановленным пакетом функций и рядом опций, которые жители домов могут подключить по своему желанию.

«Предустановленные функции обеспечивают бесключевой доступ на территорию ЖК и в дома, в системе работает видеонаблюдение в МОПах и дворах, подключены датчики дыма, протечек, которые перекрывают воду в нештатной ситуации, датчики открытия дверей, режим standby, позволяющий удаленно отключить электропитание и прочее. Эти элементы, на наш взгляд, крайне важны, поэтому мы реализуем их во всех проектах. Остальные опции: умные выключатели, управление теплыми полами, шторами и тому подобное — жители наших домов могут выбирать или не выбирать как дополнение»,— делится с Guide коммерческий директор группы «Аквилон» в Санкт-Петербурге и ЛО.

ОБЯЗАТЕЛЬНЫЙ ЭЛЕМЕНТ Директор департамента недвижимости группы ЦДС Сергей Терентьев полагает, что технологическая оснащенность и цифровизация процессов сейчас необходимое условие для эффективного управления и поддержки роста любого бизнеса, претендующего на лидерство. «Обрабатывать огромный объем информации, существующий на сегодняшний день, без автоматизации невозможно. Так что в компании этому процессу уделяется первоочередное внимание»,— рассказывает эксперт.

Генеральный директор Element Development Виталий Коробов с тем, что клиенты устали от гаджетов, не согласен. «Цифровые решения в премиальных проектах используются для повышения комфорта и безопасности жильцов. Они позволяют контролировать и автоматизировать различные функции в доме, включая освещение, микроклимат, безопасность, автоматику, мультимедиа, электрику.

Премиальные системы обеспечивают расширенный функционал, контроль территории, оповещение хозяина о событиях, а также управление домашним персоналом и сложными инженерными системами. Я полагаю, что насыщения не произойдет: с каждым годом жизнь становится все комфортнее и комфортнее. От этого устать нельзя»,— категоричен господин Коробов.

Начальник отдела цифровизации «Главстрой Санкт-Петербург» Константин Иваницкий рассуждает: «Цифровизация — закономерное развитие технологий строительства жилых комплексов и изменение представления клиента о классности жилья. Если ранее система «умный дом» была доступна только покупателям квартир премиум-сегмента, то теперь становится обязательным атрибутом в ЖК комфорт-класса. Кроме того, клиенты вследствие интенсивного повышения цифровой грамотности и распространения информационных технологий в быту выдвигают повышенные требования к „интеллекту“ продуктов девелоперов»,— предупреждает эксперт.

На взгляд господина Иваницкого, эти решения оправданны, так как закрывают важные потребности жильцов в безопасности, приватности и экономии ресурсов. «Так, IP-видеонаблюдение и IP-домофония позволяют в режиме реального времени следить за играющими во дворе детьми, регулировать доступ посторонних на территорию квартала и дома, предупреждать возникновение несчастных случаев и оперативно обнаруживать нарушителей порядка»,— перечисляет начальник отдела компании «Главстрой Санкт-Петербург».

С помощью современного оснащения также можно своевременно собирать показания приборов учета воды и электроэнергии и контролировать потребление ресурсов. «Наконец, такая недвижимость — это экономия времени. С помощью приложения на телефоне или планшете жители открывают и закрывают калитки, шлагбаумы, двери и т. д. Набор опций расширяется по желанию потребителя, но не исключаю, что со временем технологии станут еще более функциональными»,— полагает господин Иваницкий.

ИГНОРИРОВАТЬ НЕЛЬЗЯ Девелоперы в сегменте комфорт-класса уже интегрируют технологии, которые позволяют дистанционно включать и выключать электричество в каждой комнате, делать свет более ярким или приглушенным, отключать розетки, отслеживать проникновение в квартиру, перекрывать горячее и холодное водоснабжение и даже подключать к телефону видеокамеру домофона и смотреть, кто звонил к вам в ваше отсутствие. Все это помогает сохранить имущество в безопасности, не допускать перерасхода воды, особенно если кран неисправен.

«Однако нельзя сказать, что для большинства покупателей цифровая инфраструктура является определяющей при покупке квартиры. Тем более что в среднем такая система стоит от 80 тыс. рублей и выше. Техноэнтузиасты могут самостоятельно оснастить дом похожими по функциональности приборами, но у самих девелоперов пока нет острой необходимости в системной установке: особых конкурентных преимуществ не получишь. Даже покупатели, которые выбрали квартиру с функциями умного дома, не включают эти функции в повседневную жизнь»,— аргументирует руководитель направления разработки продукта ГК «А101» в Санкт-Петербурге Булат Мирзаханов.

