Код безопасности

Защита порталов государственных услуг в современных реалиях

КОДАНЕВ КИРИЛЛ
Менеджер по продукту

2016

Код Безопасности

ПРОБЛЕМАТИКА НА 2017 ГОД

ТРЕБОВАНИЯ РЕГУЛЯТОРОВ 2016

ГОСТ Р 56938-2016
Защита информации. Защита информации при использовании технологий виртуализации.

№ 374-ФЗ о внесении изменений в закон «О противодействии терроризму»
Пакет Яровой…

Поручение об обеспечении разработки и реализации комплекса мероприятий, необходимых **для перехода органов власти на использование российских криптографических алгоритмов и средств шифрования.**

*Предоставление безвозмездного доступа гражданам Российской Федерации к использованию российских средств шифрования для электронного взаимодействия с органами государственной власти и органами местного самоуправления.

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ К МЕЖСЕТЕВЫМ ЭКРАНАМ
от 28 апреля 2016 г. N 240/24/1986

СМЭВ 3.0
Перезагрузка.
Минкомсвязи отходит в сторону…

Реестр отечественного ПО
Тоже многих взбодрит…

Минкомсвязь России

Код Безопасности

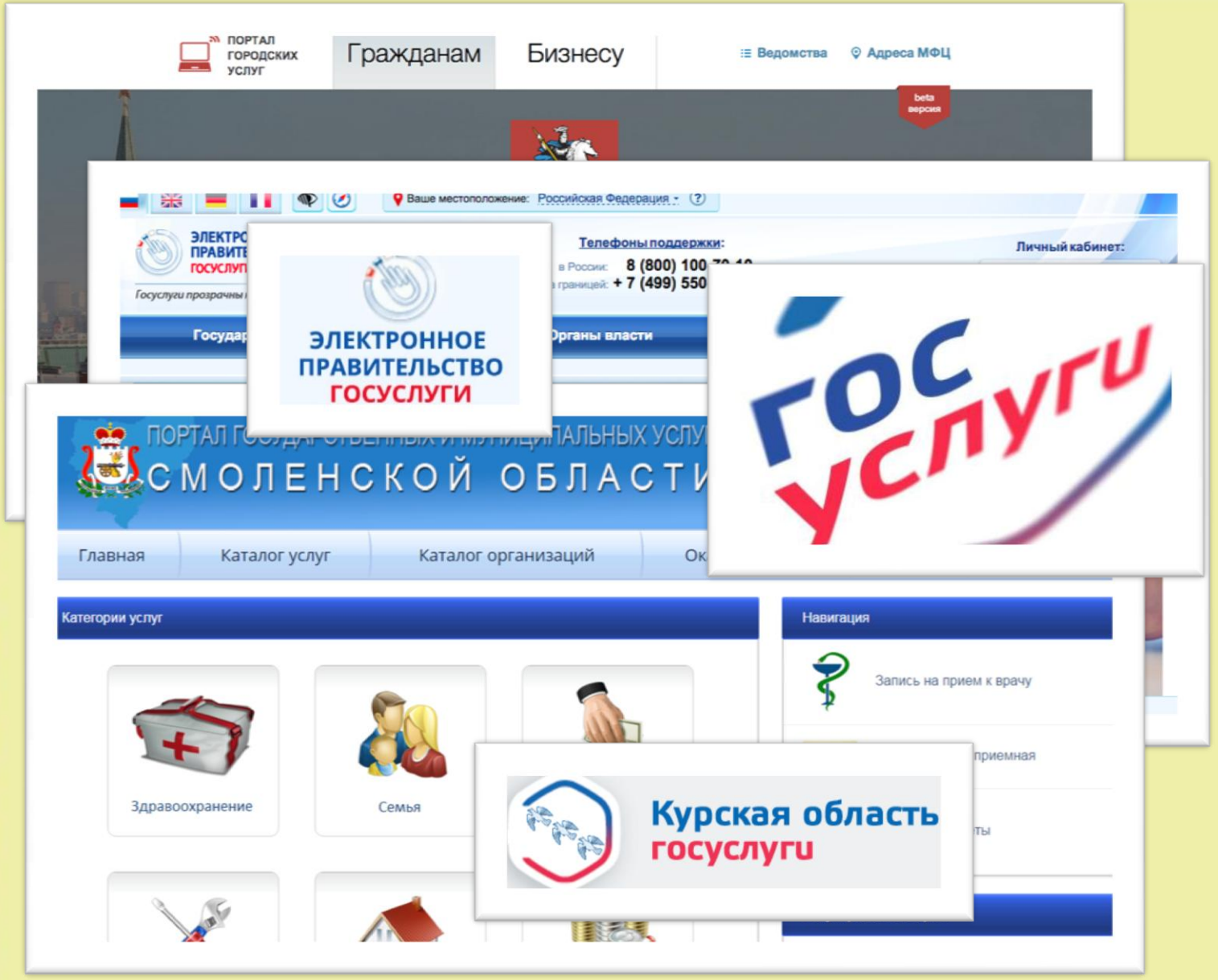
ПРЕДМЕТНО

Обеспечивают доступ физических и юридических лиц к сведениям о государственных и муниципальных услугах в Российской Федерации, государственных функциях по контролю и надзору, об услугах государственных и муниципальных учреждений, об услугах организаций, участвующих в предоставлении государственных и муниципальных услуг, а также предоставление в электронной форме государственных и муниципальных услуг.

