ИНФОСИСТЕМЫ ДЖЕТ

Безопасность как на ладони

Игорь Ляпунов
Директор Центра информационной безопасности
ЗАО «Инфосистемы Джет»

24 февраля 2014 г.

ИНФОСИСТЕМЫ ДЖЕТ

или

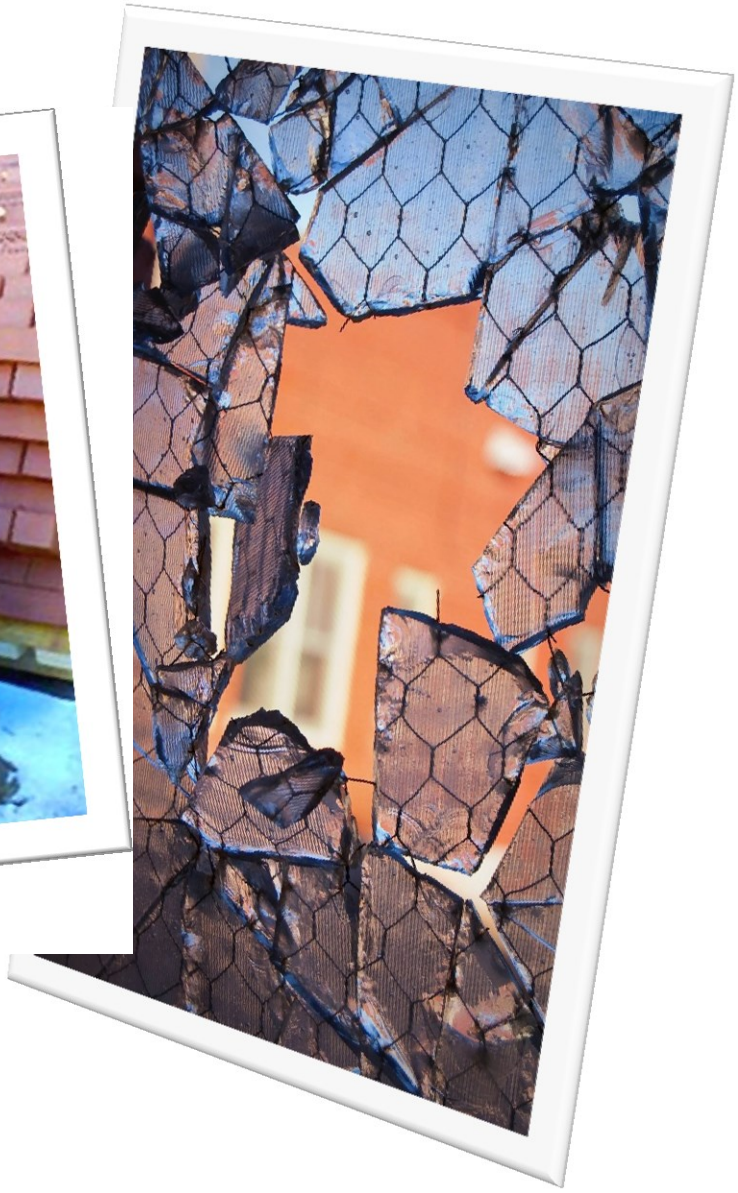
Системы поддержки принятия решений для руководителей ИБ

Игорь Ляпунов
Директор Центра информационной безопасности
ЗАО «Инфосистемы Джет»

24 февраля 2014 г.

Откуда мы узнаем о проблемах?

Откуда мы узнаем о проблемах?



Проблематика и очевидное решение?

- Большое количество средств обеспечения ИБ
- Трудность получения целостной картины о состоянии ИБ
- Дефицит человеческих ресурсов для анализа информации, полученной от средств ИБ

SOC

И целого SOC'а мало…

- Что «интересного» из SOC показать руководству?
- Стали ли мы лучше и защищеннее?
- Как проведенные мероприятия повлияли на уровень ИБ, была ли отдача?
- Как инциденты на объектах инфраструктуры влияют на критичные ИС, бизнес-процессы?
- Допустимо ли возникновение инцидентов на этой ИС именно в это время?