«Со временем эти технологии неизбежно будут распространяться, „умные“ функции охватят больше бытовых мелочей и мы, скорее всего, просто не заметим, как это случится. Но пока массовый потребитель, как в случае с любыми другими цифровыми технологиями, в них не заинтересован», — говорит господин Мирзаханов.

Директор по маркетингу LEGENDA Всеволод Глазунов объясняет: «На наш взгляд, потребители не пресытились гаджетами, а, скорее, научились ими пользоваться и очень хорошо понимают, какие нужны, а какие избыточны. Очевидно, что количество и доступность технологий, повышающих комфорт через цифровизацию взаимодействий в квартире,— это актуальный тренд, который нельзя игнорировать».

Вице-президент по маркетингу и продукту группы RBI Михаил Гущин считает, что все еще впереди: «Мы находимся не на том этапе развития девелоперского продукта, чтобы можно было говорить о пресыщении жителей дома цифровыми сервисами. Все же проекты, полностью оснащенные системами с искусственным интеллектом,— штучный продукт, таких примеров на рынке немного. Причем владельцы там, как правило, сами комплектуют квартиру интеллектуальными помощниками. То есть отдают себе отчет о ежедневных потребностях и понимают, какие цифровые сервисы должны их удовлетворять. Но как правило, такой индивидуальный подбор опций относится к индивидуальному же проектированию в высоких классах жилья». ■

«УСТОЯТЬ ПРИ ВЫСОКОМ УРОВНЕ КИБЕРАТАК В ОДИНОЧКУ ДОРОГО, А ИНОГДА НЕВОЗМОЖНО»

В СЛОЖИВШЕЙСЯ ГЕОПОЛИТИЧЕСКОЙ СИТУАЦИИ РОССИЙСКИЕ ГОСОРГАНИЗАЦИИ И БИЗНЕС ПРОДОЛЖАЮТ ПОДВЕРГАТЬСЯ МАССИРОВАННЫМ КИБЕРАТАКАМ, ЧТО ЗАСТАВЛЯЕТ IT-КОМПАНИИ МАКСИМАЛЬНО БЫСТРО ИСКАТЬ И ВНЕДРЯТЬ ЭФФЕКТИВНЫЕ РЕШЕНИЯ ДЛЯ ОТРАЖЕНИЯ ТАКИХ УГРОЗ. КОРРЕСПОНДЕНТ GUIDE ПОГОВОРИЛ С ЗАМГЕНДИРЕКТОРА — ТЕХНИЧЕСКИМ ДИРЕКТОРОМ КОМПАНИИ «ГАЗИНФОРМСЕРВИС» НИКОЛАЕМ НАШИВОЧНИКОВЫМ О ТРЕНДАХ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ИБ) В 2024 ГОДУ, СТРАТЕГИЯХ И СПОСОБАХ ЗАЩИТЫ ИНФРАСТРУКТУРЫ КЛИЕНТОВ, АУТСОРСИНГЕ И МОДЕЛЯХ ВЗАИМОДЕЙСТВИЯ ЗАКАЗЧИКОВ И ИСПОЛНИТЕЛЕЙ В ИБ. ВЛАДИМИР КОЛОДЧУК


«ГАЗИНФОРМСЕРВИС»

GUIDE: Какие тенденции сейчас актуальны в сфере информационной безопасности? С какими проблемами сталкивается отрасль?

НИКОЛАЙ НАШИВОЧНИКОВ: Чем сильнее цифровизация и автоматизация проникают во все сферы жизни, тем больше становится угроз информационной безопасности для государства и бизнеса. В процессе поиска универсальных решений директора по информационной безопасности (CISO) пересматривают привычные, а иногда и устаревшие стратегии, выбирая новые концепции. Появляется множество новых угроз, нарушающих устойчивость функционирования цифровых экосистем. Россия — один из лидеров среди стран мира по уровню проникновения IT-технологий во все сферы жизни общества. И любой современный бизнес в нашей стране сегодня является по-своему полнофункциональной цифровой экосистемой. Но за плюсы иногда приходится платить. С 2022 года поднялась волна кибератак на государственные организации, частные компании, но и простые люди тоже от этого страдают.

G: Могли бы привести примеры?

Н. Н.: В новостях часто передают громкие истории о кибератаках на компании. Возьмем, например, СДЭК — это гигантский игрок, который недавно из-за атаки на цифровую платформу потерял примерно 1 млрд рублей за пять дней. Или была хакерская атака на сеть магазинов «Верный»: сопоставимые потери в денежном эквиваленте. А ведь это только два резонансных случая за май — июнь 2024 года.

