Как жить в условиях неопределенности компаниям, использующим иностранные ИБ-решения?

Николай Фокин
директор Центра информационной безопасности компании «ЛАНИТ-Интеграция»

Текущая ситуация

- (При) остановка деятельности основных зарубежных вендоров по ИБ:

- Прекращение поддержки и обновлений, продаж
- Рост цен на импортные решения из-за курса валют, логистики, предоплаты
- Сложная геополитическая обстановка и огромное количество компьютерных атак (в особенности DDOS-атаки, атаки на веб, периметр и удаленный доступ, шифровальщики)
- Проблемы с поставкой оборудования (нарушение цепочек поставок, санкционные ограничения)
- Закладки в свободно распространяемом ПО

Ключевые риски

- Уязвимости в ПО и оборудовании
- Отказ (ошибки) в работе ПО и оборудования
- Вопросы совместимости АСУ ТП с отечественными СЗИ (Honeywell, Rockwell, частично Siemens)
- Риски приостановки международного обмена об актуальных угрозах
- Возможная потеря функциональности (отсутствие аналогов, функциональных возможностей)
- Удаленная блокировка, повреждение ПО и оборудования (подписки, облака, удаленная поддержка)
- Приостановка действия сертификатов на СЗИ со стороны ФСТЭК

Не надо паники

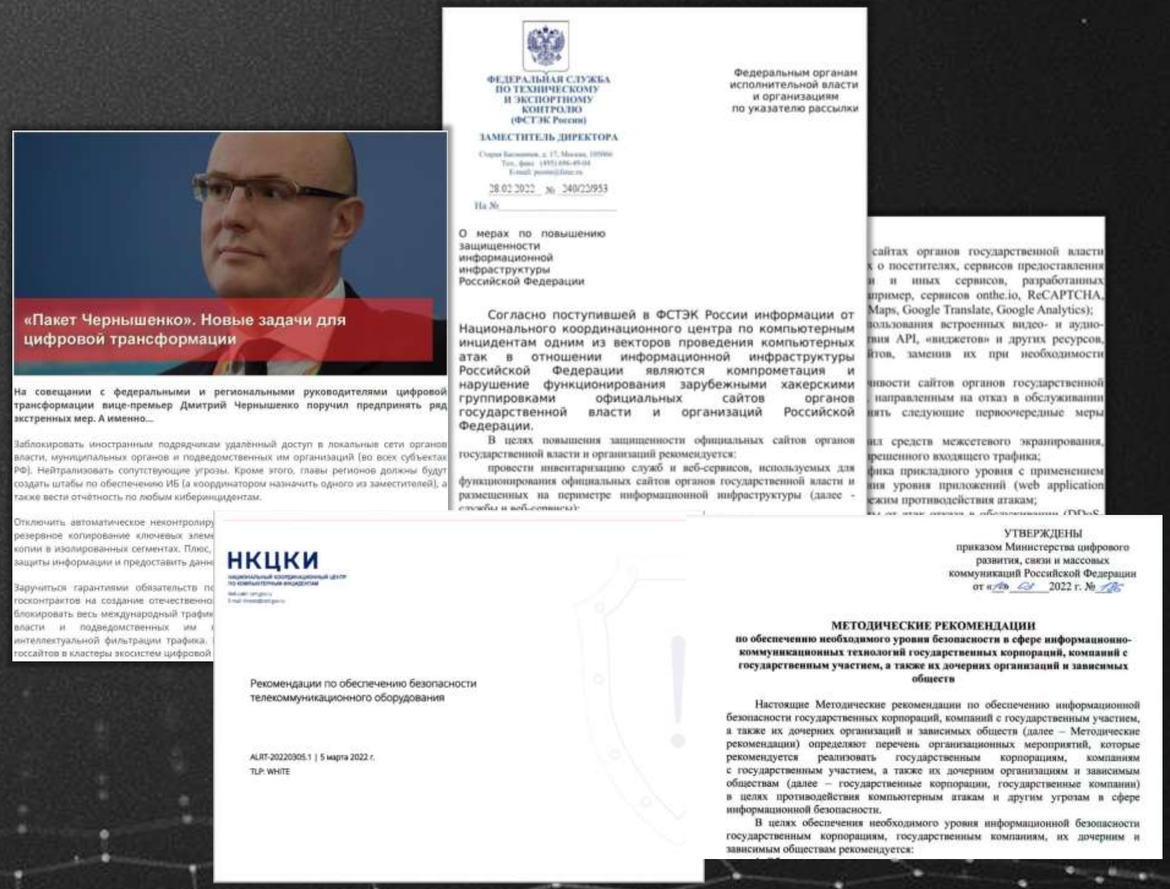
Что важно в первую очередь

- Провести аудит (инвентаризация систем, оценить риски, угрозы, уязвимости)
- Провести аудит цепочек поставок ИТ-, ИБ-решений (оценить приоритет)
- Разработать дорожную карту по замене решений, начиная с наиболее критичных
- Обеспечить безопасность периметра (эшелонированная защита)
- Усилить защиту удаленного доступа, веб-сервисов
- Обеспечить защиту инфраструктуры от DDoS атак
- Внедрить решение по защите от целевых атак, анализу сетевого трафика, сервисы по угрозам (SOC)
- Проверить процедуры реагирования и восстановления от кибератак

Рекомендации регуляторов

По состоянию на 31.03.22 были выпущены рекомендации и составлен ряд поручений:

- Бюллетень НКЦКИ с рекомендациями по обеспечению безопасности телеком. оборудования
- Информационное письмо ФСТЭК с рекомендациями по защите официальных сайтов органов госвласти
- Поручения по экстренным мерам от вице-премьера Дмитрия Чернышенко
- Методические рекомендации Минцифры



