Обзор практик взаимодействия государства и бизнеса в области защиты критичной инфраструктуры

27 июля 2018

Роман Чаплыгин
Руководитель практики кибербезопасности и непрерывности бизнеса, PwC в России

pwc

Определение SOC и CERT

Центр мониторинга информационной безопасности (SOC) –

это выделенное структурное подразделение, осуществляющее мониторинг и реагирование на инциденты информационной безопасности.

Основные функции

Непрерывное выявление кибератак и инцидентов ИБ

Упреждающая реакция на новые уязвимости и угрозы ИБ

Быстрое устранение последствий инцидентов ИБ

Computer Emergency Response Team (CERT) –

это централизованное подразделение или выделенная организация, основной деятельностью которой раннее информирование о новых угрозах ИБ и обмен.

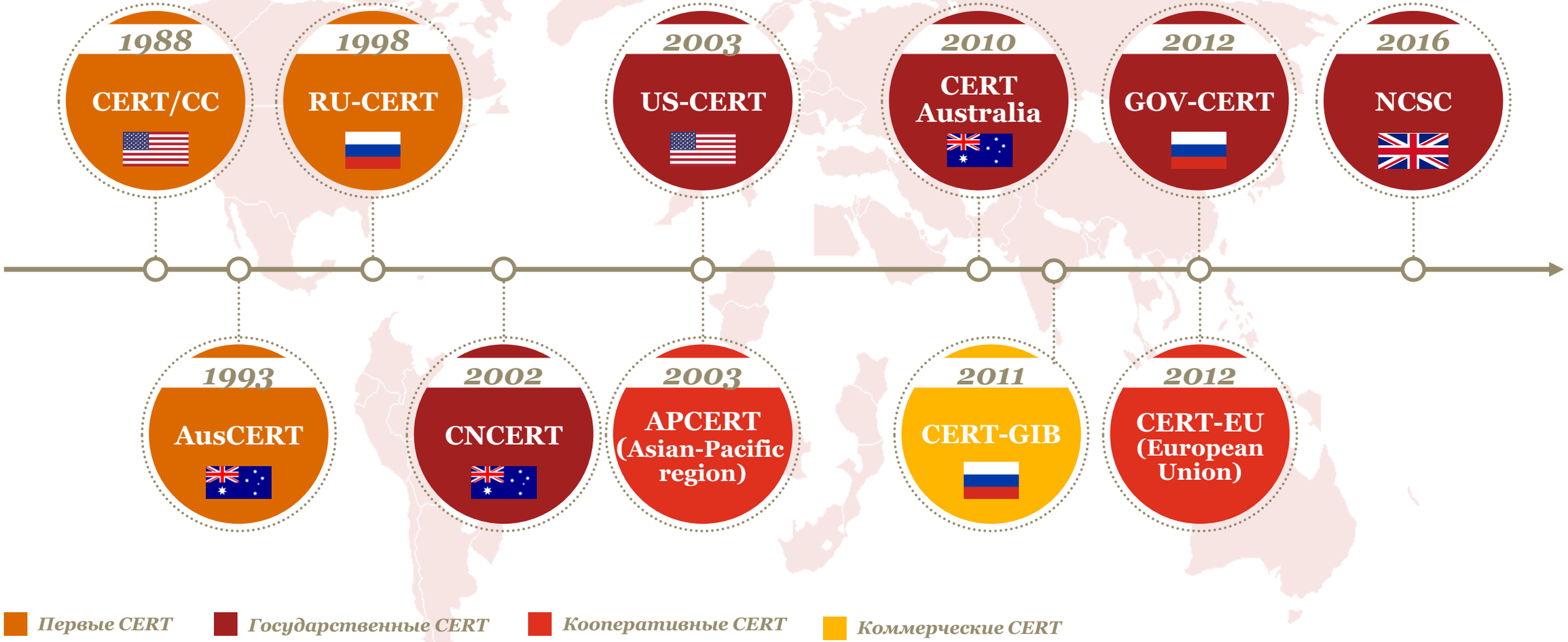
Основные функции

Глубокий анализ и подробное исследование новых угроз

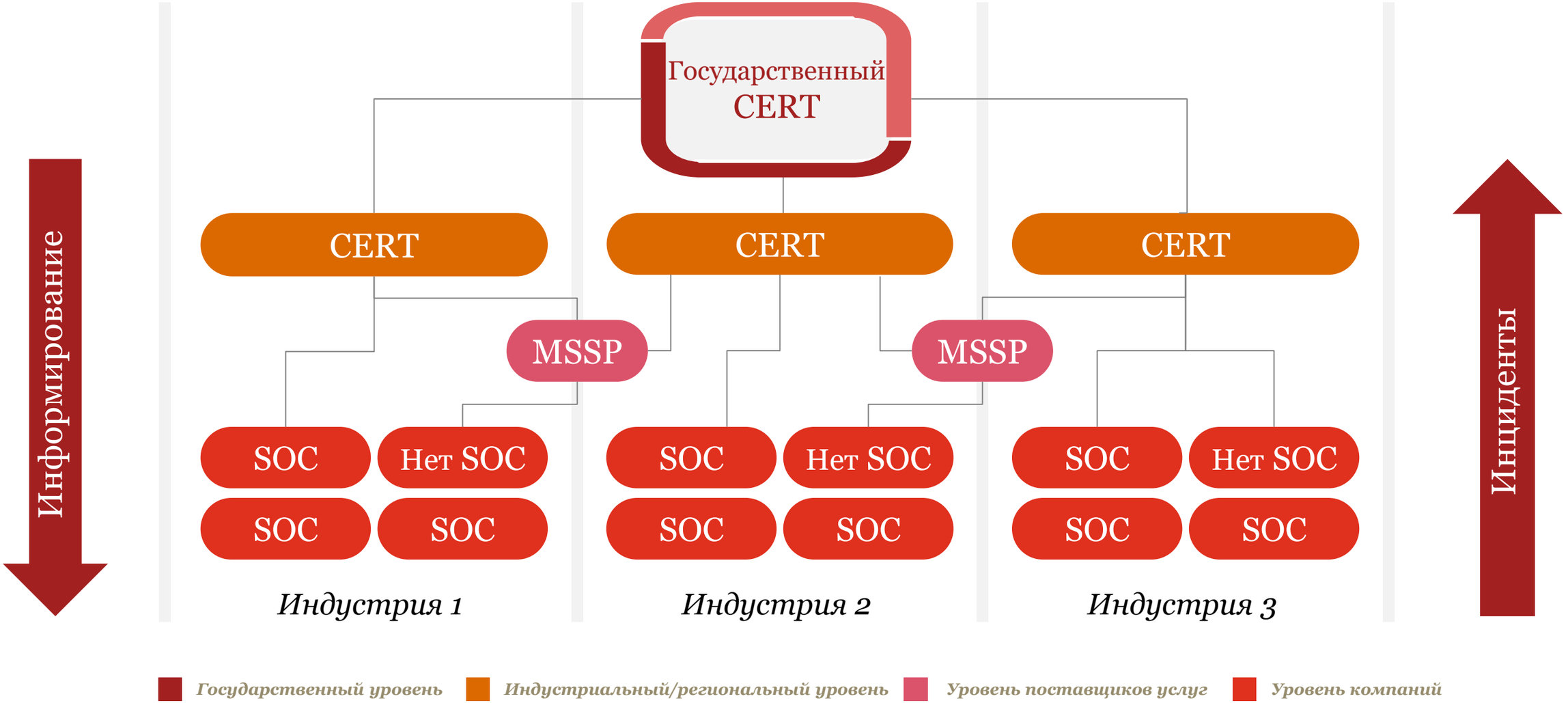
Информирование заинтересованных сторон

Координация и разработка инструкций по устранению уязвимостей

Обзор мировых практик



Инфраструктура государственного CERT

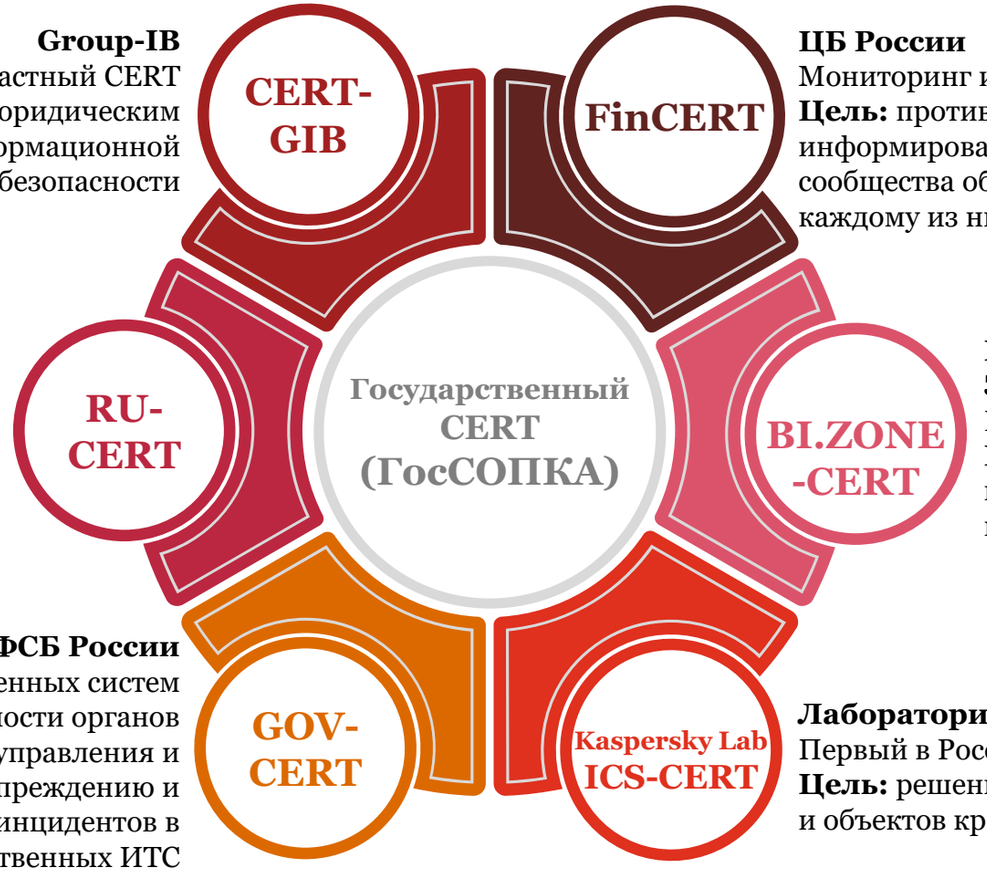


Обзор российских CERT

Group-IB
Первый в России частный CERT
Цель: : оказание оперативной помощи юридическим физическим лицам в случаях нарушения информационной безопасности

РосНИИРОС
Первый центр реагирования в России
Цель: снижение уровня угроз информационной безопасности для пользователей российского сегмента сети Интернет

ФСБ России
Защита государственных систем
Цель: обеспечение координации деятельности органов государственной власти, органов местного самоуправления и правоохранительных органов по выявлению, предупреждению и устранению последствий компьютерных инцидентов в государственных ИТС



ЦБ России
Мониторинг и реагирование в кредитно-финансовой сфере
Цель: противодействие злоумышленникам путем взаимного информирования и оповещения участников банковского сообщества об уязвимостях, угрозах и рисках, с которыми каждому из них приходится сталкиваться

BI.ZONE (Сбербанк)
Защита активов и репутации бизнеса в сети Интернет
Цель: выявление киберугроз, попыток взлома и тестирования систем безопасности крупнейшего российского банка

