Централизованное управление защитными механизмами в гетерогенных средах

Лопатин Роман
Заместитель руководителя отдела продаж

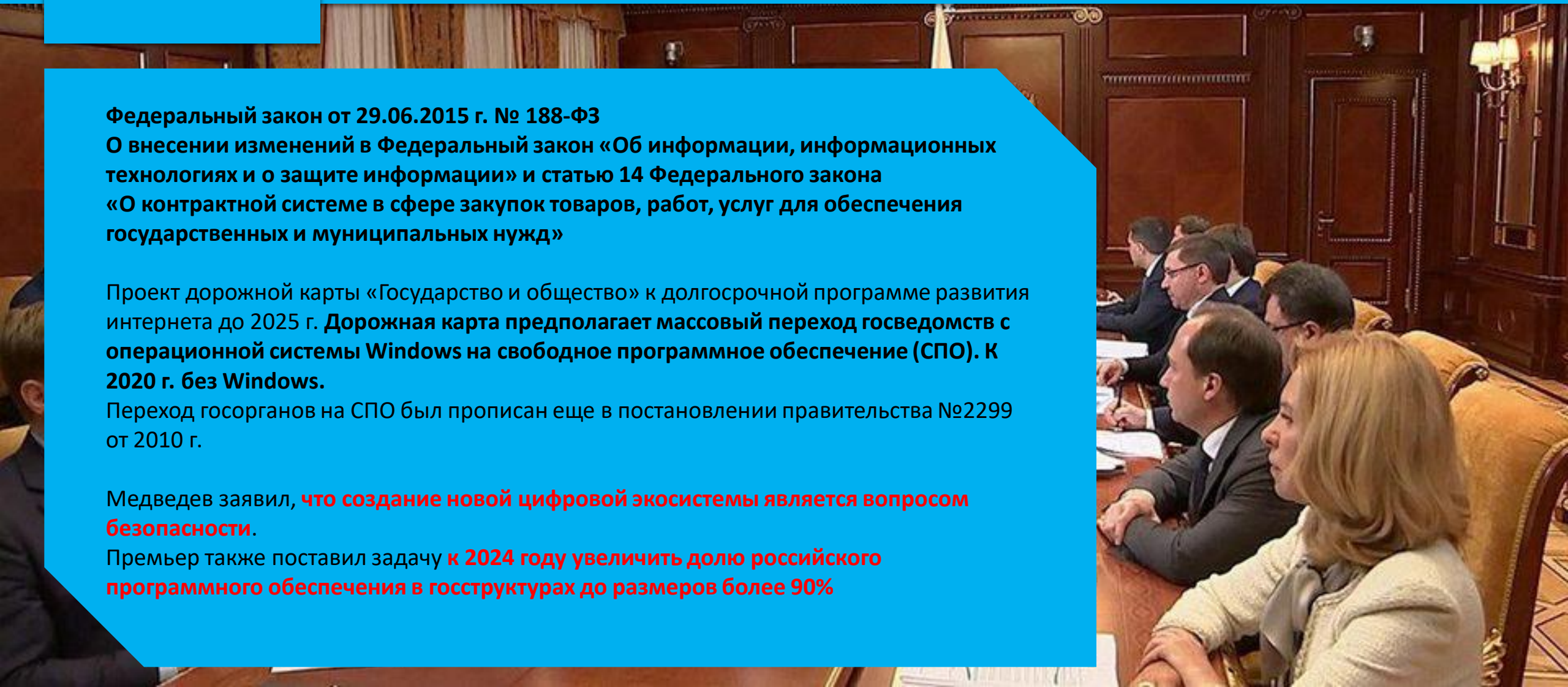
КОД БЕЗОПАСНОСТИ

СТАРТ ЦИФРОВОЙ ЭПОХИ В РОССИЙСКОЙ ФЕДЕРАЦИИ…

- ОБЕСПЕЧЕНИЕ ЦИФРОВОГО СУВЕРЕНИТЕРА РФ
- ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
- ПРОГРАММА ИМПОРТОЗАМЕЩЕНИЯ
- РЕЕСТРО ОТЕЧЕСТВЕННОГО ПО
- НАЦИОНАЛЬНАЯ ПРОГРАММА «ЦИФРОВАЯ ЭКОНОМИКА»

