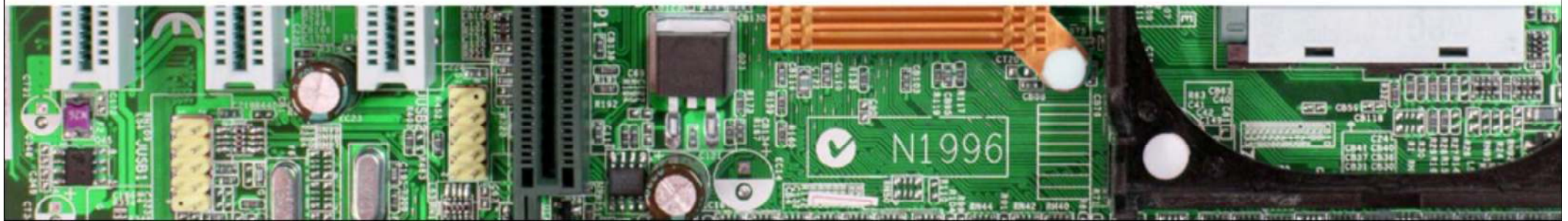
Управление инцидентами ИБ. Расследование инцидентов

Александр Астахов

Генеральный директор

Global Trust Solutions

Продукты и услуги в области информационной безопасности

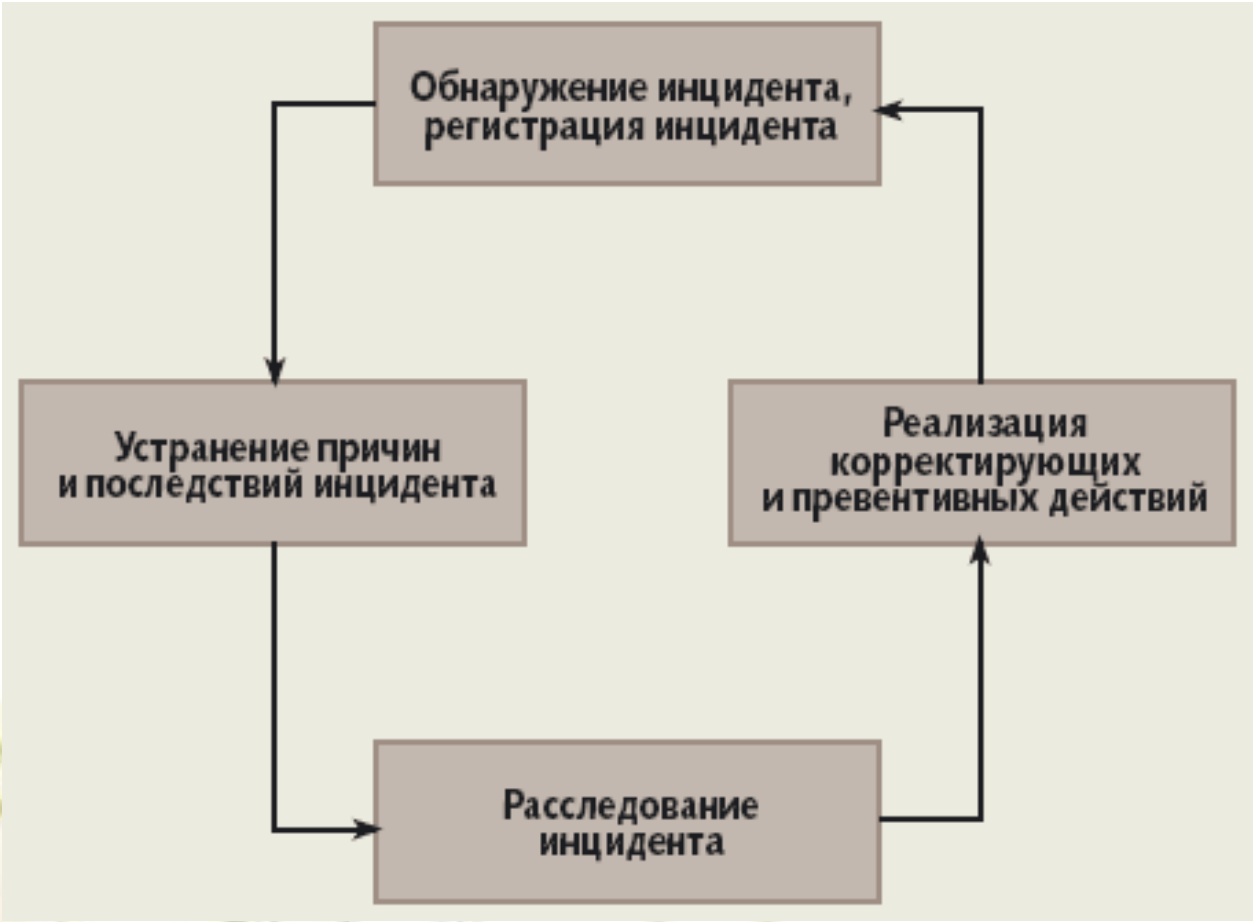


Определение понятия инцидент информационной безопасности

Инцидент ИБ – одно (или серия) нежелательных и неожиданных событий, которые могут нарушить безопасность информационных активов организации, оказать негативное воздействие на связанные с этими активами бизнес-процессы и системы и, как следствие, причинить ущерб организации.

Global Trust Solutions

Система менеджмента инцидентов ИБ



Global Trust Solutions

Классификация инцидентов ИБ

- Вирусная активность
- Попытки НСД
- Системные сбои
- Ненадлежащее использование ресурсов
- Нарушение правил политики ИБ
- Хищения (документов, носителей информации, СВТ)
- Раскрытие конфиденциальной информации

Global Trust Solutions

Категорирование и приоритезация инцидентов ИБ

- **Категории инцидента** по величине ущерба: Высокая, Средняя, Низкая
- **Последствия инцидента**: нарушение конфиденциальности, целосности или доступности информации, отказ от авторства электронного документа
- **Виды ущерба**: Прямой финансовый ущерб, ущерб коммерческим интересам, репутационной, штрафные санкции, дезорганизация деятельности