Лаборатория Касперского
Первый в России промышленный CERT
Цель: решение задач защиты промышленных предприятий и объектов критически важных инфраструктур

Российский подход к национальной кибербезопасности (ФЗ-187)

- Ведение реестра значимых объектов критической информационной инфраструктуры (КИИ), который включает в себя категоризацию объектов, детали цифрового взаимодействия объектов КИИ в телекоммуникационных сетях и др. информация
- Разработка единых требований к кибербезопасности объектов КИИ, включая интеграцию в иерархическую структуру национального CERT (ГосСОПКА)
- Проведение мероприятий по оценке степени защищенности КИИ от кибератак

Федеральный закон о безопасности критической информационной инфраструктуры Российской Федерации способствует развитию единого подхода, предназначенного для предотвращения, обнаружения и ликвидации последствий компьютерных атак на критичные объекты информационной инфраструктуры.

Подход к национальной кибербезопасности в Европейском Союзе

- Каждая из 28 стран ЕС должна создать один или несколько CERT, покрывающих все ключевые индустрии. Работа над уменьшением несоответствий в законодательстве стран ЕС
- Головным центром для всех стран становится CERT-EU, который координирует национальные CERT стран-членов ЕС
- Сотрудничество с коммерческими организациями-производителями средств защиты информации – это шаг к сокращению технологического разрыва с США для создания собственных технических решений защиты критической инфраструктуры

Директива по сетевой и информационной безопасности (NIS) дает возможность сосредоточить внимание на защите наиболее важных сервисов и активов государств - членов ЕС и позволит сократить разрыв в уровне зрелости ИБ стран ЕС.

Европейская комиссия подписала в июле 2016 года соглашение о создании государственно-частного партнерства для разработки единого подхода к обеспечению кибербезопасности.

ЕС инвестирует в данное объединение до € 450 млн в рамках своей программы исследований и инноваций Horizon 2020 на 2017-2020 гг. (4 года). Ожидается, что участники рынка кибербезопасности инвестируют в три раза больше: в общей сложности около €1800 млн.

Сравнительный анализ практики обеспечения кибербезопасности КИИ

	США	*Германия*	*Россия*	*Англия*	*ОАЭ*	*Китай*
1. Существует ли законы/политики, требующие защиты критической инфраструктуры от угроз кибербезопасности?	✓	✓	✓	✓	✓	✓
1.1. Существует ли законы/политики, которые требуют (по крайней мере) ежегодного аудита кибербезопасности?	✓	~	✗	✗	-	✓
1.2. Существует ли законы/политики, которые требуют обязательное оповещение об инцидентах кибербезопасности?	✗	✓	~	✗	✗	✓
1.3. Существуют ли санкции в случае несоблюдения этих нормативных требований?	✓	✓	✓	✓	✓	✓
1.4. Эти нормативные требования применимы к частным компаниям?	~	✓	✓	✓	-	✓
2. Существует ли государственный центр реагирования на инциденты ИБ (CERT) или группа по реагированию на инциденты ИБ (CSIRT)?	✓	✓	~	✓	✓	✓
2.1. В каком году был создан государственный центр реагирования на чрезвычайные ситуации (CERT)?	2003	2012	2012	2014	2007	2002
2.2. Существуют ли некоммерческие организации, которые поддерживают инициативы или проекты, направленные на развитие, продвижение и поддержку кибербезопасности?	✓	✓	✗	✓	✓	✓
3. Существует ли государственный центр мониторинга информационной безопасности (SOC)?	✗	✓	✗	✗	✓	✓

~ *- В процессе* ✓ *- Да* ✗ *- Нет*

Направления дальнейшего развития

www.pwc.ru/cybersecurity

Роман Чаплыгин

Руководитель практики кибербезопасности и непрерывности бизнеса, PwC в России

Email: *roman.chaplygin@pwc.com*