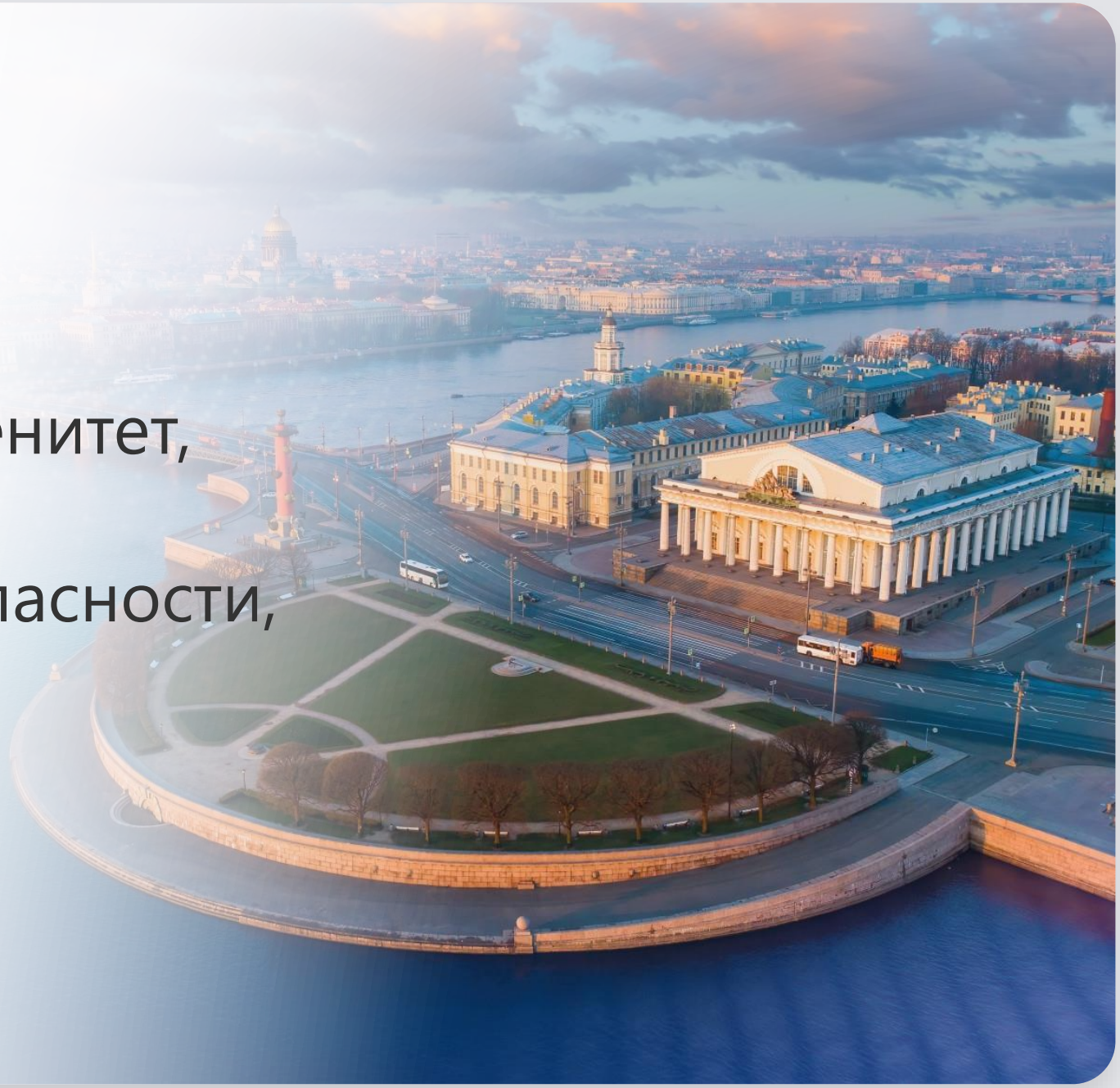
КЕЙСИСТЕМС

Тренды современности: технологический суверенитет, снижение угроз информационной безопасности, цифровые сервисы



СЕРГЕЕВ
Сергей Николаевич

Заместитель генерального директора

Парадоксы «цифрового мира» или можно ли доверять цифровым технологиям?