В голове у руководителя ИБ много интересного…

И это не только забота об обеспечении КЦД информации…

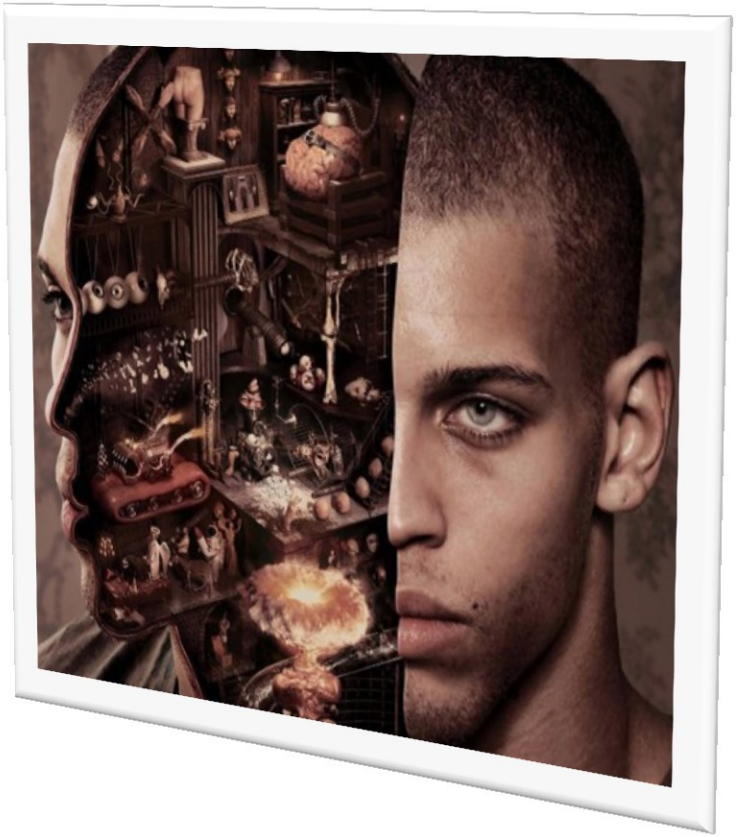
А как идут проекты по ИБ?

А что происходит в филиалах и допофисах?

А как повлиял последний инцидент на бизнес?

А сильно ли мешает ИБ бизнесу?

А как объяснить бизнес-руководителю чем мы занимаемся?



Следующий шаг

- Создание центра аналитики ИБ в рамках единого интерфейса
- Создание иерархии показателей эффективности ИБ – от бизнес-уровня до «технических» показателей
- Проведение разноуровневой аналитики по данным, получаемым от систем обеспечения ИБ