Global Trust Solutions

Расстановка акцентов при управлении инцидентами ИБ

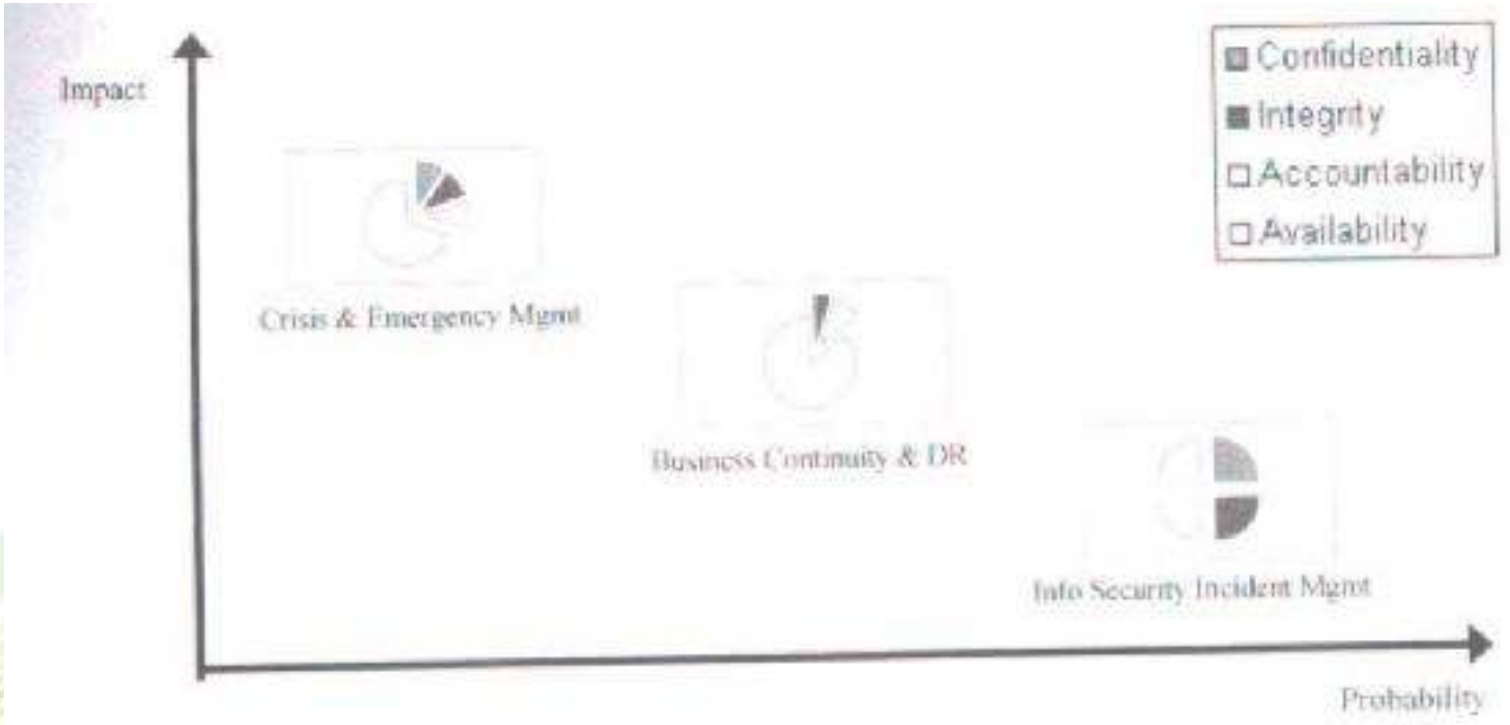
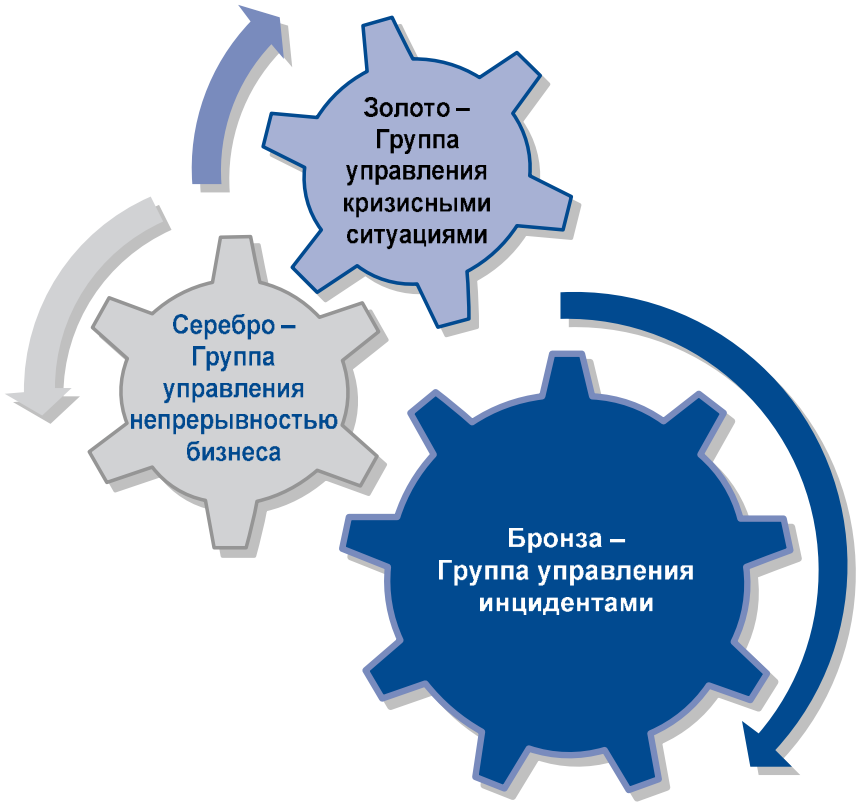