Мир ИТ полон сомнений

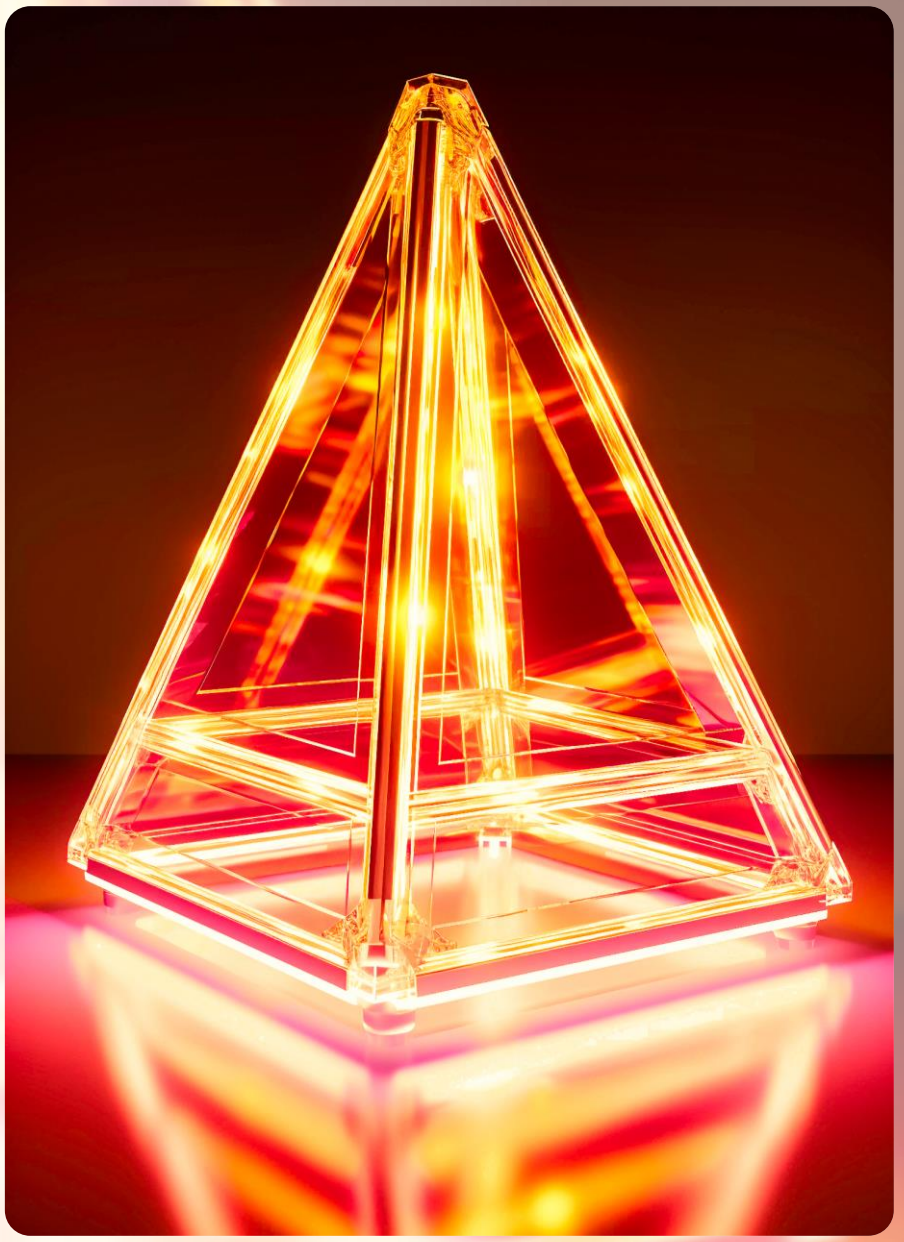
- Можно ли уже доверять российским продуктам и разработчикам?
- Обеспечивается ли информационная безопасность?
- Точно ли электронный документ заменяет бумажный?
- Достоверна ли аналитическая информация в системе?
- Когда можно верить ответам искусственного интеллекта?

Цифровая трансформация

Признаки:

1. Решаем стратегические задачи
2. Ориентируемся на цифровые платформы
3. Используем самые передовые технологии
4. Ожидаем эффективности и реальной отдачи от цифровых продуктов

И каждый раз оказывается так,
что все самое интересное еще впереди...