КОД БЕЗОПАСНОСТИ

ПЛАНЫ ПРАВИТЕЛЬСТВА СМЕСТИЛИСЬ…



Федеральный закон от 29.06.2015 г. № 188-ФЗ
О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статью 14 Федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»

Проект дорожной карты «Государство и общество» к долгосрочной программе развития интернета до 2025 г. **Дорожная карта предполагает массовый переход госведомств с операционной системы Windows на свободное программное обеспечение (СПО). К 2020 г. без Windows.**
Переход госорганов на СПО был прописан еще в постановлении правительства №2299 от 2010 г.

Медведев заявил, **что создание новой цифровой экосистемы является вопросом безопасности**.
Премьер также поставил задачу **к 2024 году увеличить долю российского программного обеспечения в госструктурах до размеров более 90%**

КОД БЕЗОПАСНОСТИ

СОВРЕМЕННЫЕ РЕАЛИИ – РОССИЯ И МИР…

ОТСУТСТВИЕ МИКРОЭЛЕМЕНТНОЙ БАЗЫ

ПРИКЛАДНОЕ ПО ЗАТОЧЕНО ПОД «WINDOWS»

УРОВЕНЬ ОТЕЧЕСТВЕННОЙ РАЗРАБОТКИ
В РАМКАХ OPEN SOURSE
ОСТАВЛЯЕТ ЖЕЛАТЬ ЛУЧШЕГО

ПОДДЕРЖКА НА УРОВНЕ ГОСУДАРСТВА НЕ НА
ДОЛЖНОМ УРОВНЕ

МОБИЛЬНОСТЬ И КРОССПЛАТФОРМЕННОСТЬ

СКОРОСТЬ И USABILITY

BLOCHAIN, CLOUD, BIG DATA

АВТОМАТИЗАЦИЯ ПРОЦЕССОВ
И ИСКУСТВЕННЫЙ ИНТЕЛЛЕКТ

КОД БЕЗОПАСНОСТИ

РЕГУЛЯТОРЫ. МИНКОМСВЯЗИ. РЕЕСТР ОТЕЧЕСТВЕННОГО ПО…

100%
обеспе

СРЕДИ ПРОЧЕГО В РАМКАХ КЛАССА ПО:

ОПЕРАЦИОННЫЕ СИСТЕМЫ – 51 продукт…
ОФИСНЫЕ ПРИЛОЖЕНИЯ – 198 продуктов…
СИСТЕМЫ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ – 54 продукта…
ПРИКЛАДНОЕ ПО ОБЩЕГО НАЗНАЧЕНИЯ – 923 продукта…
СРЕДСТВА ВИРТУАЛИЗАЦИИ И ОБЛАЧНЫХ ТЕХНОЛОГИЙ – 92 продукта
СЕРВЕРНОЕ И СВЯЗУЮЩЕЕ ПО – 360 продуктов
СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – 422 продукта…