Очевидно, что набор рекомендаций и поручений будет дополняться и уточняться

Что важно учесть при переходе

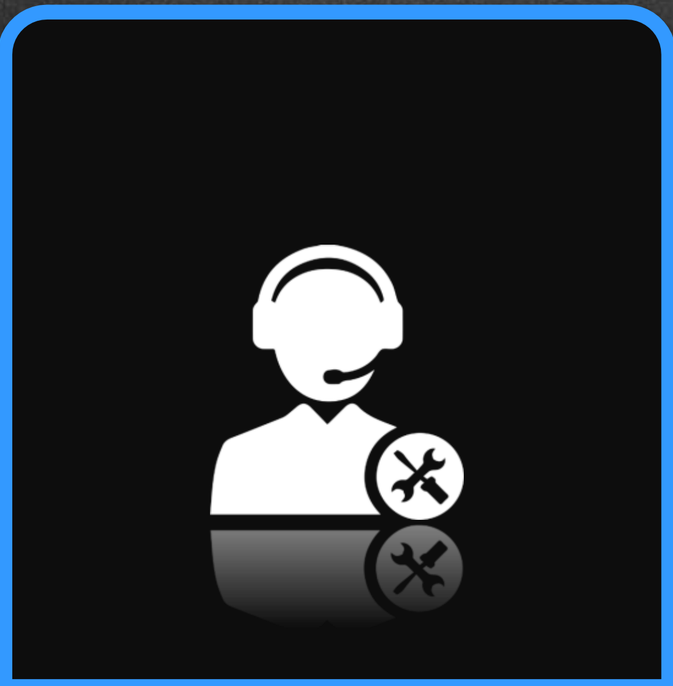
Этапы, дорожная карта перехода

Унификация и стандартизация решений, совместимость

Пилотирование и пробные версии решений

Чем мы можем помочь

Подбор, поставка
и внедрение решений



Техническая
поддержка решений

Обучение сотрудников
по решениям

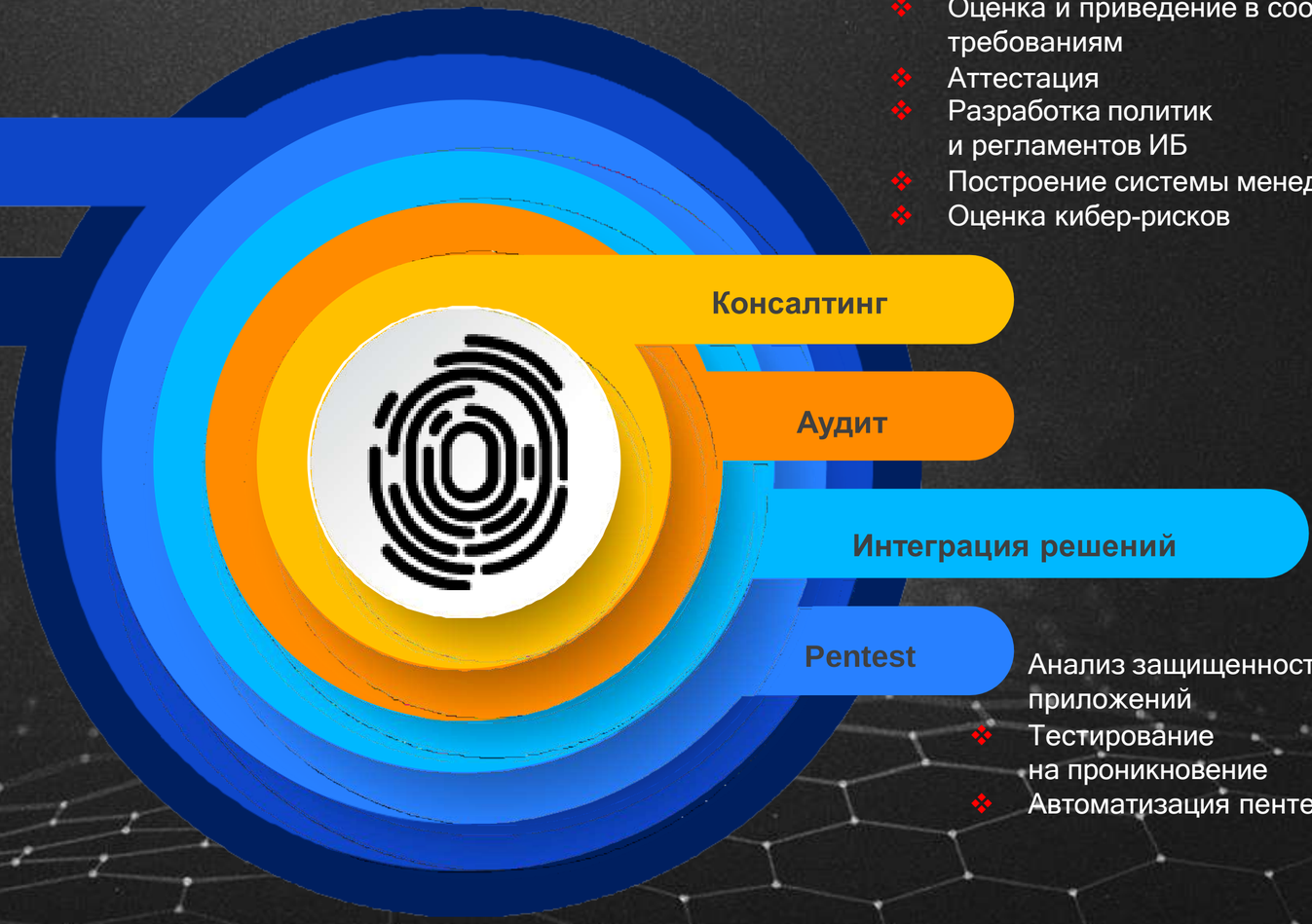
Услуги по информационной безопасности

- Техническое сопровождение и техническая поддержка решений по ИБ
- Аутсорсинг систем ИБ

Услуги и сервисы

Соответствие требованиям Законодательства

- 152-ФЗ «О персональных данных»
- ФЗ-149 «Об информации, информационных технологиях и защите информации»
- ФЗ-98 «О коммерческой тайне»
- ФЗ-187 «О защите КИИ», ФСТЭК 239 Приказ
- Защита ГИС, ФСТЭК 17 Приказ
- 382-П, Гост 57580
- ISO/IEC 2700X



Консалтинг

- Комплексный аудит ИБ
- Разработка стратегии и концепции
- Оценка и приведение в соответствие требованиям
- Аттестация
- Разработка политик и регламентов ИБ
- Построение системы менеджмента ИБ
- Оценка кибер-рисков

Аудит

Интеграция решений

Pentest

- Анализ защищенности приложений
- Тестирование на проникновение
- Автоматизация пентеста

Спасибо за внимание
Вопросы?

Николай Фокин
директор Центра
информационной безопасности
компании «ЛАНИТ-Интеграция»