Figure 1 – Importance given to information security components for incident types handled by different management disciplines

Global Trust Solutions

Структура управления инцидентами (PAS 77:2006)

- **Золото** - топ-менеджмент организации, с привлечением МЧС, МВД, МО, аварийные службы и органы власти
- **Серебро** – служба управления рисками и непрерывностью бизнеса
- **Бронза** – ИТ и ИБ-подразделения, с привлечением кадров, юристов, физической безопасности и правоохранительных органов



Global Trust Solutions

Источники сообщений об инцидентах

- Пользователи и администраторы
- Клиенты и контрагенты
- IDS, SIEM и DLP-системы
- Системы мониторинга действий пользователей
- Системы контроля целостности
- Системы управления изменениями
- Антивирусные системы
- Анализ журналов аудита событий
- Аудит ИБ
- Антифрод-системы
- Системы мониторинга финансовых транзакций
- Системы мониторина доступности (на базе snpm, icmp, ping и т.п.)

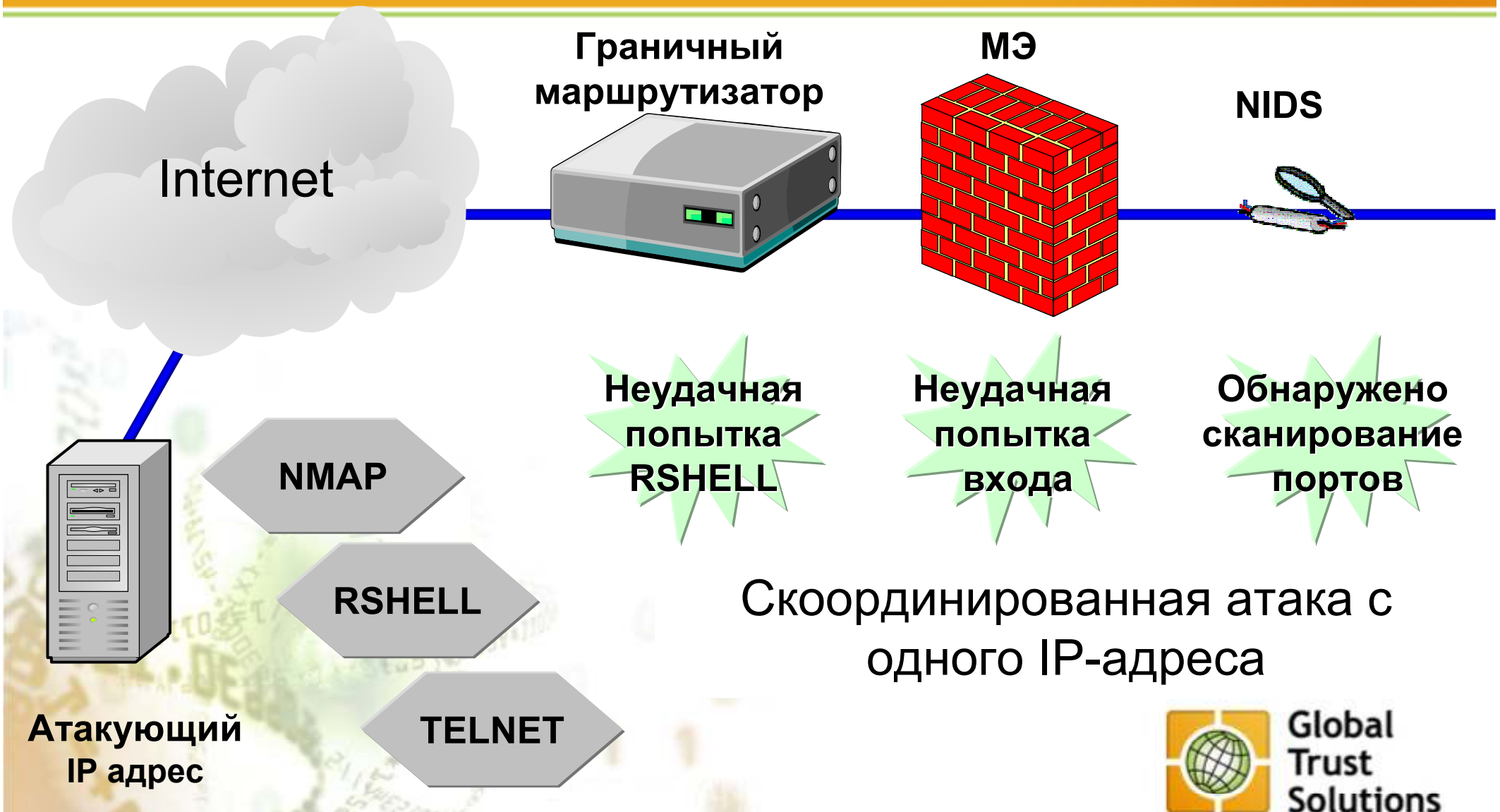
Global Trust Solutions

Признаки происходящего инцидента ИБ

- сбой WEB–сервиса, недоступность сайта
- пользователи сообщают о крайне низкой скорости работы сети, приложений, Интернет и т.п.
- администратор фиксирует наличие подозрительных файлов с нечитабельными названиями
- пользователи сообщают о наличие в своих почтовых ящиках множества повторяющихся сообщений
- записи в журналах аудита об изменении конфигурации ПО и оборудования
- приложение фиксирует в журнальном файле множественные неудачные попытки авторизации
- администратор сети фиксирует резкое увеличение сетевого трафика

Global Trust Solutions

Корреляция событий в реальном времени



Архитектура системы мониторинга событий безопасности

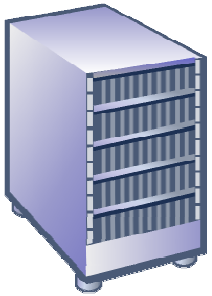
Агенты

Windows Agent