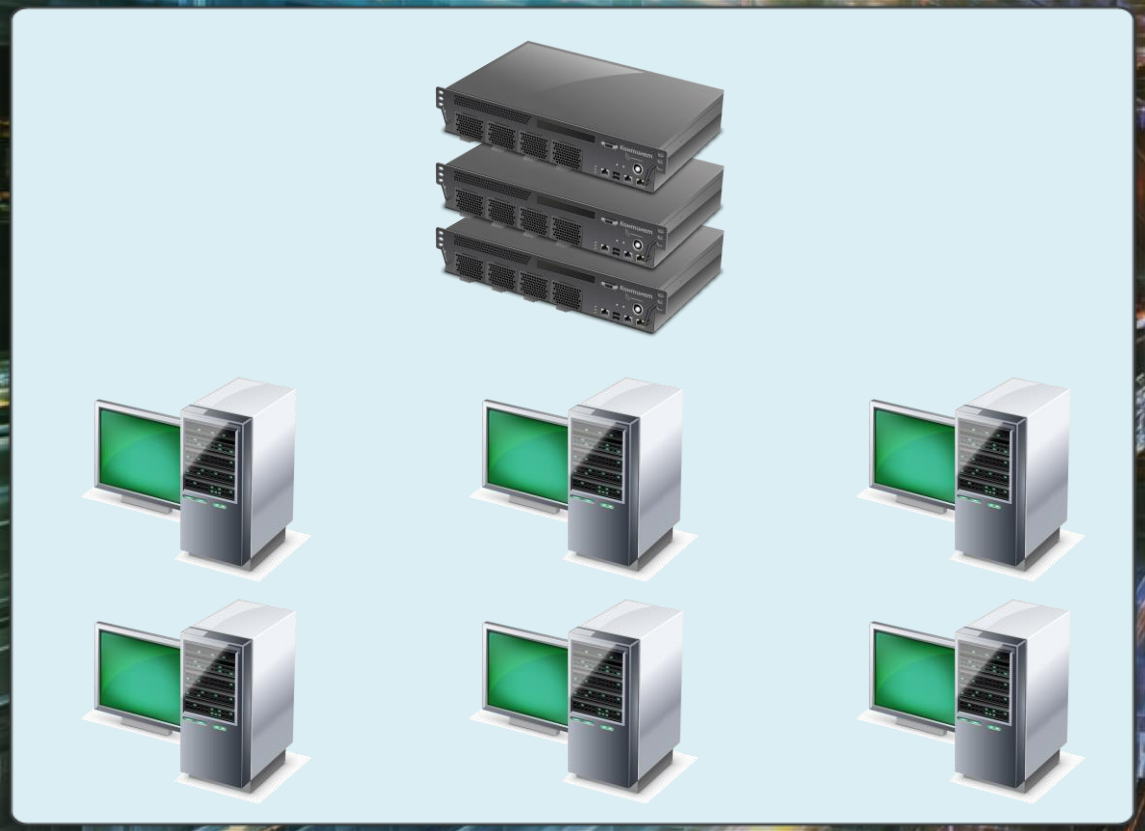
КОД БЕЗОПАСНОСТИ

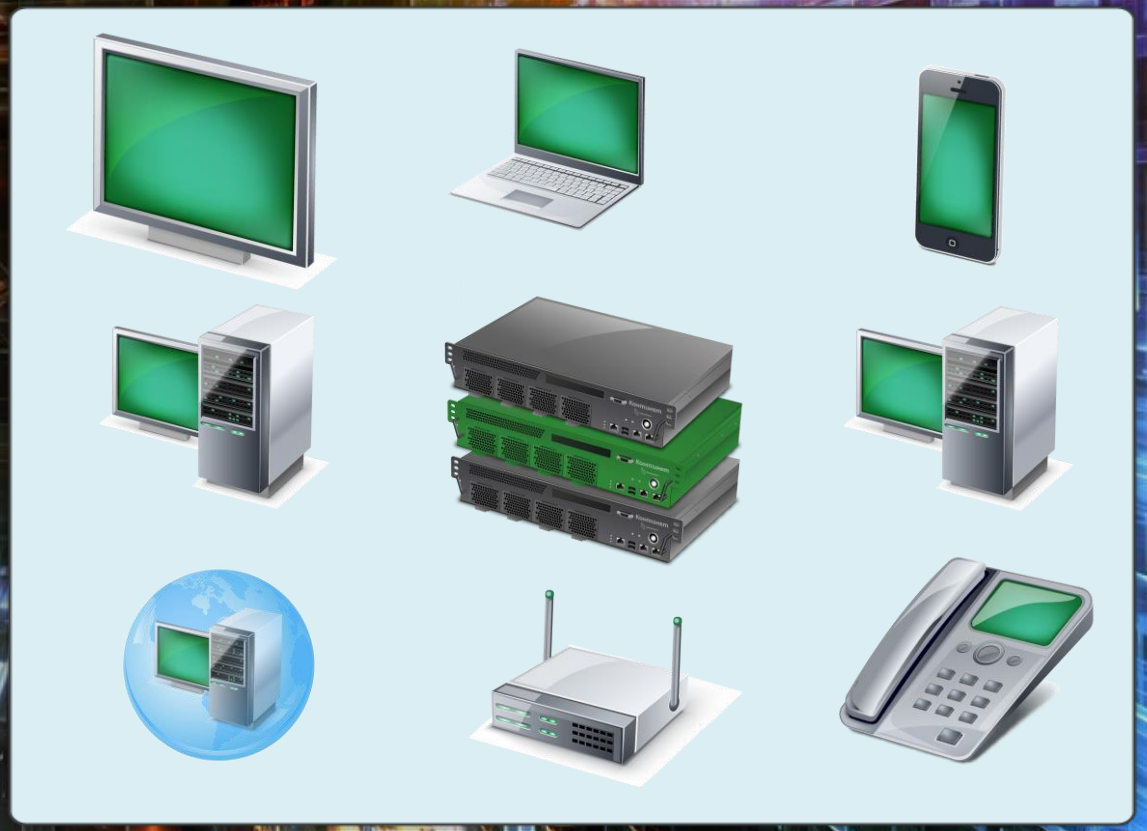
ОРИЕНТИРЫ…

МАКСИМАЛЬНО БЫСТРО СОКРАТИТЬ ОТСТАВАНИЕ В ТЕХНОЛОГИЯХ
ОБЕСПЕЧИТЬ ПОЛНУЮ НЕЗАВИСИМОСТЬ РАБОТЫ ОТЕЧЕСТВЕННЫХ ТЕХНОЛОГИЙ В СЕГМЕНТЕ ИТ
СДЕЛАТЬ НОВЫЕ БАЗИСНЫЕ ТЕХНОЛОГИИ УСТОЙЧИВЫМИ К КОМПРОМЕТАЦИИ И АТАКАМ

КОД БЕЗОПАСНОСТИ

ИНФРАСТРУКТУРА. РАЗМЫТИЕ ПЕРИМЕТРА…





КОД БЕЗОПАСНОСТИ

СЕРВИСЫ. СЛОЖНОСТЬ МИГРАЦИИ…

- ДОЛГИЕ СРОКИ
- ОТСУТСТВИЕ ГАРАНТИИ УСПЕХА МИГРАЦИИ
- НЕТ МАСШТАБНЫХ USE-CASE В ЭТОМ НАПРАВЛЕНИИ
- НЕТ КОМПЕТЕНЦИЙ В OPENSOURCE

КОД БЕЗОПАСНОСТИ

КСТАТИ! ВОПРОС В ЗАЛ!...

МОЖЕТ ЭКСПЛУАТИРОВАТЬ И НАСТРАИВАТЬ:

MS WINDOWS / AD / SERVER
SQL / ORACLE
VMWARE / HYPER-V
IBM, HP, DELL, LENOVO
SAP
CISCO, JUNIPER, MICROTIC, CHECK POINT

МОЖЕТ ЭКСПЛУАТИРОВАТЬ И НАСТРАИВАТЬ:

ОТЕЧЕСТВЕННЫЕ ОС (Серверные ОС и Десктопные)