Возможные объекты мониторинга

Защита БД

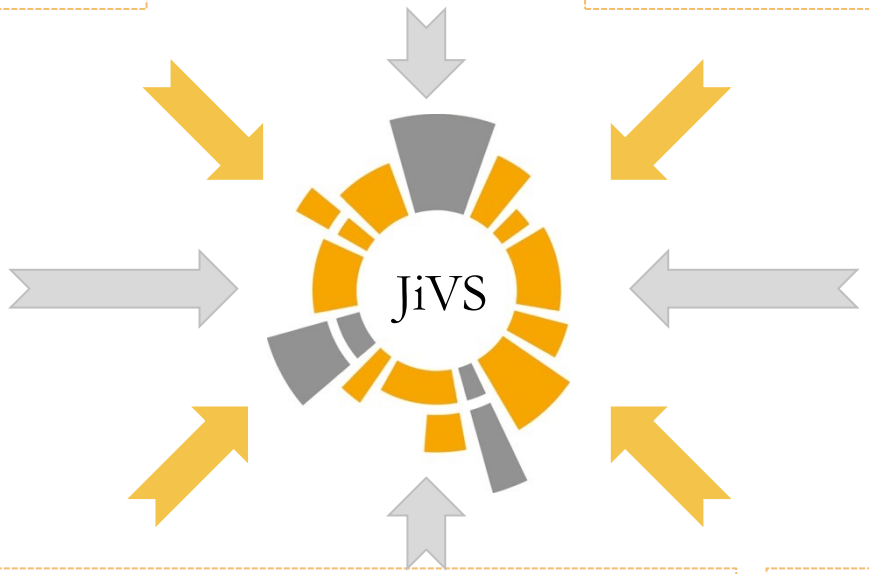
SIEM

Сканер защищенности

Защита web-приложений

Antivirus

DLP



Защита каналов

ITSM

Web-фильтрация

Сетевая защита

Любая иная система

Защита от утечек через съемные носители

Структура Jet inView Security

Уровни мониторинга и аналитики

Security Intelligence

SOC

Стратегический уровень

- Соответствие бизнес-целям
- Анализ и прогнозирование

Тактический уровень

- Контроль KPI
