Технологическая независимость в России

Введение

В конце мая состоялась встреча Президента России Владимира Путина с представителями отечественных деловых кругов, приуроченная ко Дню российского предпринимательства. Глава государства отметил внесенный в развитие экономики нашей страны в XXI веке вклад бизнеса, включая молодое поколение предпринимателей: “Возрождение сельского хозяйства, строительного комплекса, целых секторов индустрии и современных сервисов, в укреплении нашего суверенитета, в том числе промышленного, технологического, финансового. А без этого суверенитета невозможен никакой другой суверенитет, потому что на этом все стоит, это фундамент”. Также Владимир Путин назвал российское программное обеспечение одним из элементов национальной безопасности. А говоря о работе зарубежных ИТ-сервисов, которые не до конца ушли с российского рынка, президент подчеркнул: “Они нас пытаются “душить” — надо отвечать им взаимностью”.

Одной из российских компаний, производящих ИКТ-оборудование уже более 20 лет, является ООО “Интеком”. Все производимое оборудование проходит обязательную сертификацию. Рассмотрим, насколько важно применять ИКТ-оборудование данного типа именно российского производства.

Диспетчерский центр оперативного управления

Диспетчерский центр оперативного управления (ДЦОУ) — это рабочие места операторов, оснащенные различными средствами индивидуального и коллективного управления, звуковой, видео- или другой компьютерной информацией, получаемой от внешних источников или серверов центра, и предназначенные для мониторинга, анализа и управления процессами в реальном времени.

Рабочие места операторов состоят из эргономичных станций, оснащенных:

специализированными компьютерами с сенсорными экранами и дополнительными сенсорными мониторами для визуализации данных;

средствами управления — клавиатурой, мышью, джойстиками, сенсорными панелями и другими;

системами голосовой связи — рациями, телефонией, гарнитурами;

системами отображения информации (СОИ) — видеостенами (LED, LCD, проекционные), индивидуальными и групповыми экранами для вывода видео, графиков, карт, схем;

источниками данных — внешними системами (датчики, камеры, телеметрия, SCADA, ГЛОНАСС/GPS), внутренними серверами (базы данных, архивы, аналитические системы);

средствами коммуникации — IP-телефонией, радиосвязью, чат-системами;

системами оповещения — сиренами, световыми сигналами;

программным обеспечением — диспетчерскими программами (АСУ ТП, GIS, BMS) и аналитическими системами (AI, машинное обучение для прогнозирования).

Основное применение ДЦОУ — в сфере транспорта (диспетчерские центры управления), энергетики (диспетчеризация, технологическая связь и ТСОП), в промышленности (безопасность и управление производственными процессами), при оповещении и управлении в чрезвычайных ситуациях (МЧС, службы 112).

Такой центр отвечает всем требованиям, включая надежность (резервирование систем), эргономику (удобство работы оператора), защиту данных (пограничные контроллеры, кибербезопасность), и обеспечивает оперативное реагирование на события и эффективное управление ресурсами.

Необходимо, чтобы оборудование для диспетчерского центра оперативного управления было отечественного производства и информация не передавалась за пределы страны. Использование отечественного оборудования и обеспечение суверенитета данных в диспетчерских центрах критически важно, особенно для государственной безопасности (защита от внешнего вмешательства), технологической независимости (отсутствие рисков санкционных ограничений) и контроля над критической инфраструктурой (энергетика, транспорт, оборона).

Ключевые требования к оборудованию и ПО ДЦОУ:

отечественное производство и аппаратное обеспечение серверов и рабочих станций, средств отображения, сетевых решений и программного обеспечения ОС (PARMA, ALT Linux, “РЕД ОС”, Astra Linux);

защита данных (импортозамещение инфраструктуры) — серверы и хранилища должны находиться на территории РФ, использоваться только российские облака (SberCloud, VK Cloud, MTC Cloud);

замкнутый контур управления — локальные сети без выхода в глобальный интернет, если не требуется, VPN и защищенные каналы связи;

соответствие требованиям регуляторов — к импортозамещаемому ПО (Минцифры), к российскому производству печатных плат (Минпром).

Для ДЦОУ критически важно использовать российское оборудование и ПО, чтобы исключить риски утечки данных за рубеж, саботажа (например, отключение зарубежных систем в кризис) и зависимости от иностранных вендоров.

Это особенно актуально для систем управления критической инфраструктурой.

Учрежденческие производственные автоматические телефонные станции

Применение учрежденческих производственных автоматических телефонных станций (УПАТС) российского производства (например, “Плагин”) значительно повышает безопасность переговоров благодаря нескольким ключевым факторам:

отсутствие зависимости от иностранного ПО и “закладок”. Российские УПАТС разрабатываются с закрытым кодом, что исключает наличие уязвимостей, внедренных иностранными разработчиками;

данные не покидают территорию России. Вся обработка сигналов, шифрование и маршрутизация происходят на серверах внутри страны, минимизируя риски перехвата через зарубежные узлы (как в случае с Zoom, Skype, Teams);

соответствие требованиям регуляторов;

защита от киберугроз;

локализация и суверенитет.

Полный цикл производства в РФ исключает риски санкционных ограничений и блокировок со стороны западных вендоров.