Отечественные базы данных
Отечественные гипервизоры
Российские АРМ на аппаратном уровне
ERP-системы / 1С
Российское сетевое и коммутационное оборудование

Microsoft выпустила обновление W… …мпьютеры

В Microsoft объяснили, как защититься от новых уязвимосте

КОД БЕЗОПАСНОСТИ

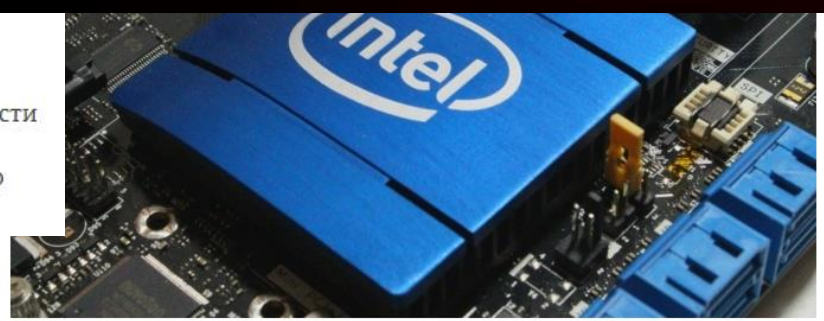
КОМПРОМЕТАЦИЯ ЗАПАДНЫХ РЕШЕНИЙ…

Майерсон, риску подвержены пользователи смартфонов и ПК, а также серверы. В

Microsoft выпустила экстренный патч для критической RCE-уязвимости в Windows

Мария Нефёдова , 10.05.2017 3 мин на чтение 0 2 30711

Корпорация Microsoft приостановила распространение обновления безопасности для Windows, которое закрывает уязвимости Meltdown и Spectre. Патч стал причиной полного отключения компьютеров с процессорами AMD. Об этом во вторник, 9 января, сообщает The Verge.