Преимущества для граждан:

- централизация.
- удобство.
- оперативность.
- прозрачность операций.

ПОРТАЛЫ ГОСУДАРСТВЕННЫХ УСЛУГ



Код Безопасности

С ДРУГОЙ СТОРОНЫ

Владельцы инфраструктур, обеспечивающих функционирование порталов государственных услуг, также озадачены своими проблемами на эксплуатационном уровне:

- бесперебойность

- отказоустойчивость

- возможность масштабирования

- возможность варьирования функционалом предоставления услуг

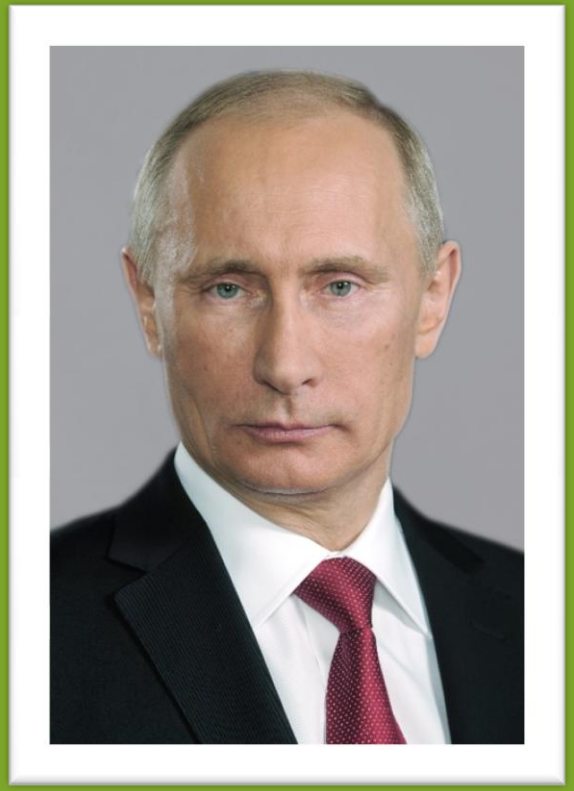
- обеспечение доступности оказания услуг физическим и юридическим лицам

- безопасность как самой инфраструктуры, так и обрабатываемых и передаваемых данных в рамках запросов.

ПОРТАЛЫ ГОСУДАРСТВЕННЫХ УСЛУГ

Код Безопасности

ПРО БЕЗОПАСНОСТЬ



Поручение об обеспечении разработки и реализации комплекса мероприятий, необходимых для перехода органов власти на использование российских криптографических алгоритмов и средств шифрования

ПОРТАЛЫ ГОСУДАРСТВЕННЫХ УСЛУГ

При разработке указанного комплекса мероприятий предусмотрите в числе прочих:

1) предоставление безвозмездного доступа гражданам Российской Федерации к использованию российских средств шифрования для электронного взаимодействия с органами государственной власти и органами местного самоуправления…

Таким образом функциональные владельцы ИТ-инфраструктур, обеспечивающих работу порталов государственных услуг обязаны в срок до 1 декабря 2017 года организовать безвозмездный доступ к порталам при помощи алгоритмов отечественного шифрования.

Помимо прочего требуется реализовать ряд мер по защите ГИС:

- Требования ФСТЭК (17-й приказ)
- Требования ФСБ (378-й приказ)

А также:

- Обеспечить безопасность самой инфраструктуры по части отказоустойчивости.
- Обеспечить отсутствие возможности компрометации прикладного ПО.
- Обеспечить безопасность обработки и передачи ПДн между ведомствами, участвующими в процессе предоставления услуг.

Код Безопасности

КРИПТОГРАФИЯ

Как решается задача сейчас?

ГОСТовая криптография встраивается в каждый веб-сервер с помощью криптобиблиотеки.

Основные риски встраивания криптобиблиотеки:

- Затягивание сроков ввода в строй или модернизации портала
- Выход за рамки бюджета из-за закупок дополнительных лицензий и дополнительных работ по контролю встраивания СКЗИ.

Особенности контроля встраивания СКЗИ

Контроль встраивания СКЗИ для госорганов обязателен.