Применение этих станций критически важно в госорганах (переговоры МВД, ФСБ, Минобороны РФ), крупных корпорациях (банки, нефтегазовая сфера, энергетика), в транспортной сфере и логистике (защита диспетчерских переговоров). Использование российских УПАТС, таких как “Плагин”, не просто соот-

Сравнение российской УПАТС с иностранными аналогами

Характеристика	УПАТС "Плагин" (РФ)	Cisco Unified CM (США)	Avaya Aura (США)
Шифрование	ГОСТ + СКЗИ	TLS 1.2 (NSA backdoor)	Proprietary
Локализация данных	Только РФ	США/ЕС	США/Ирландия
Цена (на 100 абонентов)	1 млн руб.	4 млн руб. + валютные риски	3,8 млн руб.

ветствует требованиям импортозамещения, но и существенно снижает риски утечки данных, обеспечивая полный контроль над коммуникациями (см. таблицу):

серверы защищены от внешних воздействий пограничными контроллерами сеансов с защитой от DDoS и Deep Packet Inspection с собственной ОС "ПАРМ", или российской Astra Linux, или "РосА", которые сертифицированы ФСТЭК;

совместимость с СЭД (VK WorkMail, Р7-Офис), 1С, "Битрикс24";

замена импортных АТС (Avaya, Cisco) на российские аналоги с развертыванием УПАТС "Плагин" для исключения перехвата через зарубежные серверы (ранее трафик шел через Германию и США);

защита переговоров диспетчеров (риски саботажа и перехвата) за счет установки УПАТС собственной ОС "ПАРМ" и резервирования серверов для повышения отказоустойчивости даже при отключении глобального интернета.

Внедрение состоит из следующих шагов:

аудит текущей АТС (выявление уязвимостей),

миграция из импортных решений (Cisco — "Плагин"),

обучение сотрудников (курсы по кибербезопасности).

УПАТС "Плагин" — это не просто российский аналог, а усиленная защита и суверенитет. Установка проводится в крупнейших учреждениях и компаниях — тех, которые реально заботятся о безопасности внутреннего контура и страны.

Диспетчерский пульт

Диспетчерский пульт ТСОП "Виртуоз" — современное решение для управления технологическими процессами в электроэнергетике, аттестованное ПАО "Россети". Это подтверждает его соответствие требованиям отраслевых стандартов и возможность применения на объектах электросетевого комплекса. Допускается его использование на объектах Россетей, "Газпрома", "Транснефти" и их дочерних компаний.

Среди его функциональных возможностей: управление и мониторинг оборудования подстанций (ТП, РП, ЦП), интеграция с АСДУ, SCADA и другими диспетчерскими системами, визуализация схем электроснабжения, телеметрия, обработка аварийных сигналов.

Область применения: распределительные сети, объекты генерации и распределенной энергетики, промышленные предприятия, городские электросети.

Преимущества диспетчерского пульта: соответствие СТО ПАО "Россети", гибкость настройки под конкретные объекты, поддержка современных протоколов обмена.

Технические особенности: серверы с резервированием, групповая работа рабочих мест диспетчеров, программное обеспечение собственного производства.

При внедрении важны три условия: интеграция с существующими системами, обучение персонала, техподдержка и постоянное обновление программного обеспечения.

Заключение

Сейчас часто говорят о дефиците ИКТ-оборудования из-за ухода крупных западных компаний с российского рынка. Приходится слышать, что российское ИКТ-оборудование не самое дешевое.

В случае же с оборудованием ООО "Интеком" необходимо отметить, что его возможности вполне сопоставимы с западными аналогами, а по некоторым параметрам их превосходят. Оно отвечает требованиям безопасности и доступнее (см. таблицу).

У российского производителя на продвижение своей продукции, к сожалению, нет таких бюджетов, как у западных фирм, поскольку все деньги вкладываются в разработку, производство и модернизацию оборудования. Но те, кто уже использует эти решения, могут подтвердить, что оборудование работает и отвечает всем требованиям и заявленным параметрам.

Рассматриваемый продукт не использует облачные сервисы с отсылкой всей информации за рубеж. Об этом стоит задуматься всем, кто еще применяет небезопасные западные аналоги. А также структурам, которые должны обеспечивать информационную безопасность России.

В России есть альтернатива импортным продуктам!

Материал подготовлен ООО "Интеком"

Круглосуточное противодействие киберугрозам

В мае 2025 года специалисты Центра мониторинга и управления сетью связи общего пользования: заблокировали 13 574 фишинговых ресурса и 72 сайта, на которых распространялось вредоносное программное обеспечение; отразили 952 DDoS-атаки в отношении систем защищаемых субъектов государственного управления, операторов связи, финансового сектора и цифровых сервисов.

Максимальная мощность DDoS-атаки за указанный период достигла 1 Тбит/с, скорость — 90 миллионов пакетов в секунду (п/с). Максимальная продолжительность DDoS-атаки составила 4 дня 3 часа.

Чаще всего атаки совершались с IP-адресов, зарегистрированных на территории США, Германии, Нидерландов, Швеции, Франции.

Было выявлено и устранено 1511 нарушений маршрутизации трафика со стороны 483 организаций.