3 января пресса сообщила о серьёзной уязвимости процессоров Intel на уровне архитектуры. С её помощью злоумышленн… …т получить доступ к ядру процессора и личной информации по…

Вскоре после обнаружения уязвимост… …визво… …раци… …х систем начали спешно выпускать апдейты. … вышл… … Windows 10. Apple частично устран… …уязви…

Уязвимость обхода аутентификации в P4 предоставляет хакерам возможность раскрыть важные данные.

В продуктах SAP исправлены 26 уязвимостей

Наиболее опасные уязвимости позволяют скомпрометировать систему и осуществить DoS-атаку.

Текст Julia Glazova 7 апреля 2018 , 02:39

В Интернете зафиксирован всплеск активности бота, эксплуатирующего новую брешь на устройствах под Cisco IOS.

MICROSOFT УСТРАНИЛА 16 КРИТИЧЕСКИХ УЯЗВИМОСТЕЙ

11 января 2018 , 15:53

…елала январь весьма жарким …исправлений. Традиционный …аплат для десятков других …e, ASP.NET и версии Office для …

Шестнадцать патчей из нового набора от Microsoft устраняют критические уязвимости, 38 помечены как важные, а один — как низкой важности. Двадцать исправленных ошибок потенциально могли повлечь удаленное исполнение произвольного кода.

…интеллекта.

…бэкдор из своей …системы IOS XE

…XE 16.x …скрытой учетной …анию с именем …sco» и статическим

В решении Cisco Elastic Services Controller обнаружена опасная уязвимость

Злоумышленник может авторизоваться в учетной записи администратора с пустым полем пароля.

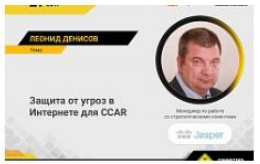
Cisco устранила критическую уязвимость в своих межсетевых экранах

Проблема позволяет удаленно выполнить код и получить контроль над устройством.

…ла ряд …язвимостей в …vEdge

Уязвимости позволяют удаленному злоумышленнику добиться отказа в обслуживании и выполнить произвольный код.

Как обезопасить умный автомобиль? Мнение экспертов из «ИнЧип» и Cisco



Хакерам ничего не стоит дистанционно взломать компьютерную систему смарткара.

Cisco устранила опасные уязвимости в ПО IOS

В общей сложности Cisco исправила 13 уязвимостей.