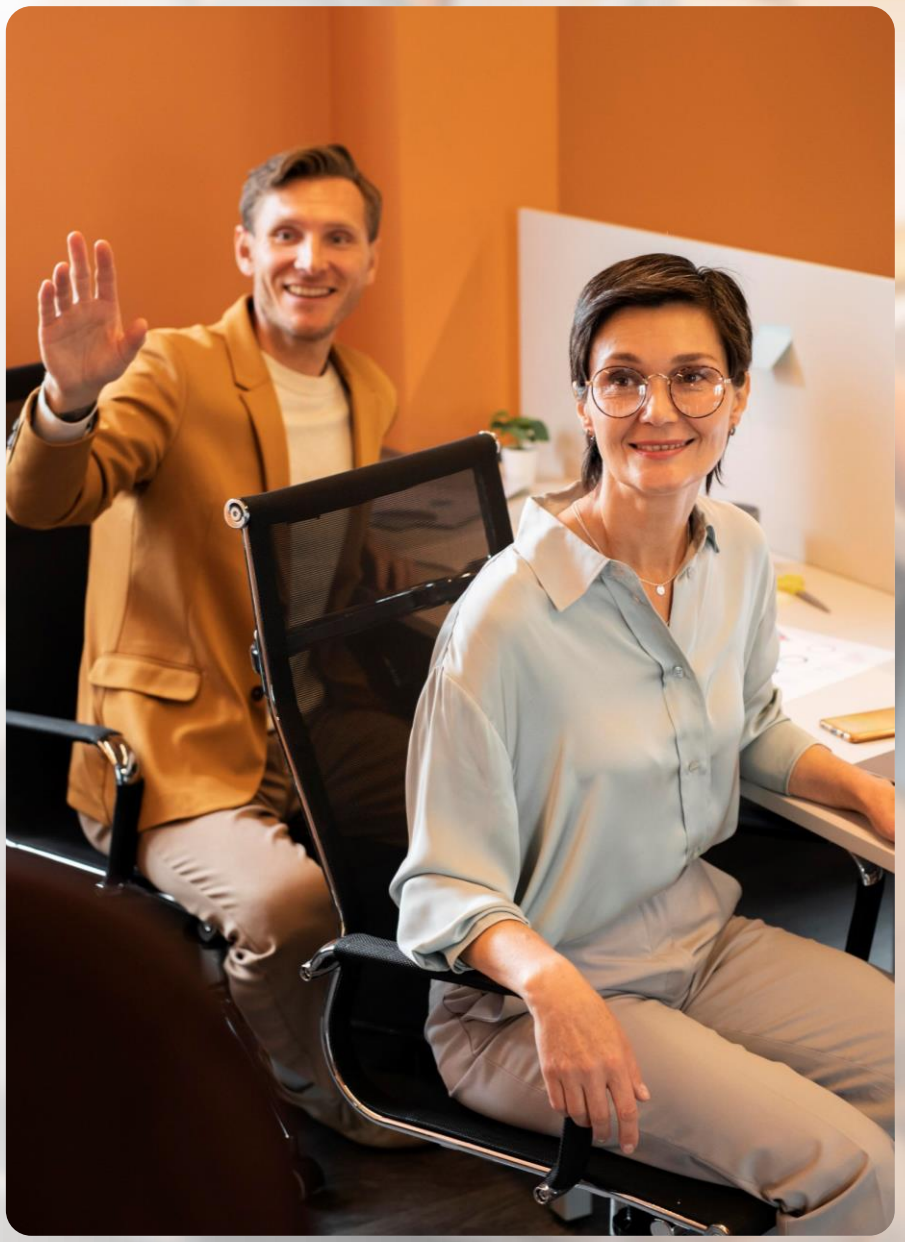


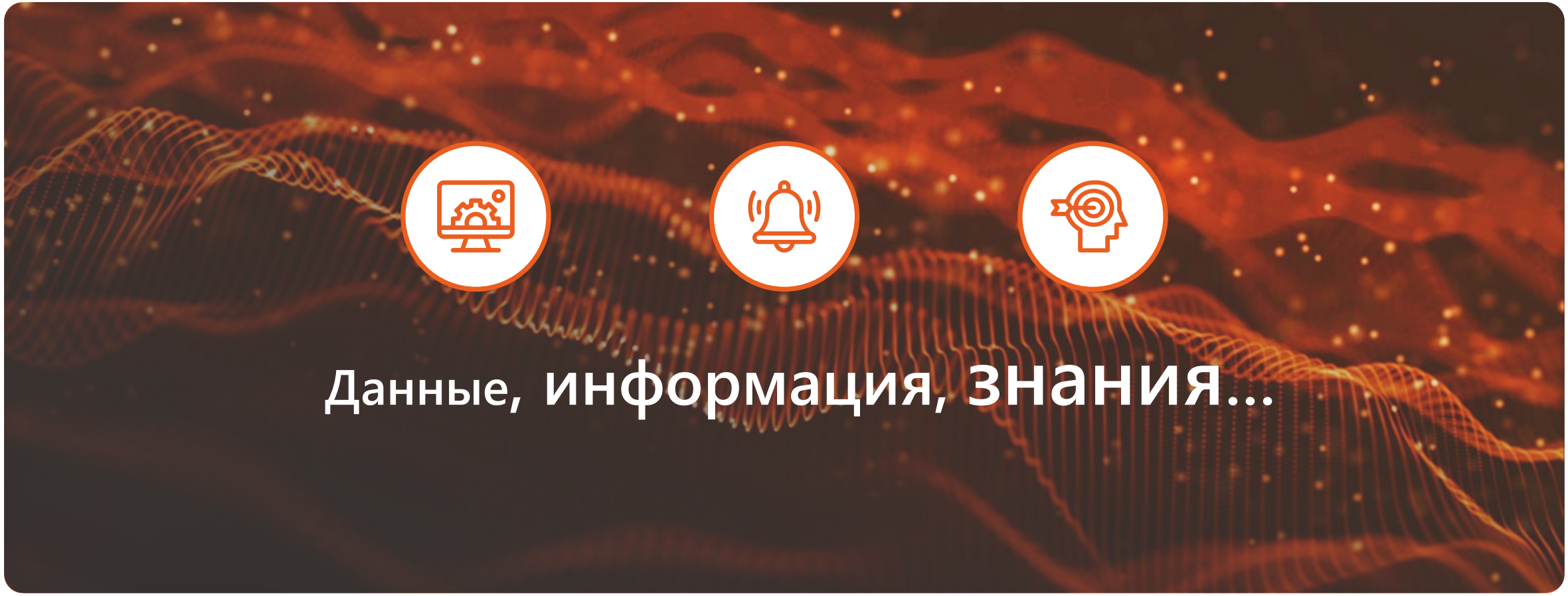
И на первом месте снова...

Люди:

1. Меняем клиентский опыт сотрудников и граждан
2. Управляем изменениями в работе людей
3. Вводим дополнительные новые «цифровые» роли
4. Испытываем жесткий кадровый дефицит

На повестке дня снова человеческий фактор и дефицит живого общения





На пути к мудрости

Аналитическая культура

Тренды:

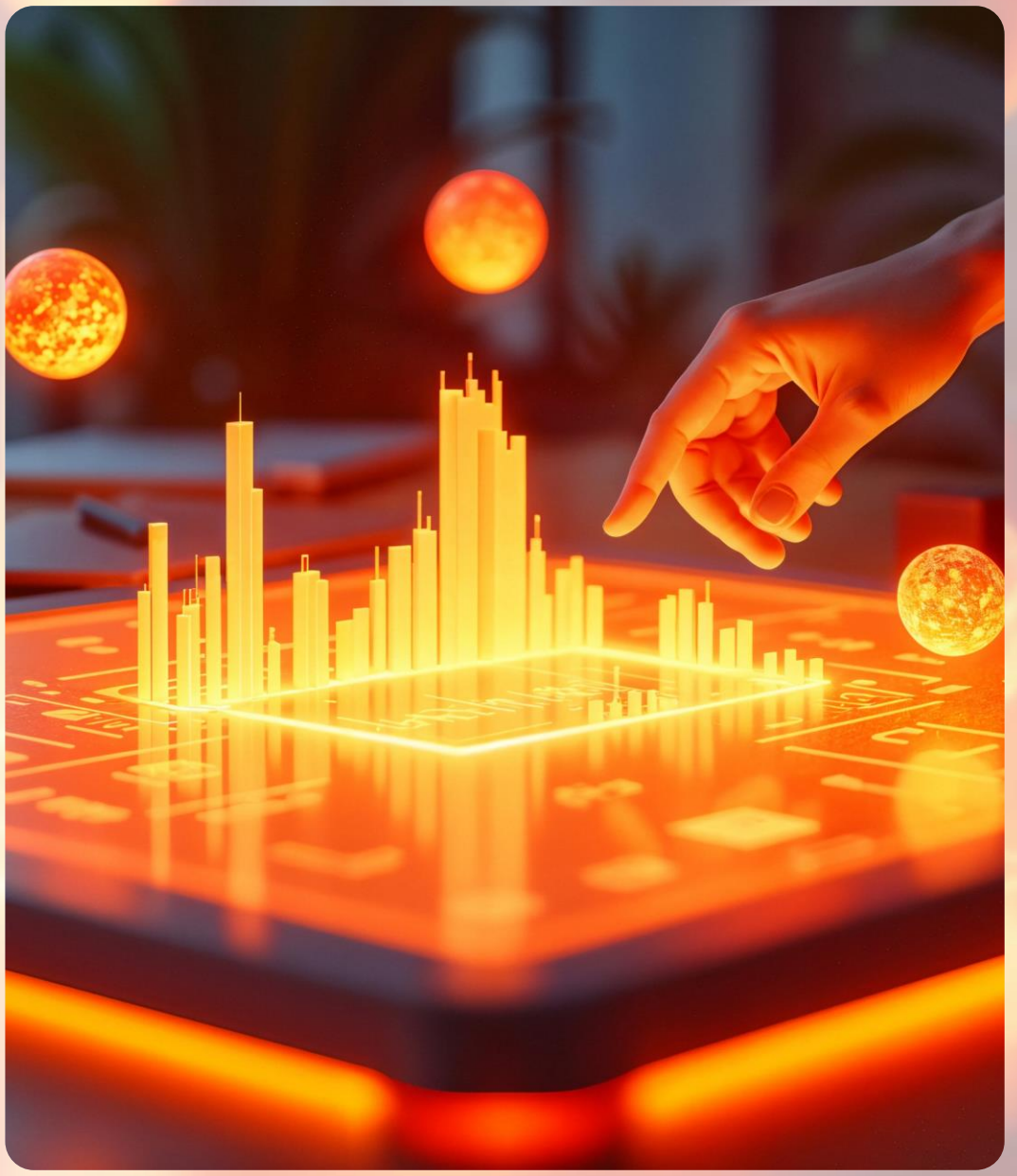
1. Аналитика повсюду:
   в планировании, в учете, в контроле
2. Замена периодической отчетности
   на «ежедневную» аналитику
3. Развитие федеральных
   информационных ресурсов