Согласно отчету Аналитического центра кибербезопасности «Газинформсервиса», в 2022–2023 годах в России массово происходили утечки данных и основные удары злоумышленников за это время приходились на сферы доставки, ритейла и финансов. Жизненный цикл атаки содержит этап разведки, подготовки — именно на этом этапе происходят утечки, а потом злоумышленник проникает в цифровую экосистему и закрепляется. В мае и июне вторжения произошли после утечек, то есть исполнители вначале собрали информацию, проникли в инфраструктуру, закрепились, создали для себя внутри цифровой платформы все необходимые опорные точки — и атаковали… А в 2024-м мы увидим еще больше финансовых потерь и отказов систем. Потому что сейчас хакеры перешли от утечек к закреплению и будут все чаще наносить удары по бизнесу.

G: Как бизнесу защитить себя от киберугроз? Какие стратегии выбирают CISO?

Н. Н.: Традиционный путь защиты известен всем директорам ИБ, и практика показала, что при больших бюджетах держать оборону можно очень долго даже крупному бизнесу с распределенной по всей России инфраструктурой. Конечно, приходится строже контролировать сотрудников, инвестировать в обучение и внедрять новые решения, но есть еще одна проблема, о которой все знают. Бюджеты на ИБ сокращаются — это факт. Да и как им не сокращаться, когда многим компаниям в короткие сроки приходится перестраивать IT-инфраструктуру на новые решения, в том числе под давлением вопросов технологического суверенитета? Еще один вызов — развитие цифровых экосистем. Вместе с ним растет уровень внедрения технологий, меняющих архитектуру и принципы, на которых строится информационная безопасность, меняются правила организации рынка труда и нарастает дефицит кадров в сфере информационной безопасности,— это тоже признанный факт.

Есть санкции и новая реальность, а есть новый виток промышленной революции (Индустрия 5.0), цифровая платформенная революция. Устоять при высоком уровне кибератак в одиночку для компании очень дорого, а иногда и невозможно. Поэтому в информационной безопасности все чаще используется аутсорсинг. Многие компании выбирают тестирование своей инфраструктуры и приглашают команды red-team (этичные хакеры), регулярно проверяя киберустойчивость. Кто-то выстраивает модель взаимодействия с центрами мониторинга (security operations centers). Эффективных решений для обеспечения должного уровня информационной безопасности на самом деле достаточно.

G: Насколько мне известно, аутсорсинг в IT провести сложнее, чем в других сферах. Почему? Не могли бы объяснить его основные принципы в ИБ?

Н. Н.: Я бы выделил не столько принципы, сколько этапы. Вначале руководство компании должно осознать риски и уровень угрозы. А потом оценить их,— для этого есть механизмы и алгоритмы действий. На втором этапе выбирается поставщик. Однако, если обращаться к опытному и надежному партнеру, то аудит информационной безопасности и оценку рисков он должен также брать на себя. Поэтому тут, конечно, многое зависит от опыта и компетенций специалистов ИБ-компании. Если она крупная, известная, давно существует на рынке, то как минимум не станет рисковать репутацией, именем и обязательно проведет аудит, совместно с бизнесом оценит риски и предложит максимально эффективное решение.

На третьем этапе уже определяются границы и условия сотрудничества, разрабатываются и внедряются регламенты, настраивается инфраструктура и выстраиваются бизнес-процессы. Каким бы хорошим ни был специалист по ИБ в SOC, он не сможет гарантировать безопасность, если на стороне бизнеса в критический момент пропадет обратная связь и не будут вовремя предприняты рекомендуемые контрмеры. А дальше, на следующих этапах, — мониторинг, контроль, управление инцидентами и восстановление, обеспечение киберустойчивости и поддержка непрерывности бизнес-процессов.

G: Есть ли взвешенная и наиболее эффективная модель взаимодействия заказчиков и исполнителей в ИБ?

Н. Н.: Глобально их всего три. Создание собственного SOC, но это долго и очень затратно. Второй вариант — использование услуг «внешнего SOC», когда вы просто платите, а компания-подрядчик работает в соответствии с вашими запросами. Это самый простой и экономичный путь. Еще один способ — гибрид: у вас собственный SOC, но для исполнения некоторых функций вы привлекаете специалистов извне. Это, пожалуй, самый сложный способ организации, однако его недостатки (высокая стоимость, скорость развертывания, согласование зон ответственности специалистов) уравновешиваются достоинствами. Такой подход — оптимальное решение для крупных компаний с распределенной инфраструктурой.

Чем хорош «внешний SOC»? Эта модель обеспечивает доступ к передовым технологиям и экспертизе компаниям, которым требуется быстрое развертывание безопасности здесь и сейчас. Конечно же, такая модель еще и приводит к снижению затрат, так как закупка оборудования, построение своего SOC — дело не самое простое. Мы в «Газинформсервисе» как раз работаем по такой модели. Создали свой внутренний SOC, разрабатываем киберполигон и программы для обучения и тренировок специалистов по ИБ и готовы предоставлять ресурсы и услуги на аутсорсинг.