КОД БЕЗОПАСНОСТИ

В КАЧЕСТВЕ ПЕРВОГО ШАГА. ГЕТЕРОГЕННАЯ СРЕДА…

С ХОДУ ЗАМЕСТИТЬ ИМПОРТНЫЕ РЕШЕНИЯ НЕ ПОЛУЧИТСЯ

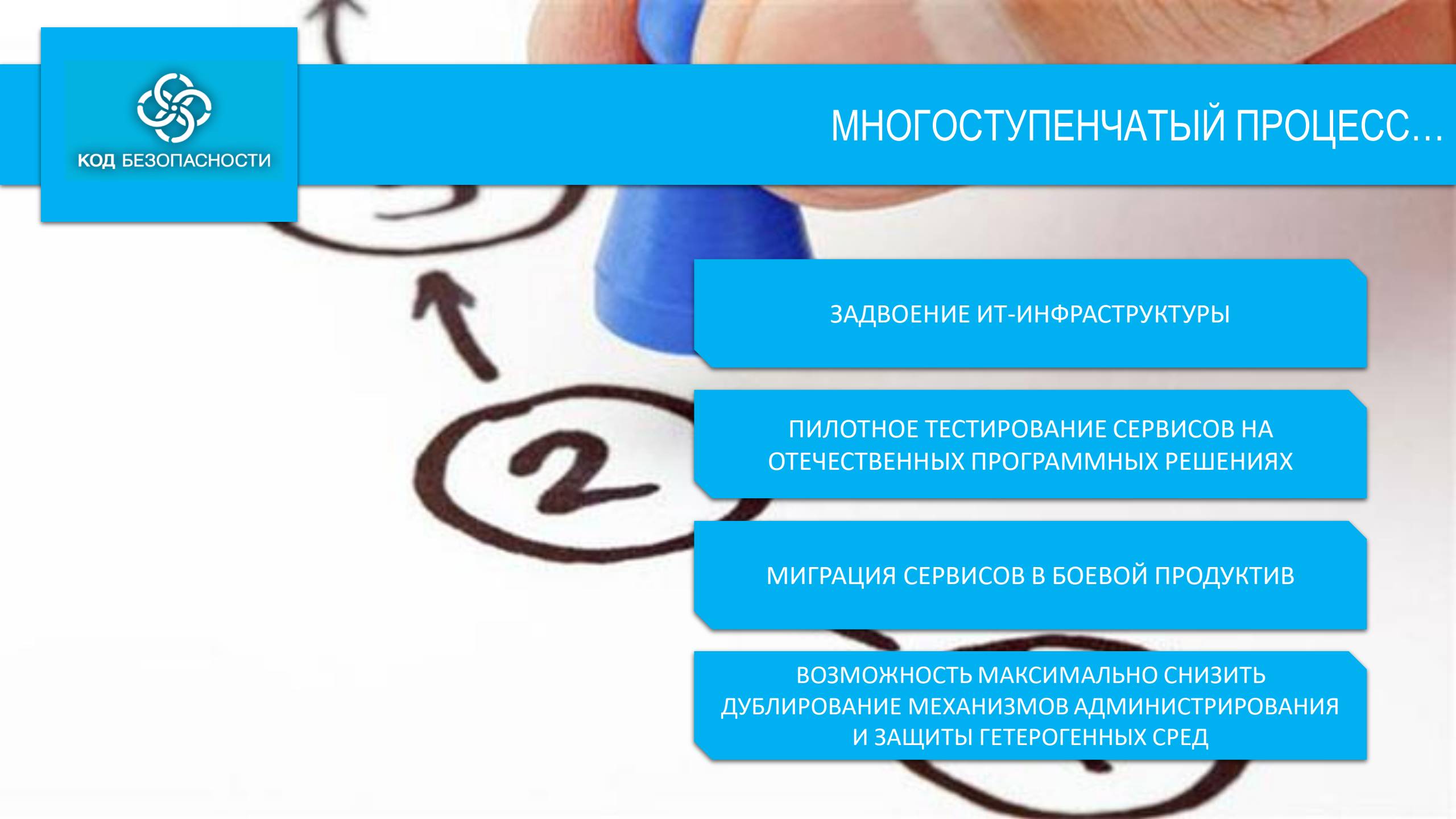
ПАРАЛЛЕЛЬНОЕ РАЗВЕРТЫВАНИЕ ИМПОРТОНЕЗАВИСИМОЙ СРЕДЫ БУДЕТ ДОЛГИМ И ДОРОГИМ

ПОДГОТОВКА И ПЕРЕКВАЛИФИКАЦИЯ КАДРОВ ОБЯЗАТЕЛЬНА! КАК И ПИЛОТИРОВАНИЕ!

ПЛАВНАЯ МИГРАЦИЯ СЕРВИСОВ И ИНФОРМАЦИОННЫХ СИСТЕМ

КОД БЕЗОПАСНОСТИ

МНОГОСТУПЕНЧАТЫЙ ПРОЦЕСС…



ЗАДВОЕНИЕ ИТ-ИНФРАСТРУКТУРЫ

ПИЛОТНОЕ ТЕСТИРОВАНИЕ СЕРВИСОВ НА ОТЕЧЕСТВЕННЫХ ПРОГРАММНЫХ РЕШЕНИЯХ

МИГРАЦИЯ СЕРВИСОВ В БОЕВОЙ ПРОДУКТИВ

ВОЗМОЖНОСТЬ МАКСИМАЛЬНО СНИЗИТЬ ДУБЛИРОВАНИЕ МЕХАНИЗМОВ АДМИНИСТРИРОВАНИЯ И ЗАЩИТЫ ГЕТЕРОГЕННЫХ СРЕД

КОД БЕЗОПАСНОСТИ

СОЗДАНИЕ ГЕТЕРОГЕННОЙ СРЕДЫ НЕ НОВОСТЬ…

ПРИКАЗ ФСТЭК №17

XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)
ЗИС.25 - Использование в информационной системе или ее сегментах различных типов общесистемного, прикладного и специального программного обеспечения (создание гетерогенной среды)