...и при этом:
Качество данных ГИС остается низким

Аналитика процессов

Тренды:

1. Запрос на повышение эффективности и продуктивности в работе
2. Клиентоцентричность – обязательное требование
3. Реинжиниринг сквозных бизнес-процессов дает наилучший эффект

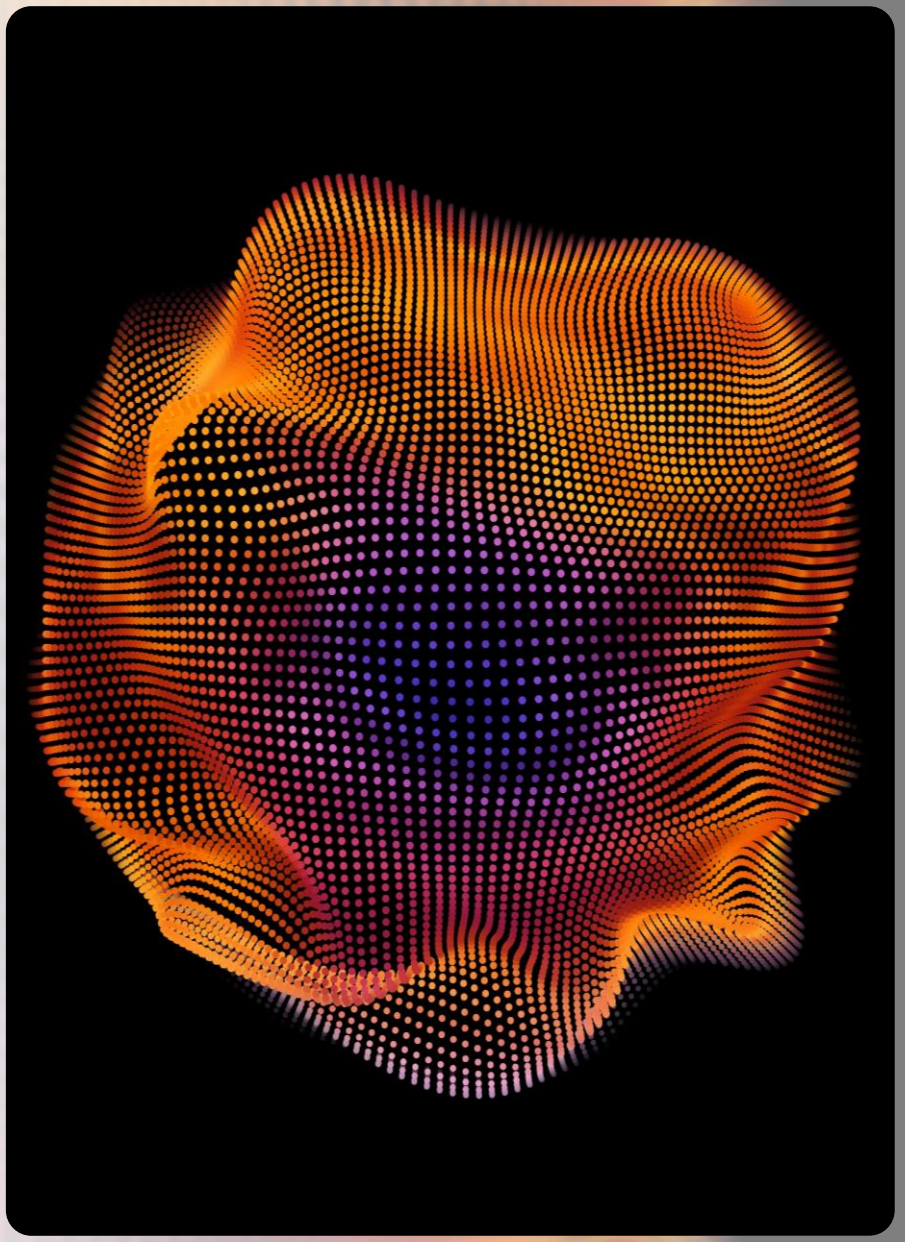


Искусственный интеллект

Тренды:

1. Приоритет – факту применения, результат – менее важен
2. Когнитивные функции: распознавание, исполнение и принятие решений
3. Усиление человека и только в связке с человеком

Залог успеха – культура работы со знаниями



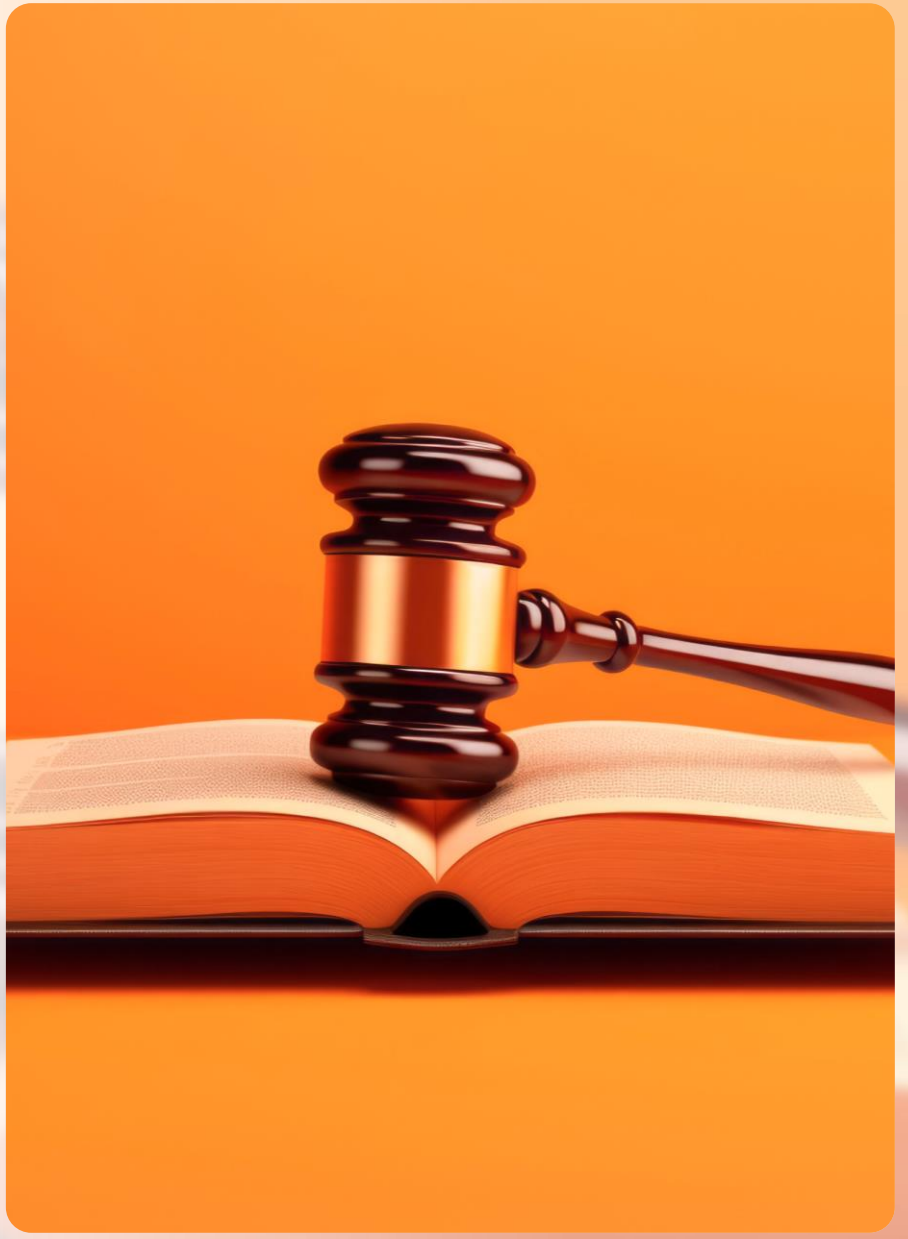
Информационная безопасность

117 приказ ФСТЭК России

Основное:

1. Вступит в силу 1 марта 2026 г.
2. Защите подлежат все ИС,
   даже если они не являются ГИС
3. Ориентирован на реальную
   и непрерывную защищенность
4. Методические рекомендации
   должны появиться до конца года