G: Какие еще инструменты можно эффективно использовать в ИБ?

Н. Н.: С уверенностью могу сказать, что услуги Red Teaming (этичный хакинг), Purple Teaming (кибертренировки и киберучения) уже доказали свою эффективность, а иногда это единственный инструмент, который покажет бизнесу, чего на самом деле стоит его команда ИБ.

G: Предоставляет ли «Газинформсервис» такие услуги? Как вы собрали свой SOC и проводите ли тестирование на прочность безопасности инфраструктуры клиентов?

Н. Н.: Да, конечно, мы достаточно давно оказываем услуги тестирования на проникновение, накопили богатый опыт, который пригодился нам сейчас,— когда спрос на них бьет все рекорды.

Часть заказчиков приходит, когда нужно удовлетворить требования регуляторов, но многие, что отрадно видеть,— с целью выявить слабые места в своей информационной безопасности и устранить соответствующие риски для бизнеса. С ростом информатизации начинает расти и грамотность в области ИБ. Тем не менее даже заказчики с тщательно выстроенной системой защиты часто оказываются уязвимы перед целевыми атаками, а мы показываем, где именно.

Новой же услугой для нас стал SOC. Если до недавнего времени компании скептически смотрели на возможность отдать собственную информационную безопасность в руки сторонних профессионалов, то в последние два года большинству стало понятно, что реализовать такую защиту своими же силами — сложно, длительно и дорого. Скажу честно, когда мы увидели зарождающуюся волну интереса к услугам SOC и приняли решение строить собственный, то питали иллюзии, что, имея богатый практический опыт, сможем решить задачу за полгода. Однако даже при всех вводных пришлось потратить больше года, чтобы быть готовыми предоставить рынку результат.

При разработке мы выбирали традиционный подход, который гарантирует надежность решения. Но и от современных трендов, таких как искусственный интеллект (ИИ), мы не отказались, а переложили на машинное обучение рутинные функции и задачи, где применение ИИ дает рост эффективности при детектировании угроз.

В основу легли как наши разработки, так и продукты других отечественных лидеров рынка информационной безопасности. Здесь же пригодился опыт тестирования на проникновение: мы проверяем защищенность нашего SOC, чтобы быть уверенными в безопасности данных своих заказчиков. ■

НЕОДНОРОДНЫЙ ПРОЦЕСС

ПО ОЦЕНКАМ ЭКСПЕРТОВ, ЦИФРОВИЗАЦИЯ В РОССИИ ИДЕТ НЕРАВНОМЕРНО. СРЕДИ ПРИЧИН УЧАСТНИКИ РЫНКА НАЗЫВАЮТ КАДРОВЫЙ ДЕФИЦИТ, НЕОБХОДИМОСТЬ УСКОРЕННОГО ИМПОРТОЗАМЕЩЕНИЯ ИЗ-ЗА УХОДА ЗАРУБЕЖНЫХ ВЕНДОРОВ И НИЗКИЙ УРОВЕНЬ ЦИФРОВОЙ ГРАМОТНОСТИ СПЕЦИАЛИСТОВ В ЦЕЛОМ. ЧЕРЕЗ ДЕСЯТЬ ЛЕТ СТРАНА СТАНЕТ СУЩЕСТВЕННО БОЛЕЕ ДИДЖИТАЛИЗИРОВАННОЙ, А ГОСУДАРСТВО И БИЗНЕС БУДУТ ВЫНУЖДЕНЫ ОЦИФРОВЫВАТЬСЯ, ЧТОБЫ УВЕЛИЧИТЬ ЭФФЕКТИВНОСТЬ И КОНКУРЕНТОСПОСОБНОСТЬ. АЛЕКСАНДРА ТЕН

В 2023 году российский индекс в ежегодном Индексе развития информационно-коммуникационных технологий (ИКТ, рассчитывается Международным союзом электросвязи ООН) был оценен в 88,9. «Это достаточно высокое значение, превосходящее показатели большинства стран, которые наряду с Россией были отнесены авторами исследования к группе стран с доходами выше среднего»,— заметил Евгений Зараменских, профессор, руководитель департамента бизнес-информатики Высшей школы бизнеса НИУ ВШЭ.

