



КОД БЕЗОПАСНОСТИ



Локализация производства как
средство защиты от НДС



Преимущества проникновения в сеть через взлом межсетевоего экрана

- Не нужно тратить много времени на подготовку атаки
- Можно получить доступ к подсети управления, что облегчит дальнейшее распространение
- Можно долго оставаться незамеченным



- Hacking Team – производитель средств негласной слежки и удаленного управления
- В результате инцидента были опубликованы:
 - Переписка
 - Исходные коды ПО
 - Информация о клиентах



- Из интернет было доступно очень мало сервисов
 - Веб-сайт
 - Почтовый сервер
 - **2 VPN шлюза**
 - **Анти-спам устройство**
- Анализ прошивки одного из устройств выявил 0-day уязвимость
- Эксплуатация уязвимости привела злоумышленника во внутреннюю сеть



Какой код необходимо проверить?

Программная часть

- Прикладное ПО
 - Библиотеки
 - Операционная система
 - UEFI
-
- Out of band управление
 - Сетевые карты
 - FPGA/ASIC чипы

Аппаратная часть





- Анализ чипа Microsemi ProASIC3 FPGA выявил подозрительный код
- Специальный ключ мог деактивировать или перепрограммировать чип, даже если тот был закрыт ключом пользователя
- В последствии разработчик заявил что это был «встроенный интерфейс отладки»



- Сертификация по НДС
- Контроль исполняемого кода в умных чипах
 - Сетевая карта
 - Материнская плата
 - Периферийные компоненты
- Спецпроверки и специсследования
- **Проектирование устройства собственными силами**



Преимущества in-house проектирования и производства



- Ниже риск получить аппаратную закладку
- Intel ME меньше влияет на работу платформы
- Ниже вероятность несанкционированного доступа к FPGA-чипу
- **Государство создает условия для развития таких инициатив**



- Требования производительности со стороны рынка
- Соотношение производительности и стоимости
- Отсутствие «обвязки»
 - Память
 - Чипсет
 - Сетевые платы