Пока еще есть время на подготовку

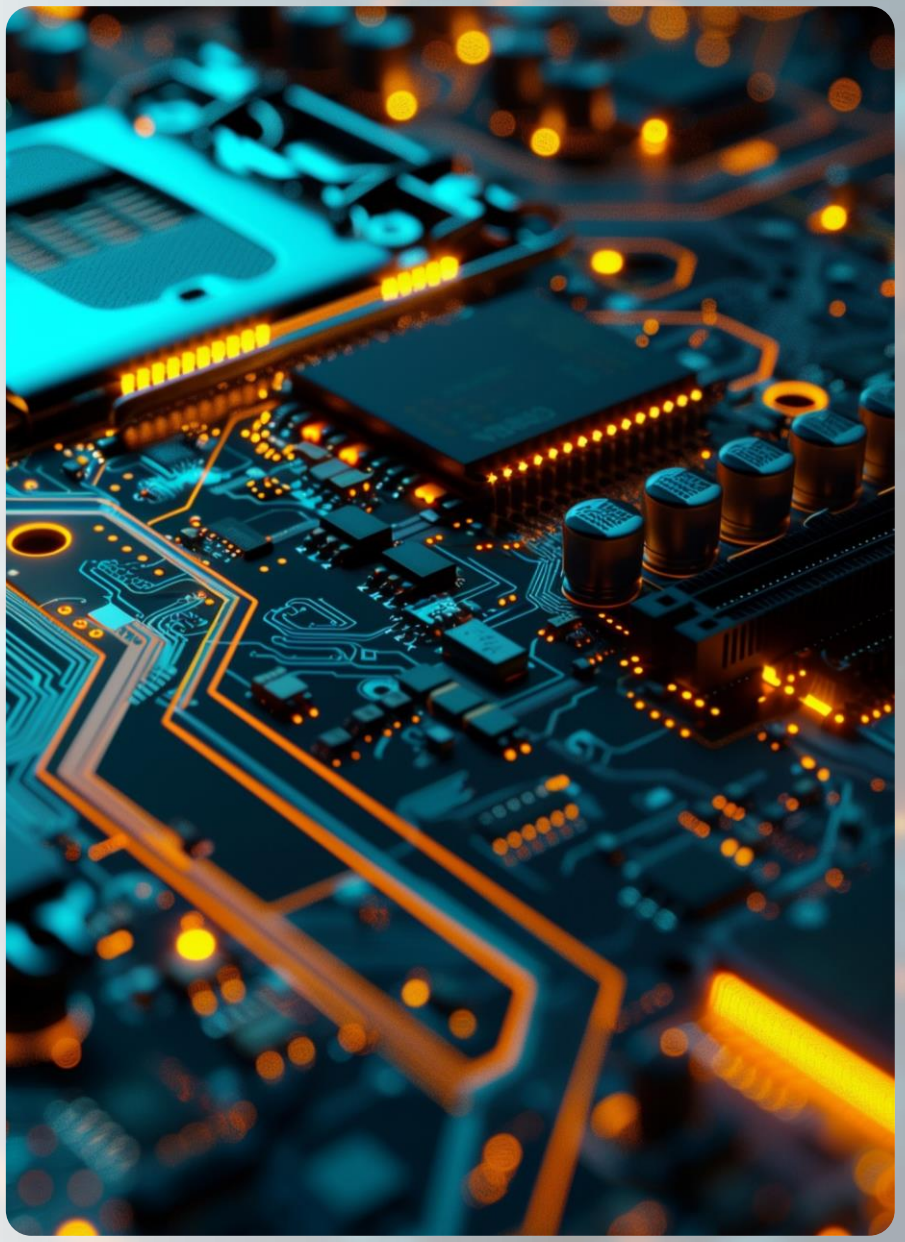


Риски новых технологий

Тренды:

1. Новые технологии несут еще более сложные киберугрозы
2. Архитектура любой современной ИС начинается с безопасности
3. Скоро: требования к доверенному ИИ

Новые технологии всегда требуют дополнительных усилий по обеспечению их ИБ



Непрерывная кибероборона

Тренды:

1. Мониторинг 24/7
2. Оценка показателей защищенности и зрелости (ПЗИ, КЗИ)
3. Приоритет – быстрой отработке инцидентов

ИБ становится управляемой и прозрачной для руководства органов государственной власти

Пространство доверия

Тренды:

1. Четкая связка юридических и технических вопросов
2. Усиление механизмов идентификации для всех пользователей ИС
3. Фиксация всех значимых решений и технических действий

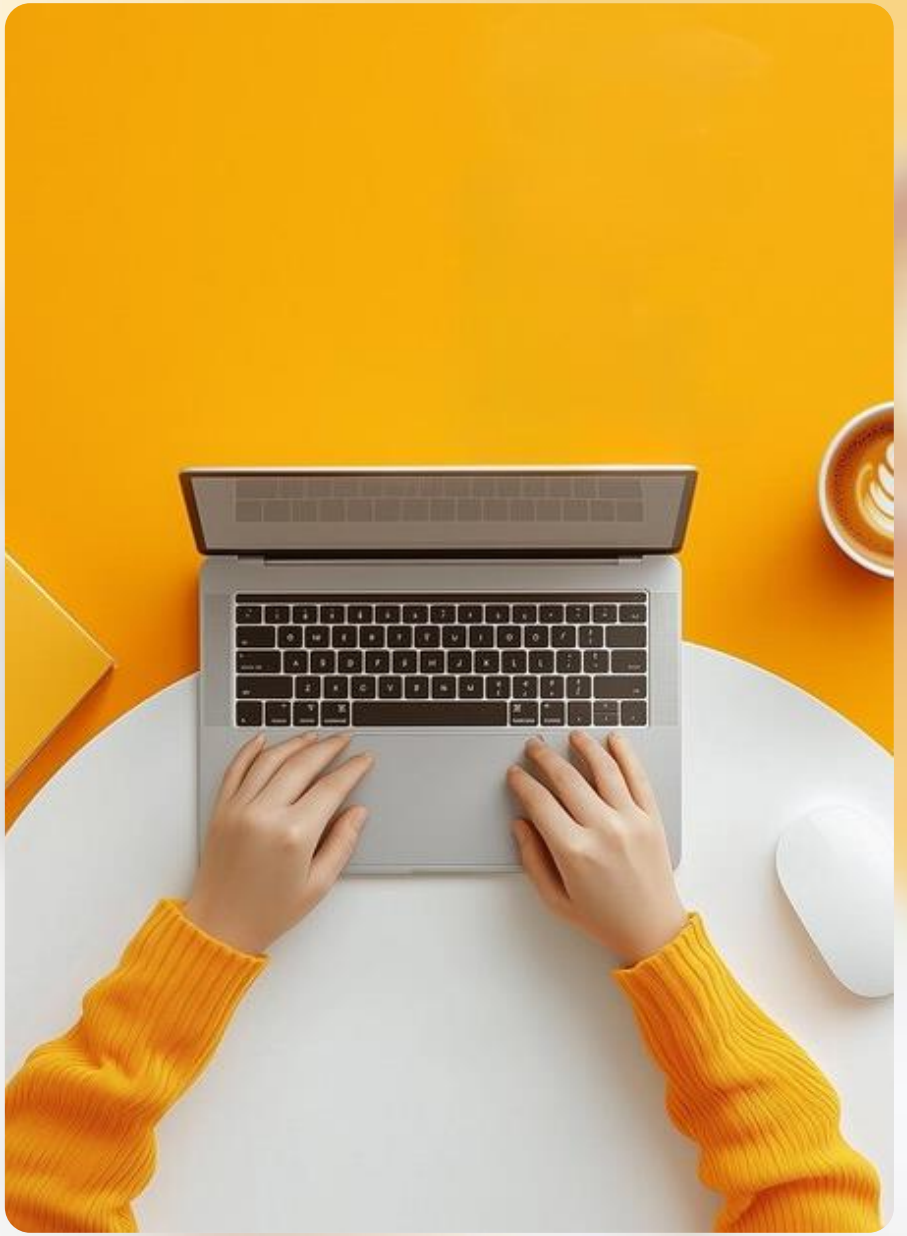
ИБ – больше не отдельная сфера, а основа цифрового доверия