- Отчетность и метрики

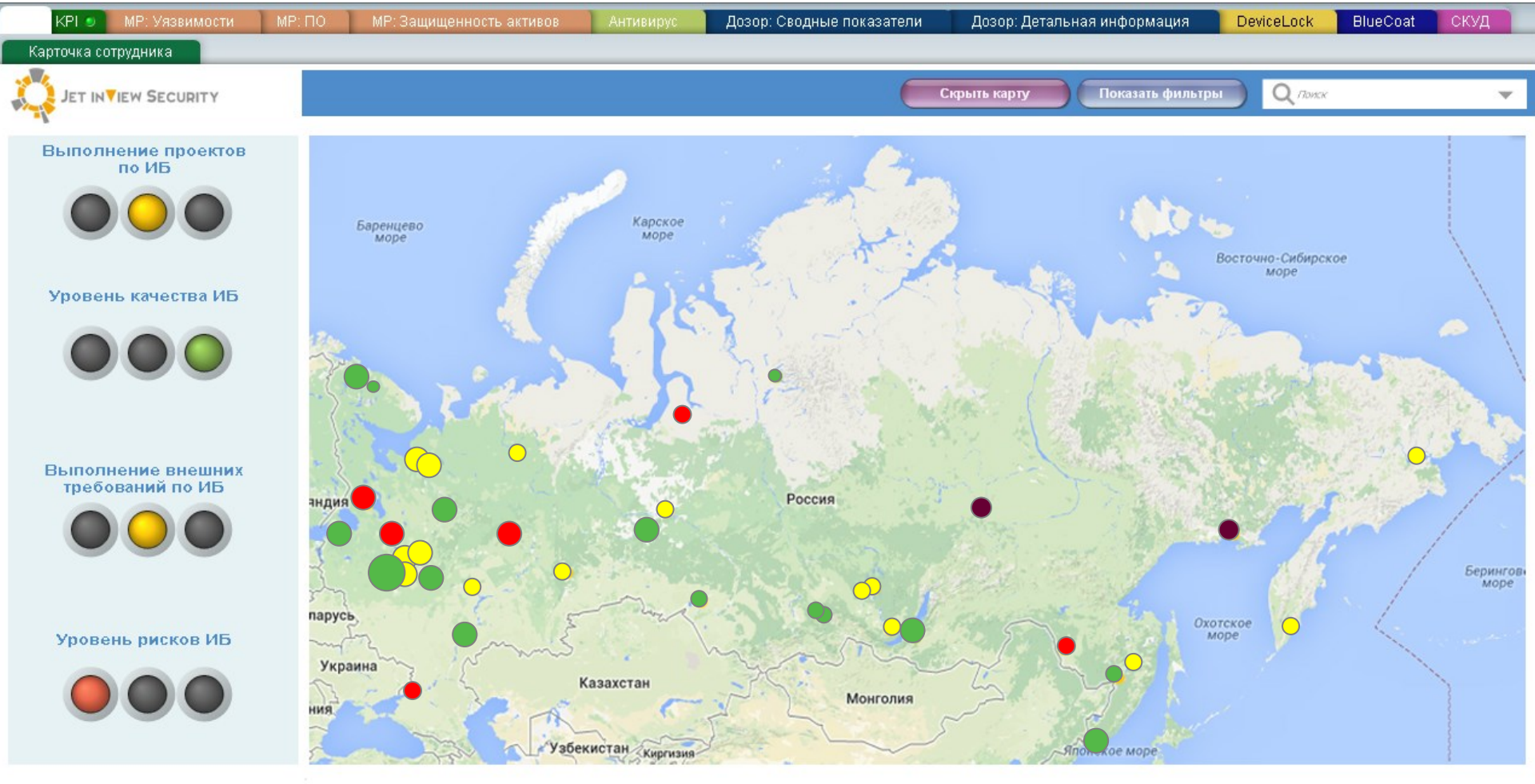
Операционный уровень

- Мониторинг ИБ

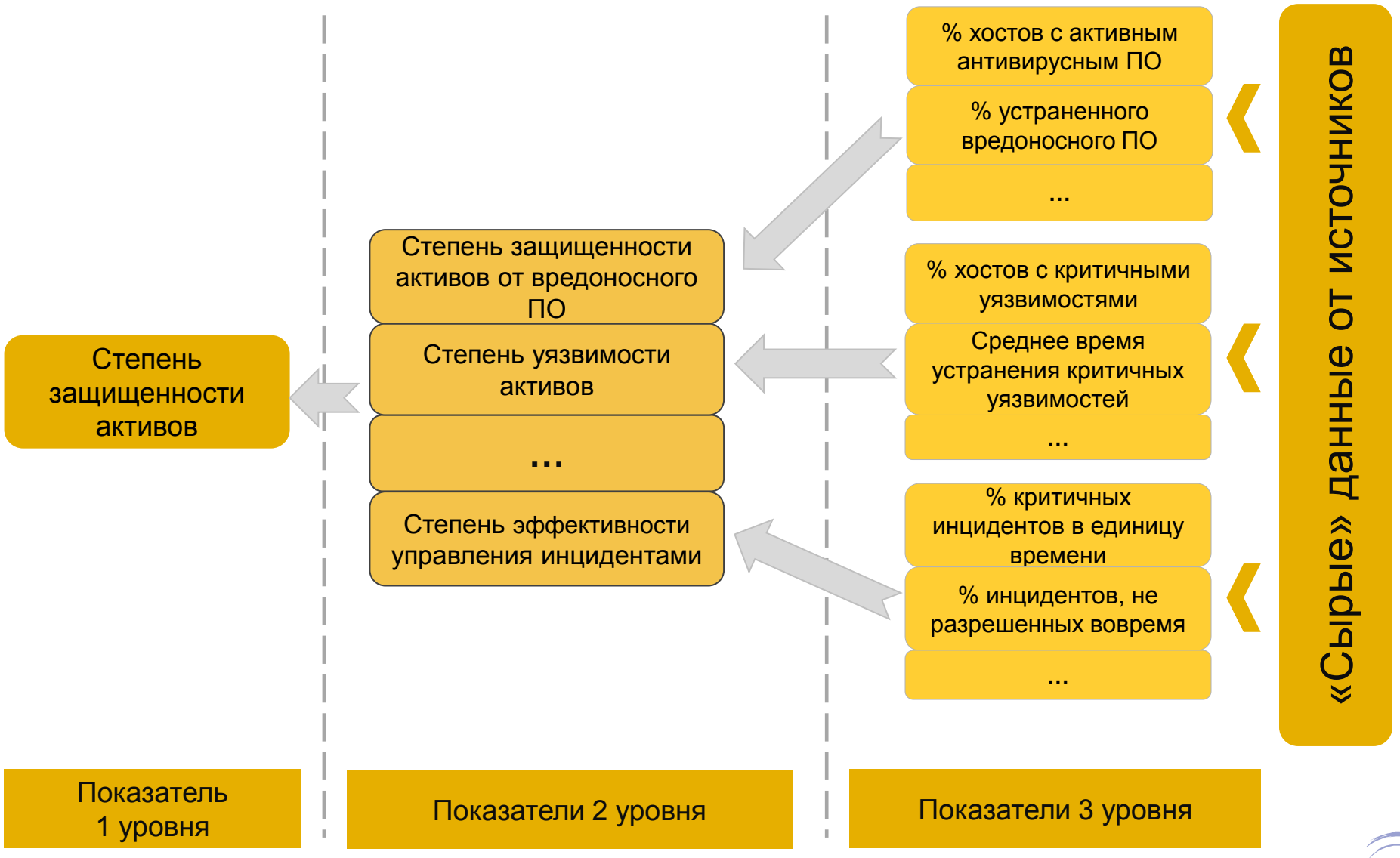
Задачи, решаемые Центром аналитики ИБ

- Централизованная аналитика деятельности по ИБ
- Оценка результативности и эффективности подразделения ИБ
- Поведенческий анализ работы систем и пользователей
- Определение реального уровня защищенности бизнес-систем
- Оценка эффективности взаимодействия подразделений при обеспечении ИБ