ДИДЖИТАЛИЗАЦИЯ В ЦИФРАХ Александр Семенов, генеральный директор ГК «Корус Консалтинг», поделился данными Института статистических исследований и экономики знаний (ИСИЭЗ) ВШЭ, согласно которым за последние несколько лет в стране увеличилось число организаций, применяющих технологии сбора, обработки и анализа больших данных (30,4%), работающих с облачными сервисами (28,9%) и пользующихся услугами ЦОД (16,5%). В 2023 году доля IT-отрасли в ВВП составила 1,96%, что в 1,5 раза больше, чем пять лет назад.

По уровню технологического развития, обращает внимание Татьяна Кулябина, владелица и генеральный директор Holding-Finance Broker, Россия занимает 14-е место в мировой двадцатке стран-лидеров и опережает по этому показателю Нидерланды, Швейцарию, Турцию и одного из наших партнеров по БРИКС — Саудовскую Аравию.

Директор по развитию платформы корпоративных коммуникаций и мобильности eXpress Сергей Артемов оценивает уровень цифровизации в РФ на тройку по пятибалльной шкале. «Это связано с тем, что мы фактически не так давно начали этот процесс, но уже хорошо понимаем, куда двигаться. Конечно, есть текущие трудности, ведь на уровень цифровизации в нашей стране оказало влияние санкционное давление. С одной стороны, оно придало стимул, а с другой — выставило на разных этапах определенные ограничения и барьеры»,— указывает эксперт.

Сергей Чуканов, генеральный директор SimpleOne, считает, что диджитализация в стране остается достаточно низкой, особенно в госсекторе и на крупных промышленных предприятиях. Главные причины этого — традиционный консервативный подход многих компаний и госструктур, нежелание менять устоявшиеся, но неэффективные процессы, страх перед новыми технологиями и опасения за информационную безопасность. Дополнительными трудностями, по мнению господина Чуканова, являются нехватка квалифицированных кадров и низкий уровень цифровой грамотности сотрудников в целом.

НА ПЕРВОМ МЕСТЕ — ГОССЕКТОР И ФИНТЕХ Однако большинство опрошенных экспертов называют госсектор в числе лидирующих отраслей по уровню цифровизации. Руководитель индустриального центра компетенций (ИЦК) «Строительство» при Минстрое РФ, основатель «Аметист Групп» Марат Хафизов напоминает: «Наша страна входит в топ-10 в мире по уровню цифровизации государственных услуг. Сейчас мы можем получить около тысячи таких услуг в электронном виде. Но вместе с тем все сферы сталкиваются с конкретными проблемами на пути к цифровой трансформации. Это санкции, уход западных вендоров, дефицит квалифицированных кадров».



АЛЕКСАНДР КОРЖОВ

С 2019 ГОДА ЦИФРОВАЯ ЗРЕЛОСТЬ РОССИИ (DIGITAL IQ, ПОКАЗАТЕЛЬ ЦИФРОВОГО РАЗВИТИЯ) ДОСТИГАЕТ 74,4% ВМЕСТО ПЛАНОВЫХ 64,2%

Петр Щербаченко, доцент Финансового университета при Правительстве РФ, приводит статистику федерального кабинета министров о том, что с 2019 года цифровая зрелость России (Digital IQ, показатель цифрового развития) достигла 74,4% вместо плановых 64,2%. В 2023 году в онлайн перевели все запланированные социально значимые услуги, а количество пользователей портала «Госуслуги» увеличилось в два раза и достигло 109 млн человек. Затраты на IT превысили 540 млрд рублей. Россия занимает 10-е место в рейтинге Всемирного банка GovTech Maturity Index по уровню цифровизации госуправления, также напоминает он.

Традиционно в цифровых лидерах остаются финансовый сектор, IT, ритейл, e-commerce, а в последние годы и обрабатывающая промышленность. Господин Семенов связывает это с постоянно растущей конкуренцией, а также с кардинальными переменами в этих отраслях: сменой рынков сбыта и поставщиков сырья, перестройкой логистических цепочек, уходом поставщиков зарубежных IT-решений и т. д.

Василий Белов, исполнительный директор ITGlobal.com, тоже полагает, что самые передовые по применению высоких технологий и искусственного интеллекта (ИИ) отрасли экономики — это те, где высокая конкуренция. Для таких компаний использование современных IT-решений — метод борьбы за потребителя. «Поэтому и скорость внедрения передовых IT-решений здесь максимальная»,— констатирует господин Белов.

Елена Баракина, доцент кафедры международного и публичного права юридического факультета Финансового университета при Правительстве РФ, думает, что финансовый сектор выступает флагманом внедрения цифровых инноваций благодаря доступу к значительным инвестициям, а также вследствие непосредственного участия Банка России, который, активно используя свою регулятивную «песочницу», успешно тестирует инновационные решения в финсфере.