Цифровой документооборот

Тренды:

1. Неснятые вопросы решаются медленно: архивы, метки времени, мобильная ЭП и др.
2. Необходимость подписания данных, а не только документов
3. Усиливающийся запрос на отказ от бумажных документов

Для применения ЭП необходимы доверенная среда и сервисы ИБ



Поставщики и продукты

Тренды:

1. Множество требований к ИБ поставщиков, включая разработку безопасного ПО (РБПО)
2. Обновления ПО должны проходить предварительные испытания
3. Контроль и фиксация всех видов работ с ИС

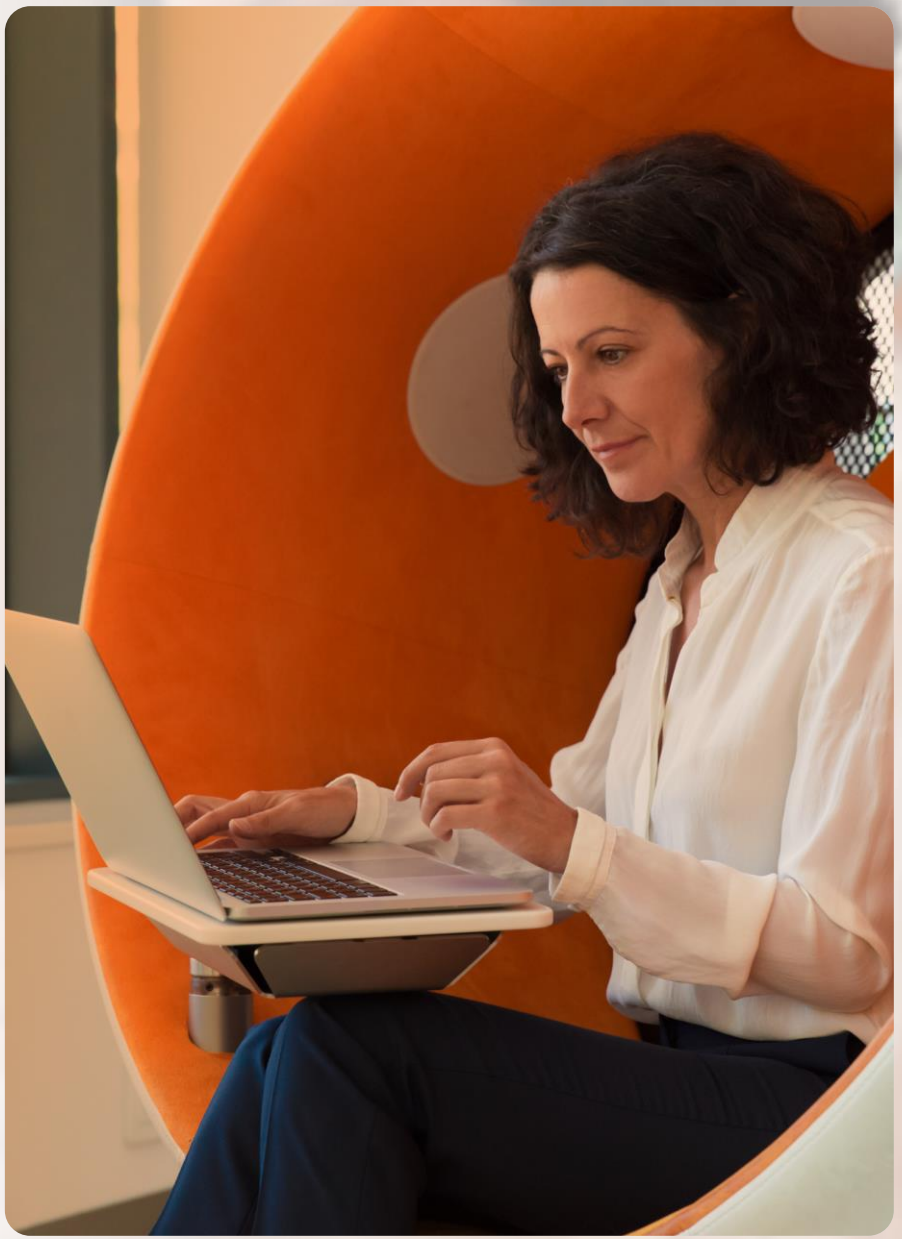
Поставщики подвергаются кибератакам чаще своих клиентов

Человеческий фактор

Тренды:

1. Новые требования к квалификации персонала
2. Практическая подготовка: киберучения и антифишинг
3. При этом существует огромный дефицит профильных специалистов

Наиболее эффективный подход – сервисные контракты по ИБ



ЧТО ДЕЛАТЬ???