КОД БЕЗОПАСНОСТИ

**Но мы внимательно изучаем все
ВОЗМОЖНОСТИ**



Анализ профильного законодательства



КОД БЕЗОПАСНОСТИ

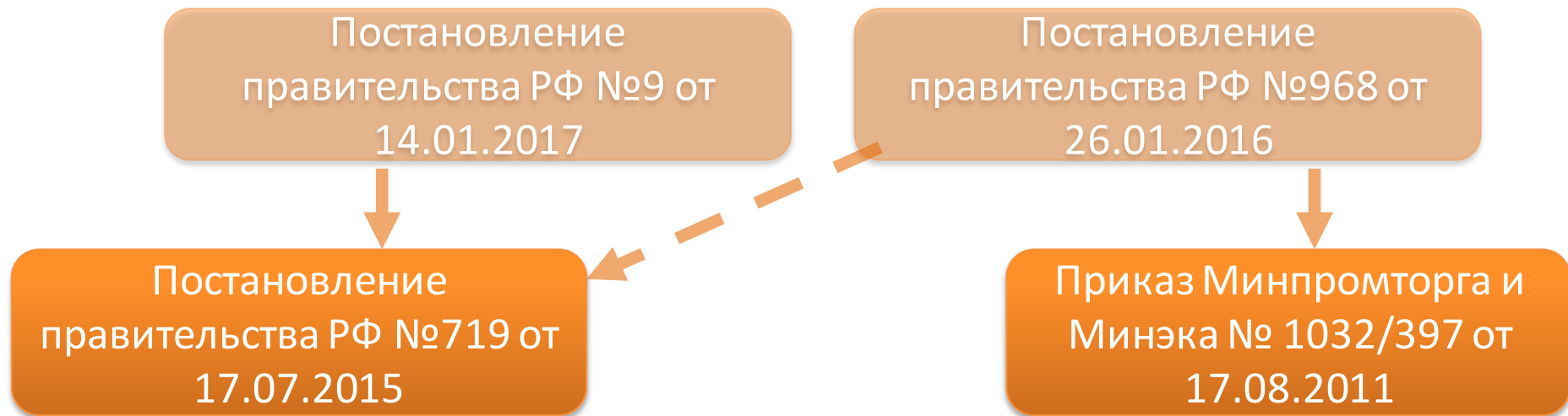




Нормативные акты в области закупок

Постановление
правительства РФ №9 от
14.01.2017

Постановление
правительства РФ №968 от
26.01.2016

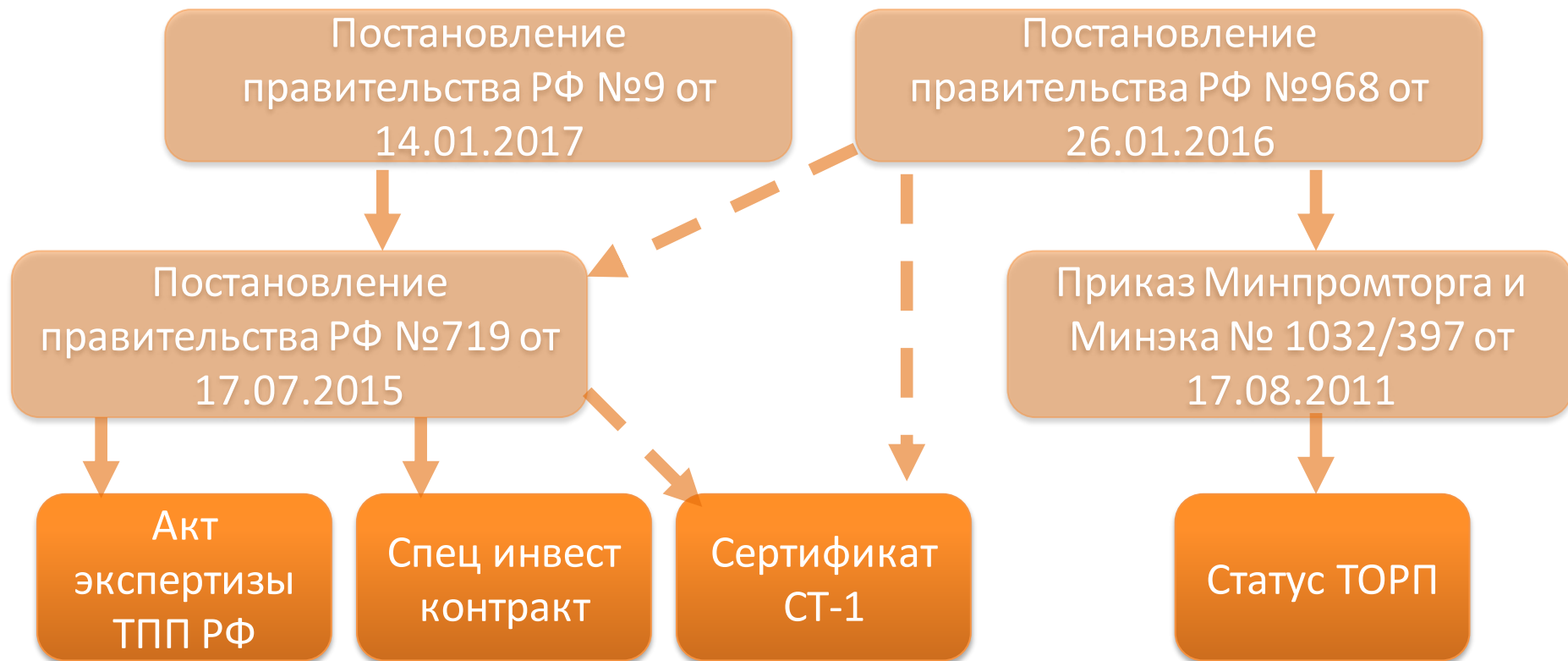


**Нормативные акты в области
определения российского
происхождения изделий**



КОД БЕЗОПАСНОСТИ

Импортозамещение в области «железа»



Свидетельства российского происхождения



КОД БЕЗОПАСНОСТИ

Импортозамещение в области «железа»





Линейка «Континент»

Планируется получение статуса
ТОРП

Линейка «Соболь»

Заканчивается экспертиза ТПП РФ





- **Более 50% акций** предприятия – российские
- Организована **база для производства и обслуживания** оборудования
- **Производство локализовано**
- **Права на документацию и ПО** принадлежат предприятию
- На территории России **осуществляется полный цикл сборки** печатных плат и финишная сборка устройств





- Для защиты от продвинутых угроз необходимо распространять контроль на аппаратную составляющую
- Перенос проектирования платформ в Россию – необходимый шаг на этом пути
- Стать российскими прямо сразу – нельзя
- Не всё, что собрано в России – является российским

**Спасибо за
внимание!**



КОД БЕЗОПАСНОСТИ

Сергей Кормушин
s.kormushin@securitycode.ru

info@securitycode.ru
<http://securitycode.ru>