ПРИКАЗ ФСТЭК №31

XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)
ЗИС.9 - Создание гетерогенной среды
ЗИС.10 - Использование программного обеспечения, функционирующего в средах различных операционных систем

ПРИКАЗ ФСТЭК №239

XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)
ЗИС.9 - Создание гетерогенной среды
ЗИС.10 - Использование программного обеспечения, функционирующего в средах различных операционных систем

КОД БЕЗОПАСНОСТИ

ПРИЧЕМ ЗДЕСЬ МЫ…

Ведущий российский разработчик
средств защиты информации.

Самый широкий портфель решений по ИБ.

3 центра разработки – Москва, Санкт-Петербург, Пенза. Более
300 разработчиков.

Полный цикл работ.
Проектирование, внедрение, сопровождение.

Более 70-ти сертификатов ФСТЭК, ФСБ, МО
на всю продуктовую линейку.

КОД БЕЗОПАСНОСТИ

ПРЕДМЕТНО ПО ЗАЩИТЕ ГЕТЕРОГЕННЫХ СРЕД…

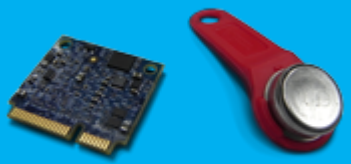
SECRET NET STUDIO 8.5	SECRET NET LSP 1.9	ПАК СОБОЛЬ 4.2
WINDOWS СЗИ ОТ НСД МЕЖСЕТЕВОЙ ЭКРАН КОНТРОЛЬ УСТРОЙСТВ СОВ АНТИВИРУС (ESET, Clam AV, Kaspersky) ЛОКАЛЬНОЕ ШИФРОВАНИЕ ДОВЕРЕННАЯ СРЕДА	ОС LINUX СЗИ ОТ НСД	WINDOWS / ОС LINUX АПМДЗ

КОД БЕЗОПАСНОСТИ

НА СТАРТЕ РАБОТЫ АРМ…

ПАК СОБОЛЬ 4.2
Аппаратно-программный модуль доверенной загрузки

КОРРЕКТНАЯ РАБОТА КАК С UEFI-БИОСОМ, ТАК И С LEGACY-БИОСОМ
ОБЕСПЕЧЕНИЕ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ
БЛОКИРОВКА ЗАГРУЗКИ ОС СО СЪЁМНЫХ НОСИТЕЛЕЙ
КОНТРОЛЬ ЦЕЛОСТНОСТИ ФАЙЛОВ И СЕКТОРОВ ЖЕСТКОГО ДИСКА
КОНТРОЛЬ ЦЕЛОСТНОСТИ АППАРАТНОЙ СРЕДЫ
КОНТРОЛЬ ЦЕЛОСТНОСТИ РЕЕСТРА ОС
СТОРОЖЕВОЙ ТАЙМЕР
ФИЗИЧЕСКИЙ ДАТЧИК СЛУЧАЙНЫХ ЧИСЕЛ
ИСПОЛНЕНИЕ - 5 ФОРМ-ФАКТОРОВ



КОД БЕЗОПАСНОСТИ

В OPEN SOURCE СРЕДЕ…

SECRET NET LSP

Средство защиты информации от несанкционированного доступа

ЗАМКНУТАЯ ПРОГРАММНАЯ СРЕДА
ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ
РАЗГРАНИЧЕНИЕ ДОСТУПА К РЕСУРСАМ КОМПЬЮТЕРА
РАЗГРАНИЧЕНИЕ ДОСТУПА К УСТРОЙСТВАМ
КОНТРОЛЬ ЦЕЛОСТНОСТИ ПРОГРАММНОЙ СРЕДЫ
ОЧИСТКА ОСВОБОЖДАЕМЫХ ОБЛАСТЕЙ ОПЕРАТИВНОЙ ПАМЯТИ