Сервисы обеспечения ИБ

Состав:

КСБ-СОФТ

- Мониторинг и реагирование на инциденты
- Поддержка документов в актуальном состоянии
- Управление уязвимостями и тестирование на проникновение (пентест)
- Оценка показателей защищенности и зрелости (ПЗИ, КЗИ)
- Поддержка инфраструктуры в стабильном состоянии
- Внедрение процессов разработки безопасного ПО (РБПО)

Обязательства поставщика

- Повышение требования к защите (процессный подход)
- Больше необходимых средств защиты информации
- ВАЖНО: контроль доступа к инфраструктуре заказчика
- Пристальное внимание регуляторов

Импортозамещение «под-ГИС»

Комплексный подход
к задаче со сроком «вчера»:

Замена

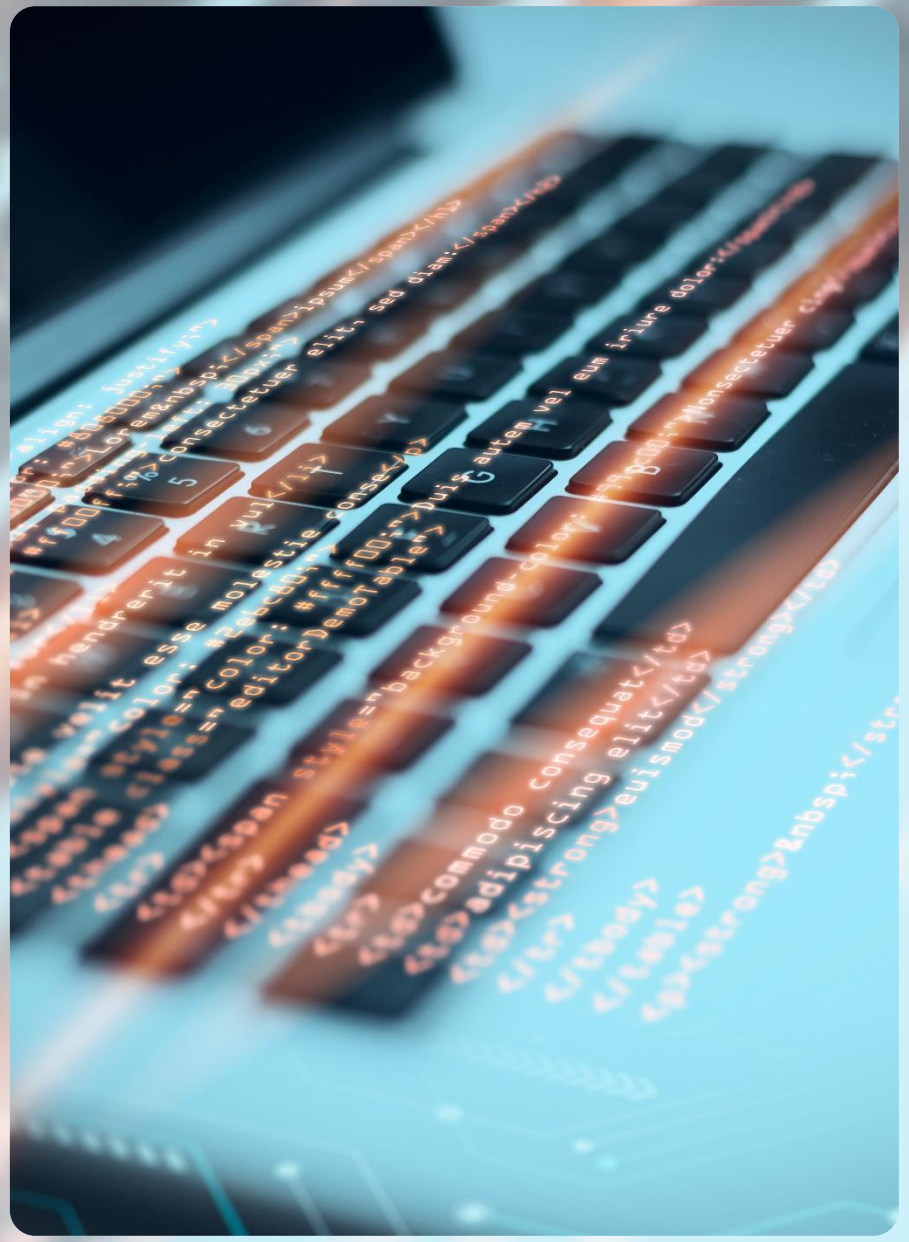
- Серверного оборудования
- Общесистемного ПО
- Систем управления БД
- Прикладного ПО

Актуализация

- Статуса аттестованного объекта

Разработка безопасного программного обеспечения

- Требования по РБПО становятся обязательными
- Активный переход «Кейсистемс» на разработку безопасного ПО, часть разработок прошла сертификацию
- НПЦ «КСБ» оказывает услуги по внедрению процессов РБПО



Центр мониторинга «SOCRAT»

КСБ-СОФТ

Услуга по мониторингу и реагированию:

1. Круглосуточный мониторинг событий информационной безопасности
2. Своевременное обнаружение и реагирование на кибератаки
3. Выявление угроз и уязвимостей
4. Формирование рекомендаций по повышению киберустойчивости

SOCRAT SECURITY OPERATION CENTER RUSSIAN ANALYTICS TEAM

Экосистема «Альфа»

альфа|док

- Управление процессом по защите информации
- Формирование актуальных документов
- Организация оценки состояния защиты информации
- Взаимодействие с регуляторами в одном окне

А еще автоматизация процесса учета и выдачи СКЗИ с альфа|крипто

Экосистема «Альфа»

альфа|интенсив

- Управление осведомленностью сотрудников
- Практическая имитация фишинговых атак
- Непрерывный контроль обучения
- Выполнение требований
  117 приказа ФСТЭК России

Экосистема «Альфа»

альфа|коннект

Единый портал подключения пользователей и подрядных организаций на базе программных комплексов «АльфаКоннект», «Альфа-ID», «КС IDM»

- Электронный портал по работе с пользователями и подрядными организациями
- Цифровые регламенты, конструкторы процессов и гибкие шаблоны документов
- Юридическая обвязка процесса
- Выполнение требований 117 приказа ФСТЭК России

КЕЙСИСТЕМС

@keysystems

@ks_it

8 (8352) 323-323

info@keysystems.ru

keysystems.ru

г. Чебоксары,
ул. К. Иванова, д. 50