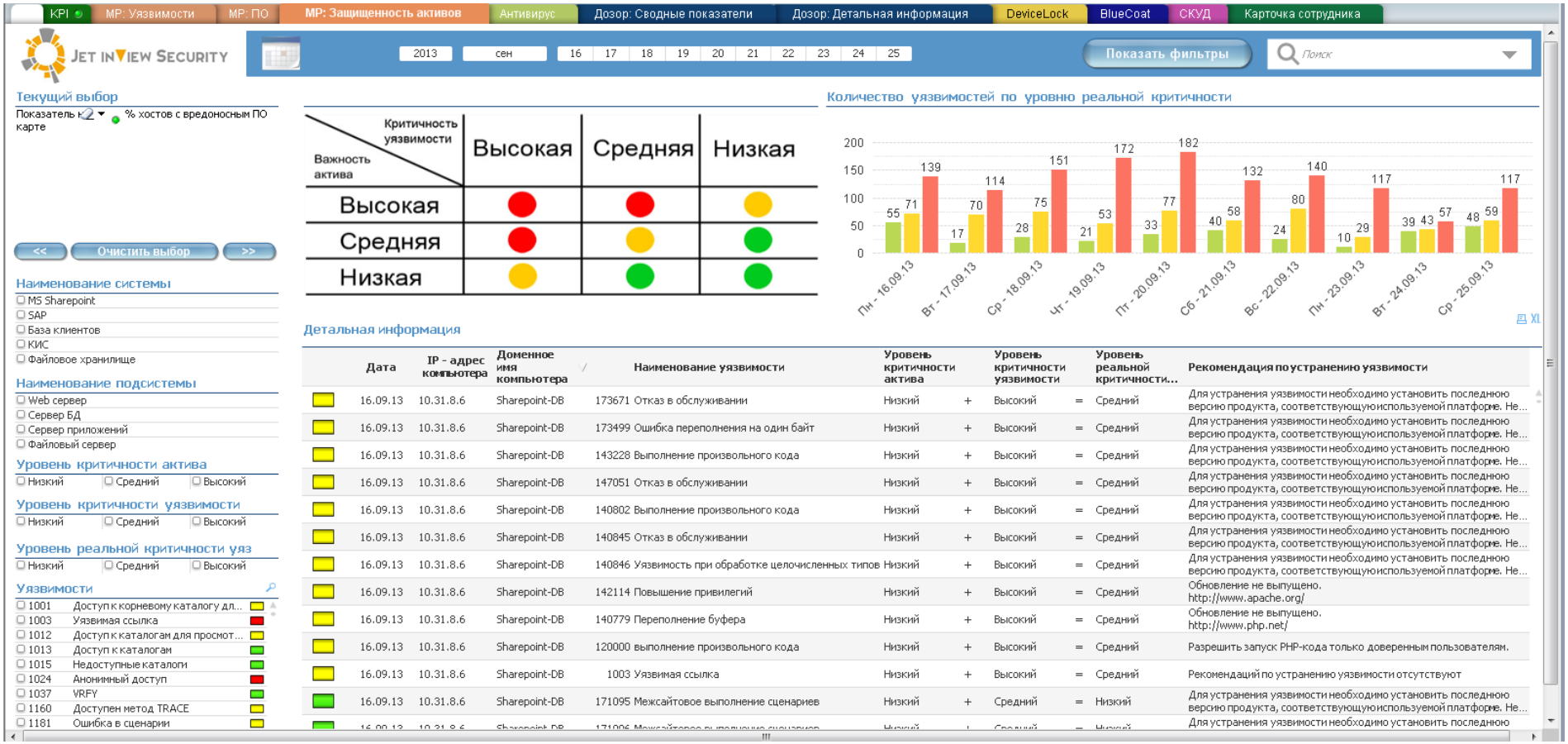
Централизованная аналитика ИБ



Оценка результативности и эффективности

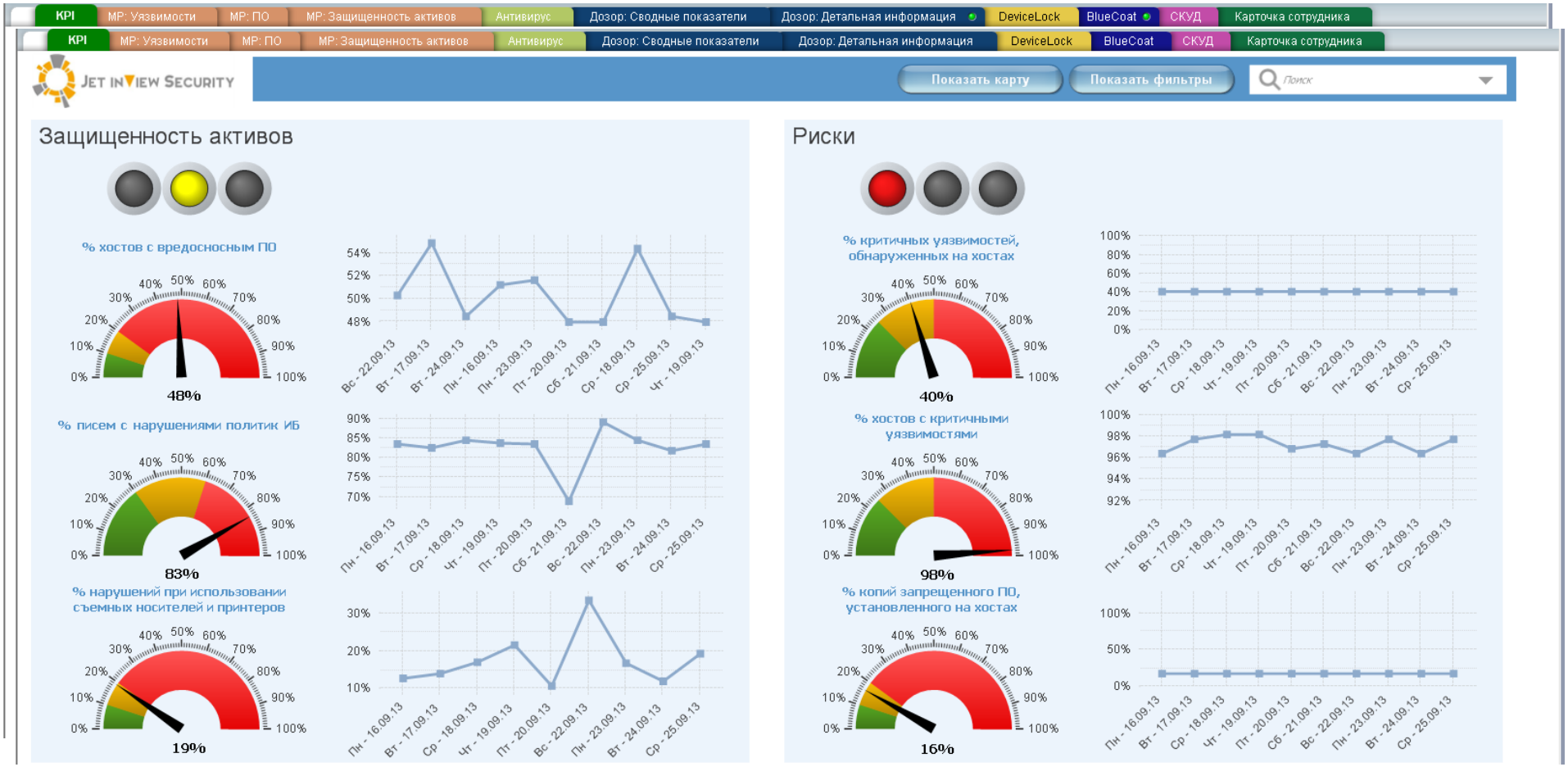


Оценка реальной защищенности бизнес-систем

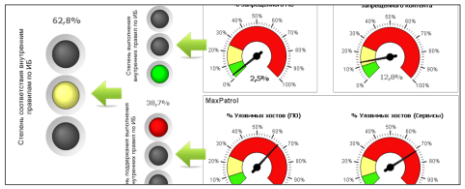


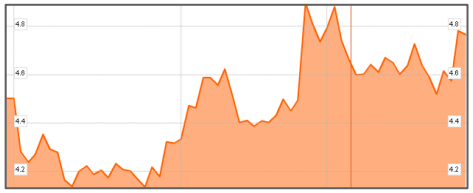
Дата	IP - адрес компьютера	Доменное имя компьютера	Наименование уязвимости	Уровень критичности актива		Уровень критичности уязвимости		Уровень реальной критичности...	Рекомендация по устранению уязвимости
16.09.13	10.31.8.6	Sharepoint-DB	173671 Отказ в обслуживании	Низкий	+	Высокий	=	Средний	Для устранения уязвимости необходимо установить последнюю версию продукта, соответствующую используемой платформе. Не...
16.09.13	10.31.8.6	Sharepoint-DB	173499 Ошибка переполнения на один байт	Низкий	+	Высокий	=	Средний	Для устранения уязвимости необходимо установить последнюю версию продукта, соответствующую используемой платформе. Не...
16.09.13	10.31.8.6	Sharepoint-DB	143228 Выполнение произвольного кода	Низкий	+	Высокий	=	Средний	Для устранения уязвимости необходимо установить последнюю версию продукта, соответствующую используемой платформе. Не...