Требование содержится в следующих документах:

- Методические рекомендации ФСБ,
- Формуляры КриптоПРО CSP, СигналКОМ CSP, КриптоКОМ МагПро CSP и т.д.

ЭТО ДОЛГО и ЭТО ДОРОГО.

Примеры рисков:

- http://www.cnews.ru/news/top/2016-07-11_itogi_proverki_minkomsvyazi_zavyshaet_tseny_na
- http://www.cnews.ru/news/top/2016-07-11_schetnaya_palata_dengi_na_elektronnoe_pravitelstvo

Код Безопасности

В КАЧЕСТВЕ АЛЬТЕРНАТИВЫ

Континент TLS-VPN
Сертифицированное решение для обеспечения защищенного доступа удаленных пользователей к защищаемым ресурсам. Предназначен для Безопасного подключения пользователей к порталам государственных услуг, электронным торговым площадкам, системам интернет-банкинга или корпоративным приложениям через веб-браузер.

Функционал шифрования по ГОСТ выделяется на отдельное устройство:

АПКШ «Континент TLS VPN»:

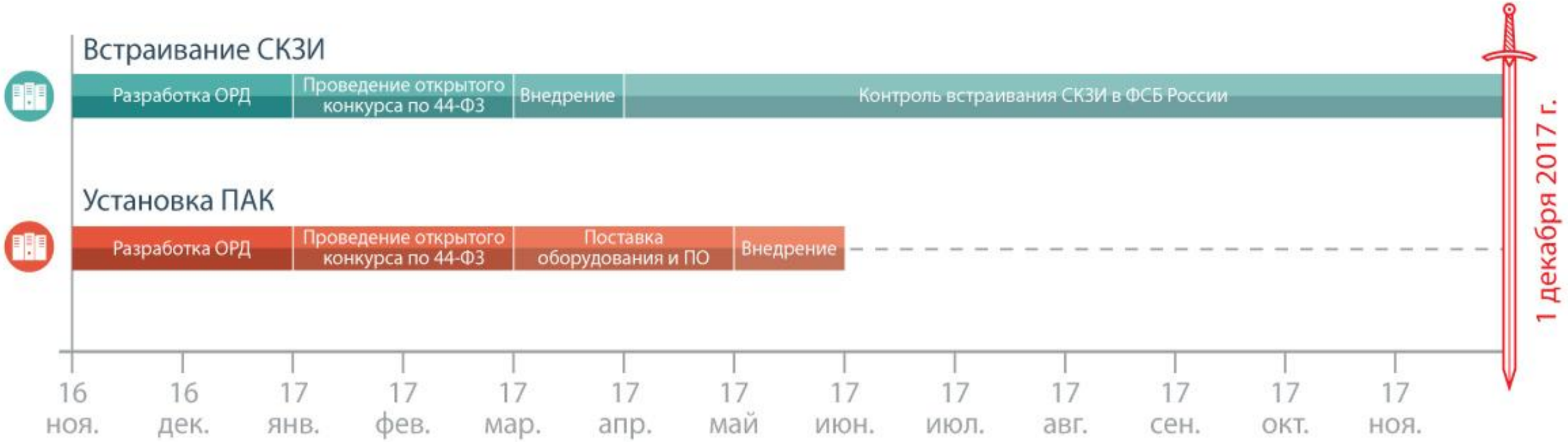
- Удаленные пользователи подключаются к «Континент TLS VPN Сервер»
- Расшифрованный трафик передается на сервер приложений

Контроль встраивания СКЗИ не нужен!

ДЛЯ СРАВНЕНИЯ

Код Безопасности

Сроки перехода госорганов на российские средства шифрования: Как успеть к 1 декабря 2017 г.?



Код Безопасности

«КОНТИНЕНТ TLS Сервер»