base alt

РЕД ОС

ЛОТОС
операционная система

ASTRA LINUX

КОД БЕЗОПАСНОСТИ

ФУНКЦИОНАЛ ДЛЯ СЕМЕЙСТВА WINDOWS…

SECRET NET STUDIO

Средство защиты информации от несанкционированного доступа

ХОСТОВЫЙ МЕЖСЕТЕВОЙ ЭКРАН С АВТОРИЗАЦИЕЙ СОЕДИНЕНИЙ
МАНДАТНЫЙ И ДИСКРЕЦИОННЫЙ ДОСТУП
КОНТРОЛЬ СЪЁМНЫХ НОСИТЕЛЕЙ
КОНТРОЛЬ ЦЕЛОСТНОСТИ ДАННЫХ
КОНТРОЛЬ ЦЕЛОСТНОСТИ ФАЙЛОВ РЕЕСТРА
ЗАМКНУТАЯ ПРОГРАММНАЯ СРЕДА
ШИФРОВАНИЕ КОНТЕЙНЕРОВ
ЗАТИРАНИЕ ДАННЫХ
ТЕНЕВОЕ КОПИРОВАНИЕ
ШАБЛОНЫ ПОЛИТИК БЕЗОПАСНОСТИ
HIPS – СОВ
ДОВЕРЕННАЯ СРЕДА
ОЕМ-ДОПОЛНЕНИЯ ОТ ЛАБОРАТОРИИ КАСПЕРСКОГО

КОД БЕЗОПАСНОСТИ

ОЕМ-СОТРУДНИЧЕСТВО…

ИНТЕГРИРОВАННЫЙ АНТИВИРУС
(KASPERSKY AV)
БЛОКИРОВКА ВРЕДОНОСНЫХ IP-АДРЕСОВ
БЛОКИРОВКА ФИШИНГОВЫХ URL-АДРЕСОВ
БЛОКИРОВКА БОТНЕТ СЕТЕЙ

KASPERSKY lab

КОД БЕЗОПАСНОСТИ

ДОВЕРЕННАЯ СРЕДА…

- Реагирование на попытки влияния (деактивации) механизмов защиты информации
- Защита от подмены драйверов и эксплуатации уязвимости драйверов
- Блокирование выгрузки штатных драйверов
- Предотвращение выгрузки процессов защитных механизмов
- Аварийное прекращение работы ИТ-ресурса при обнаружении проведения целевой атаки

КОД БЕЗОПАСНОСТИ

ЕДИНАЯ ПОЛИТИКА ПОДДЕРЖКИ ИДЕНТИФИКАТОРОВ…

JaCarta PRO	JaCarta U2F	Рутокен ЭЦП SC
JaCarta-2 PRO/ГОСТ	iBUTTON	Рутокен Lite
JaCarta-2 SE	JaCarta WebPass	Рутокен S

КОД БЕЗОПАСНОСТИ

ГОТОВОЕ ИНФРАСТРУКТУРНОЕ РЕШЕНИЕ…

WEB-интерфейс управления
Поддержка клиентов удаленных сессий
Работа с веб-приложениями
Возможность установки на терминал дополнительного ПО
Поддержка периферийного оборудования
Встроенная система печати и сканирования
Проброс устройств
Гибкая настройка работы в пользовательских сценариях
Авторизация пользователей Active Directory
Поддержка VDI-платформ VMware Horizon и Citrix ICA

CONTINENT OS
ВСТРОЕННОЕ СЗИ ОТ НСД
ВСТРОЕННЫЙ АПМДЗ
ВСТРОЕННЫЙ ПРОГРАММНЫЙ VPN

КОД БЕЗОПАСНОСТИ

РЕЗЮМИРУЯ…

Централизованное управление защитными механизмами под Windows и Linux из одной точки

Минимизация человеческих ресурсов для обслуживания средств защиты на рабочих станциях и серверах

Выгрузка событий по информационной безопасности в SIEM-системы из единой консоли управления

БЛАГОДАРЮ ЗА ВНИМАНИЕ!

Роман Лопатин
r.lopatin@securitycode.ru
+7 (495) 982 30 20 (*491)
+7 (926) 567 39 86