16.09.13	10.31.8.6	Sharepoint-DB	147051 Отказ в обслуживании	Низкий	+	Высокий	=	Средний	Для устранения уязвимости необходимо установить последнюю версию продукта, соответствующую используемой платформе. Не...
16.09.13	10.31.8.6	Sharepoint-DB	140802 Выполнение произвольного кода	Низкий	+	Высокий	=	Средний	Для устранения уязвимости необходимо установить последнюю версию продукта, соответствующую используемой платформе. Не...
16.09.13	10.31.8.6	Sharepoint-DB	140845 Отказ в обслуживании	Низкий	+	Высокий	=	Средний	Для устранения уязвимости необходимо установить последнюю версию продукта, соответствующую используемой платформе. Не...
16.09.13	10.31.8.6	Sharepoint-DB	140846 Уязвимость при обработке целочисленных типов	Низкий	+	Высокий	=	Средний	Для устранения уязвимости необходимо установить последнюю версию продукта, соответствующую используемой платформе. Не...
16.09.13	10.31.8.6	Sharepoint-DB	142114 Повышение привилегий	Низкий	+	Высокий	=	Средний	Обновление не выпущено. http://www.apache.org/
16.09.13	10.31.8.6	Sharepoint-DB	140779 Переполнение буфера	Низкий	+	Высокий	=	Средний	Обновление не выпущено. http://www.php.net/