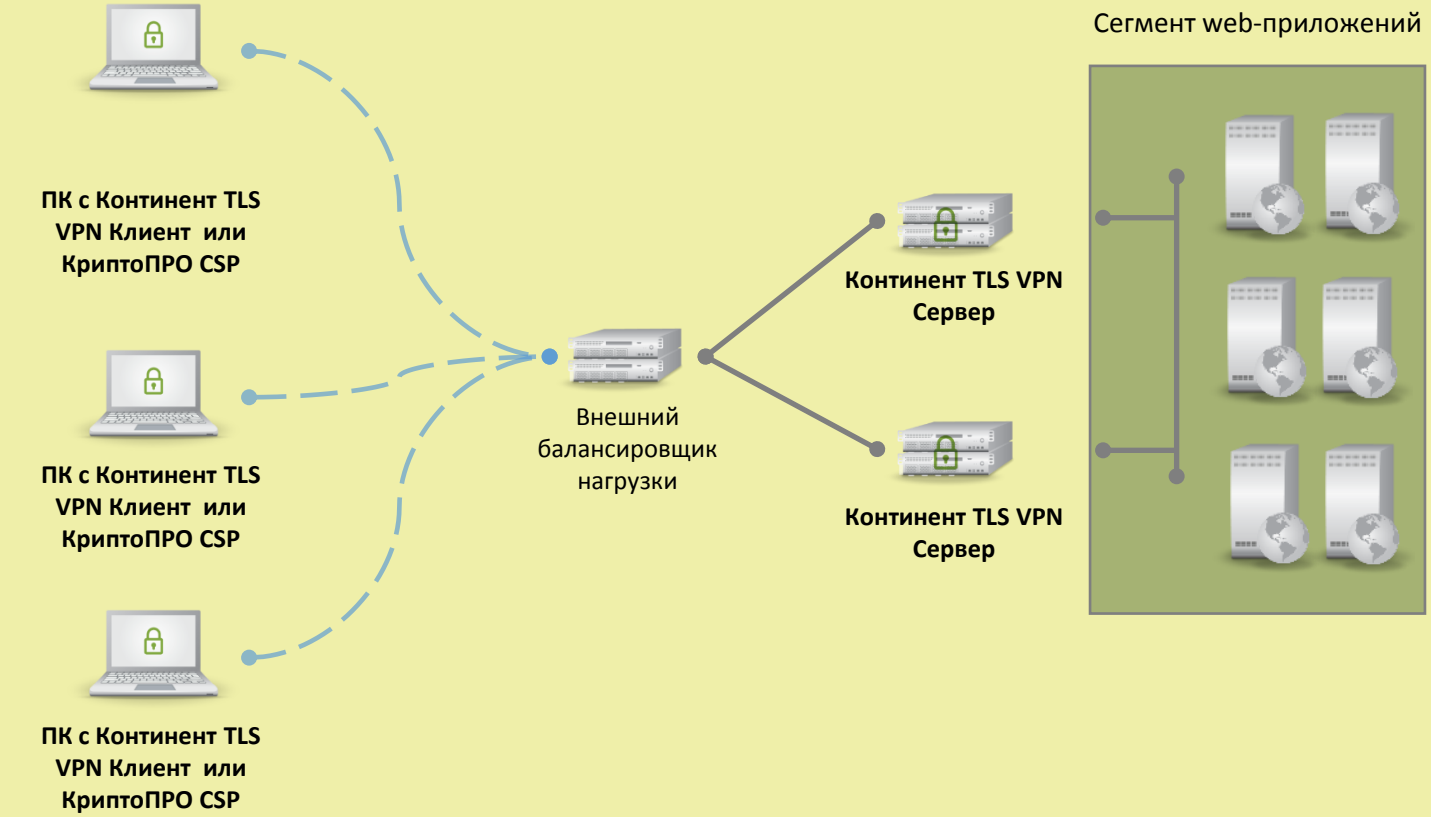
Задачи:

- Доступ удаленных сотрудников к внутренним web-ресурсам
- Разграничение доступа к web-приложениям
- Удаленный доступ с помощью «толстых» клиентов
  - Клиенты ERP-приложений
  - Доступ к терминальному серверу/VDI
- Создание портала госуслуг
- Создание системы дистанционного банковского обслуживания
- Создание электронной торговой площадки

АПКШ «КОНТИНЕНТ»

Континент TLS-VPN

Сертифицированное решение для обеспечения защищенного доступа удаленных пользователей к защищаемым ресурсам. Предназначен для Безопасного подключения пользователей к порталам государственных услуг, электронным торговым площадкам, системам интернет-банкинга или корпоративным приложениям через веб-браузер.



Код Безопасности

ОСТАЛЬНЫЕ ТРЕБОВАНИЯ

- Доверенная загрузка
- Защита виртуальной среды
- Несанкционированный доступ
- Межсетевое экранирование
- Аутентификация
- Системы обнаружения или предотвращения вторжений

Задачи	Решения
Защита от несанкционированного доступа	Secret Net / Secret Net Studio Secret Net Card ПАК «Соболь»
Межсетевое экранирование	Security Studio Endpoint Protection Trust Access АПКШ «Континент» АПКШ «Континент-АП»
Аутентификация	Secret Net ПАК «Соболь» Rutoken, eToken PRO, iButton
Защита виртуальной инфраструктуры	vGate Secret Net Trust Access
Защита каналов связи	АПКШ «Континент» АПКШ «Континент-АП»
Системы обнаружения вторжений / атак.	Security Studio Endpoint Protection АПКШ «Континент-ДА»
Антивирусная защита	Security Studio Endpoint Protection Secret Net Studio

Код безопасности

СПАСИБО!

КОДАНЕВ КИРИЛЛ
Менеджер по продукту

k.kodanev@securitycode.ru
+7 (916) 330-24-83
+7 495 982 30 20 (*182)