Технический директор DIS Group Олег Гиацинтов согласен, что онлайн-банкинг на российском рынке — один из лучших и опережает зарубежные аналоги на несколько шагов. Также очень развита сфера электронной коммерции — приложения маркетплейсов на уровне продукта и пользовательского опыта могут составить достойную конкуренцию западным.

«В нашей стране очень сильная инженерная школа, и это позволяет делать качественные IT-продукты»,— убежден Евгений Перов, директор по продукту в корпоративном мессенджере Compass.

ЦИФРОВОЕ НЕРАВЕНСТВО Участники рынка также сходятся во мнении, что уровень цифровизации в России довольно существенно отличается по отраслям. В отличие от банков, телекоммуникационных компаний и ритейла во многих сферах промышленности цифровизируются только отдельные задачи. «На самом деле эта тенденция соответствует мировой: организации, которым для развития требуется много данных, цифровизируются быстрее»,— объясняет господин Гиацинтов.

Антон Балагаев, директор по консалтингу Arenadata, также считает развитие цифровых технологий в России одновекторным: «Мы умеем оцифровывать процессы: выделять в чем-то аналоговом измеримую составляющую и сохранять ее, для этого у нас есть научно-техническая база, специалисты, лучшие мировые практики. Основные трудности связаны со второй составляющей цифровой трансформации — автоматизацией». Долгое время отечественных автоматизаторов, продолжает господин Балагаев, душили демпингом транснациональные корпорации. «Сейчас возможности есть, но в сравнении с западными вендорами нашим автоматизаторам не хватает наработанного опыта, лояльности клиентов, емкости рынка»,— сетует он.

Признавая неравномерность цифрового развития, эксперты говорят, что высокие технологии пока практически не затронули, например, сферу АПК. Значительные различия по уровню цифровизации регионов и отраслей замечает основатель российско-китайской транспортной компании RusTransChina Александр Стрельников. Бизнесмен напоминает, что до сих пор отсутствует доступ к высокоскоростному интернету на сельских и отдаленных территориях страны.

Татьяна Кулябина объясняет технологическую отсталость аграрной отрасли ее консервативностью. «Технологии разрабатывают в крупных городах, а агробизнес часто находится за сотни и тысячи километров. Правда, крупные агрохолдинги уже начали интегрировать технологические решения в повседневные процессы — теперь дело за более мелкими предприятиями»,— призывает госпожа Кулябина.

ВЗГЛЯД В БУДУЩЕЕ Евгений Александров, руководитель комплекса «Цифровое моделирование материалов» центра НТИ «Цифровое материаловедение» МГТУ им. Баумана надеется, что через десять лет изменится представление обывателя об искусственном интеллекте. Скорее всего, рассуждает ученый, азы этой технологии будут преподавать в школе. «Также ИИ может быть повсеместно внедрен как помощник учителя, водителя, врача. Предположу, что подсчет налогов и их оплата будут производиться автоматически, как и все социальные выплаты: без подачи заявлений, в один клик подтверждения. Больше станет автомобилей с автопилотом»,— обозначает перспективы эксперт.

Андрей Кондратьев, заместитель технического директора по комплексным проектам Step Logic, предполагает, что через десятилетие квантовые вычисления станут привычным делом и вытеснят традиционные вычислители, по крайней мере в корпоративных и облачных ЦОД. Это приведет к смене подхода к разработке ПО. Процесс перестанет быть таким трудоемким, ускорится, а кодером сможет стать практически каждый.

Дмитрий Григорьев, технический директор Step Logic, предупреждает, что дальнейший уровень цифровизации в России будет зависеть от общей политической и экономической ситуации. «Это вовсе не означает, что ограничения в доступе к технологиям, с которыми наша страна столкнулась за последние два года, обязательно отбросят назад. Вероятно, найти ответ на вызовы получится именно через форсированную цифровизацию. Некоторым компаниям — как производителям, так и заказчикам,— поневоле придется стать пионерами: не копировать устаревшие, хотя и широко распространенные в мире модели, а сразу внедрять новые поколения решений»,— рассуждает эксперт. ■

Тематическое приложение к газете «Коммерсантъ» (онлайн-выпуск Санкт-Петербург, Guide «Цифровая экономика»)

Владимир Желонкин — генеральный директор АО «Коммерсантъ», главный редактор
Анатолий Гусев — автор дизайн-макета
Андрей Ершов — главный редактор СПб страниц
Александр Коряков — бильд-редактор
Валерий Грибанов — выпускающий редактор
Евгения Старкова — корректор
Мария Громова — верстка
Марина Победенная — рекламная служба

Адрес редакции и издателя: 123112, г. Москва, Пресненская наб, д.10 этаж 35. Тел. (495) 797-6970. Адрес редакции в Санкт-Петербурге: 191024, Харьковская ул., д. 8А, лит А. Тел. (812) 324-6949