16.09.13	10.31.8.6	Sharepoint-DB	120000 выполнение произвольного кода	Низкий	+	Высокий	=	Средний	Разрешить запуск PHP-кода только доверенным пользователям.
16.09.13	10.31.8.6	Sharepoint-DB	1003 Уязвимая ссылка	Низкий	+	Высокий	=	Средний	Рекомендаций по устранению уязвимости отсутствуют
16.09.13	10.31.8.6	Sharepoint-DB	171095 Межсайтовое выполнение сценариев	Низкий	+	Средний	=	Низкий	Для устранения уязвимости необходимо установить последнюю версию продукта, соответствующую используемой платформе. Не...
16.09.13	10.31.8.6	Sharepoint-DB	171096 Межсайтовое выполнение сценариев	Низкий	+	Средний	=	Низкий	Для устранения уязвимости необходимо установить последнюю

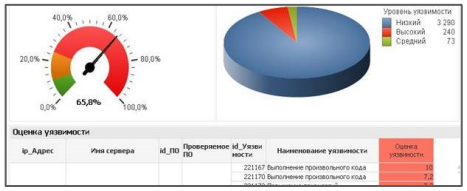
Пример реализации. Оценка эффективности ИБ



Результаты внедрения Центра аналитики ИБ







- Наглядная демонстрация руководству результатов работы
- Оценка соответствия ИБ ожиданиям бизнеса
- Контроль состояния ИБ и эффективности внедряемых мер в «одном окне»
- Сокращение трудозатрат на рутинную деятельность

Спасибо!

Игорь Ляпунов
Директор Центра информационной безопасности
+7 (495) 411-7601
+7 (495) 970-9278
liapunov@jet.msk.su