JET SECURITY CONFERENCE

VIII ежегодная конференция
Центра информационной безопасности

1-2 июня 2017 года

WWW.JET.SU

Radisson BLU

Check Point SOFTWARE TECHNOLOGIES LTD
Premier Business Partner IBM
Hewlett Packard Enterprise
f5
IMPERVA
SKYBOX SECURITY
INFOWATCH МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ
TREND MICRO
paloalto NETWORKS
FireEye
KASPERSKY PLATINUM PARTNER
POSITIVE TECHNOLOGIES
tufin
FORTINET
SOLAR SECURITY software&services
CYBERARK
TRAPX SECURITY
ONE IDENTITY
RAPID7
iDeals VIRTUAL DATA ROOM

JET CONFERENCE

01/06/2017

Немного про ГосСОПКУ

Екатерина Сюртукова,
руководитель направления сервиса и аутсорсинга ИБ

JET

CONFERENCE

ГосСОПКА

Система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

JET

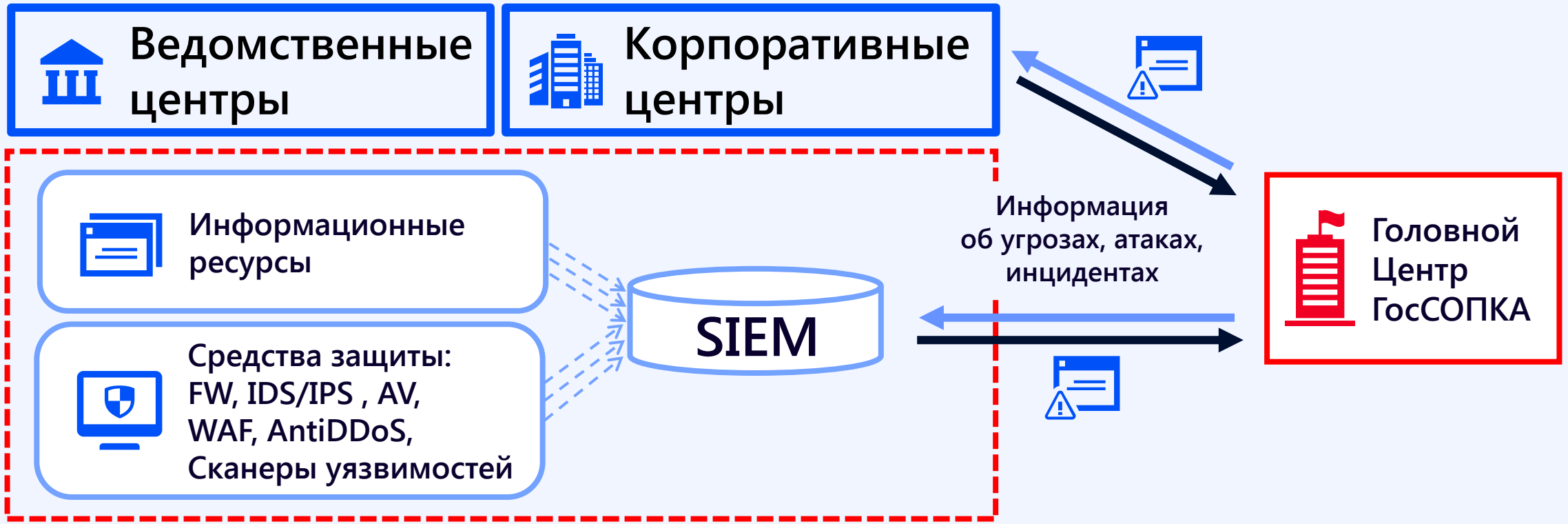
CONFERENCE

Нормативная база

- **Указ Президента РФ от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»**
- **«Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»**
  (утв. Президентом РФ 12.12.2014 № К 1274)
- **На рассмотрении Законопроект «О безопасности критической информационной инфраструктуры Российской Федерации»**
- **Разрабатываются «Методические рекомендации по созданию ведомственных и корпоративных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».**

JET CONFERENCE

Как это будет



JET
CONFERENCE

Типы инцидентов

Группа 1 (вес — 4)

- ВПО (включая APT и бот-агент)
- несанкционированный доступ
- эксплуатация уязвимости

Группа 2 (вес — 3)

- DoS/DDoS
- перебор паролей
- ЦУ бот-сети

Группа 3 (вес — 2)

- фишинг (мошенничество)
- вредоносный ресурс
- запрещенный контент

Группа 4 (вес — 1)

- сканирование ресурсов
- спам
- нарушение политики безопасности, другое

JET
CONFERENCE

Что нужно

Тех. средства

- SIEM
- Сканер
- Средства защиты
- Service Desk
- …

Процессы

- Мониторинг
- Реагирование
- Сканирование
- Анализ угроз
- …

Люди

- Группа мониторинга
- Группа реагирования
- Аналитик
- Администраторы
- …

JET

CONFERENCE

Где взять людей?

- Группа мониторинга — 5-7 чел.
- Группа реагирования — 2-3 чел.
- Аналитик — 1 чел.
- Технически эксперт — 1 чел.
- Администратор SIEM — 1-2 чел.
- Администратор СЗИ — 5 чел.
- …

JET CONFERENCE

01/06/2017

ИНФОСИСТЕМЫ ДЖЕТ

Спасибо за внимание!