Учредитель: АО «Коммерсантъ».
Тематическое приложение к газете «Коммерсантъ», зарегистрировано Роскомнадзором, регистрационный номер и дата принятия решения о регистрации ПИ №ФС77-76923 от 11.10.2019 года

В печатном виде номер не выходит.
Распространяется бесплатно.
16+

Фото на обложке: Евгений Павленко

ВЕНДОРНЫЙ СУВЕРЕНИТЕТ

СОВРЕМЕННОЕ ПРОИЗВОДСТВО РАЗВИВАЕТСЯ В СТОРОНУ АВТОМАТИЗАЦИИ ПРОЦЕССОВ: РУТИННЫЕ ОПЕРАЦИИ УПРАВЛЕНИЯ И КОНТРОЛЯ ПЕРЕХОДЯТ ОТ ЧЕЛОВЕКА К ПРИБОРАМ И ЦИФРОВЫМ УСТРОЙСТВАМ. КОРРЕСПОНДЕНТ GUIDE РАЗБИРАЛАСЬ, КАК ПРОХОДИТ ТЕХНОЛОГИЧЕСКАЯ ТРАНСФОРМАЦИЯ В КРУПНОМ БИЗНЕСЕ, ЗАДАЮЩЕМ IT-ТРЕНДЫ ДЛЯ ВСЕЙ ПРОМЫШЛЕННОЙ ОТРАСЛИ. ВАСИЛИСА МОТОВА

Автоматизированные системы управления технологическим процессом (АСУ ТП) позволяют добиваться существенного экономического эффекта за счет контроля и снижения простоев и издержек, а также могут быть инструментом инновационного развития для производств. Процесс выпуска продукции осуществляется на основе работы датчиков и контроллеров, а их связь между собой обеспечивают протоколы передачи данных.



АЛЕКСАНДР МИРИДОНОВ

КРУПНЫЕ ИНДУСТРИАЛЬНЫЕ ПРЕДПРИЯТИЯ ВСЕГДА БЫЛИ В АВАНГАРДЕ ТЕХНОЛОГИЧЕСКИХ ИЗМЕНЕНИЙ. СЕГОДНЯ ИМЕННО ОНИ ИСПЫТЫВАЮТ НАИБОЛЕЕ СИЛЬНУЮ ПОТРЕБНОСТЬ В ОБНОВЛЕНИИ АСУ ТП

НА ОСТРИЕ ПРОГРЕССА

Крупные индустриальные предприятия всегда были в авангарде технологических изменений. Сегодня именно они испытывают наиболее сильную потребность в обновлении АСУ ТП. С учетом количества установленных решений замена систем АСУ сейчас слишком дорогостоящая, сопряженная с рисками для бизнеса процедура. «Предложений для автоматизации процессов много, но сложность и стоимость их внедрения настолько высока, что многие компании, начавшие внедрение, не доходят до пожинания плодов, то есть не в состоянии оценить экономическую отдачу,— констатирует руководитель направления отраслевых решений EKF Андрей Ельцов. — Кроме того, предложения, как правило, ограничиваются не самодостаточными процессами, а теми, которые необходимо интегрировать в существующие информационные системы. Это постоянно увеличивает стоимость и сроки внедрения».

По оценкам специалистов, невозможность своевременно обновить системы промышленной автоматизации грозит в среднесрочной перспективе стать ощутимым конкурентным недостатком.

Сейчас на рынке представлены либо иностранные, либо российские, но узкоспециализированные решения, зачастую предыдущего поколения. Компания «Газпром нефть» предложила рассмотреть переход от разрозненных закрытых автоматизированных систем к единой и универсальной платформе промышленной автоматизации.

ОТКРЫТОСТЬ И НЕЗАВИСИМОСТЬ

Речь идет о вендоронезависимой платформе с открытой архитектурой, основанной на открытых международных промышленных стандартах и протоколах и позволяющей строить системы промышленной автоматизации любой специфики.

Принцип открытости АСУ ТП заключается в совместимости всех элементов вне зависимости от производителя. Это достигается за счет открытой архитектуры платформы, открытых интерфейсов и протоколов взаимодействия, доступных всем участникам рынка. Такой подход обеспечивает гибкость в использовании как самими производствами, так и клиентами, поскольку подразумевает возможность разработки сквозных решений, выстраивания сквозных цепочек между предприятиями.

Переход к вендоронезависимой логике и применение современных решений при построении новой архитектуры АСУ ТП позволяет снизить уровень стратегических средне- и долгосрочных рисков и значимо сэкономить на этапах проектирования систем управления для новых объектов строительства, развития и модернизации производства, эксплуатации действующих систем, развернутых в соответствии с этими принципами.

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ

Разрабатывая открытую платформу промышленной автоматизации, компания «Газпром нефть» проводит исследования по ее практическому внедрению в производственные процессы. Компоненты платформы протестированы, подтверждены ее основные свойства. В настоящее время завершено шесть НИОКР-проектов по разработке платформы и оценке ее применимости для различных бизнесов компании.

Пилотные стенды, демонстрирующие принципы и возможности платформы, тестируются на площадках «Газпром нефти» в Санкт-Петербурге, Омске и Тюмени. С 2022 года стенды посетили более 50 компаний из сфер металлургии, химии, нефтехимии, энергетики, представители ведущих вузов, более 30 предприятий — производителей IT-решений и решений для промышленной автоматизации.

В ОБЩИХ ИНТЕРЕСАХ

Концепция платформенности и открытости для сегмента АСУ ТП уже нашла широкую поддержку у крупнейших потребителей в различных отраслях промышленности.

Приказом Министерства промышленности и торговли РФ в августе 2023 года создана рабочая группа по открытым АСУ ТП, в которую вошли более 30 компаний. Всего же участие в ее работе принимают свыше 60 участников рынка. В задачи группы входят разработка и утверждение национальных и отраслевых стандартов, опытно-промышленные испытания и пилотные внедрения для тиражирования решений, а также кросс-отраслевое развитие открытой АСУ ТП.

Платформа развивается в интересах всего рынка с участием крупнейших компаний. Ключевая идея открытой платформы — внедрить в системы автоматизации открытые промышленные стандарты. Единые стандарты позволят обеспечить совместимость различных компонентов и, следовательно, сделают возможным участие в проектах широкого круга разработчиков и производителей таких продуктов.

Автоматизация производства, построенная на открытых стандартах, — задача трудновыполнимая, требующая осознанных совместных усилий от всех участников рынка: федеральных органов исполнительной власти, вертикально интегрированных нефтяных компаний, интеграторов, производителей оборудования и ПО.

Для объединения отраслевых усилий и интенсификации разработки решений для задач нефтегазовой отрасли проект открытой платформы промышленной автоматизации внесен в перечень особо значимых проектов ИЦК «Нефтегаз и нефтехимия», он развивается рабочей группой по проекту открытой платформы промышленной автоматизации Консорциума технологической независимости индустриального ПО и Институтом нефтегазовых технологических инициатив.

«Стремясь стать лидером в направлении промышленной автоматизации, «Газпром нефть» поставила перед собой амбициозную цель. Мы готовы делиться наработками со всеми участниками рынка. Наши основные задачи сегодня: объединение крупных заказчиков для унификации требований на рынке, вовлечение государственных органов, а также разработка концепции для обучения кадров будущего»,— отмечает начальник департамента ИТАТ «Газпром нефти» Антон Думин.

НАУЧНО-ОБРАЗОВАТЕЛЬНАЯ БАЗА

Последняя задача предполагает участие крупного бизнеса в подготовке кадров. В 2024 году по инициативе «Газпром нефти» на базе Санкт-Петербургского политехнического университета Петра Великого (СПбПУ) откроется дополнительная профессиональная программа повышения квалификации (международная образовательная программа) «Киберфизические системы».

С 2025 года выпускники программы станут сотрудниками «Газпром нефти», тем самым осуществив бесшовный переход на российские промышленные решения и получив возможность включиться в работу над созданием платформы как открытой среды разработки с унифицированными требованиями к оборудованию и комплектующим, вендоронезависимым софтверным программируемым логическим контроллером (ПЛК) и другими открытыми решениями.

Задачи по промышленной автоматизации включаются в IT-чемпионат нефтяной отрасли. Конкурсанты в сжатые сроки разрабатывают перспективный комплекс программных средств для моделирования и автоматизации технологических процессов на нефтедобывающих предприятиях с применением концепции «Индустрия 4.0» и современных практик информационных технологий. ■

Коммерсантъ

ПАРТНЕРСКИЙ ПРОЕКТ

ПЕТЕРБУРГ@

Истории бизнеса

320 лет предпринимательства для экономического развития города



РЕКЛАМА, 16+, www.kommersant.ru

Ответственные предприниматели заботятся не только об увеличении доходности своих компаний, но и о том, какой позитивный след они оставят в богатой истории нашего города



«Петербургъ. Истории бизнеса»

Вместе пишем современную энциклопедию петербургских компаний

ПРИНЯТЬ УЧАСТИЕ В ПРОЕКТЕ / **(812) 325-85-96,** e-mail: **M.pobedennaya@kommersant.ru**