Unix Agent

iSeries Agent

Менеджеры



Central Computer

- Управление событиями
- Управление журналами
- Корреляция
- Анализ

Базы данных

Audit

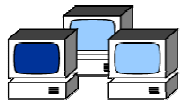
Summary

Log

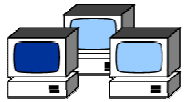
Configuration

OLAP Куб

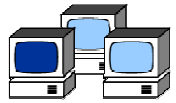
Интерфейсы



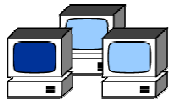
Monitor Console



Analysis Console



Dashboard



Web Console

Global Trust Solutions

Признаки будущих инцидентов ИБ

- журнальные файлы сервера или МЭ фиксируют сканирование портов
- объявление в СМИ о появлении нового вида вредоносного ПО или эксплойта
- поступает информация о возможном инциденте от эксперного сообщества, правоохранительных органов

Global Trust Solutions

Регистрация инцидентов ИБ

- описание характера инцидента и его последствий;
- место, дата и время возникновения;
- предпринятые меры по инциденту;
- описание последующих действий и текущий статус расследования;
- комментарии участников расследования;
- причины возникновения инцидента и результаты расследования, включая привлечение виновных к ответственности;
- перечень свидетельств (с обязательным указанием источников), собранных в ходе обработки инцидента;
- планировавшиеся и внедренные контрмеры, оценка результатов внедрения контрмер.

Global Trust Solutions

Анализ инцидента ИБ

- Факт попытки НСД
- Продолжается ли НСД в настоящий момент
- Кто является источником НСД
- Что является объектом НСД
- Когда происходила попытка НСД
- Как и при каких обстоятельствах была предпринята попытка НСД
- Точка входа нарушителя в систему
- Была ли попытка НСД успешной
- Определить системные ресурсы, безопасность которых была нарушена
- Какова мотивация попытки НСД (получение прибыли, саботаж, шпионаж, любопытство и т.д.)

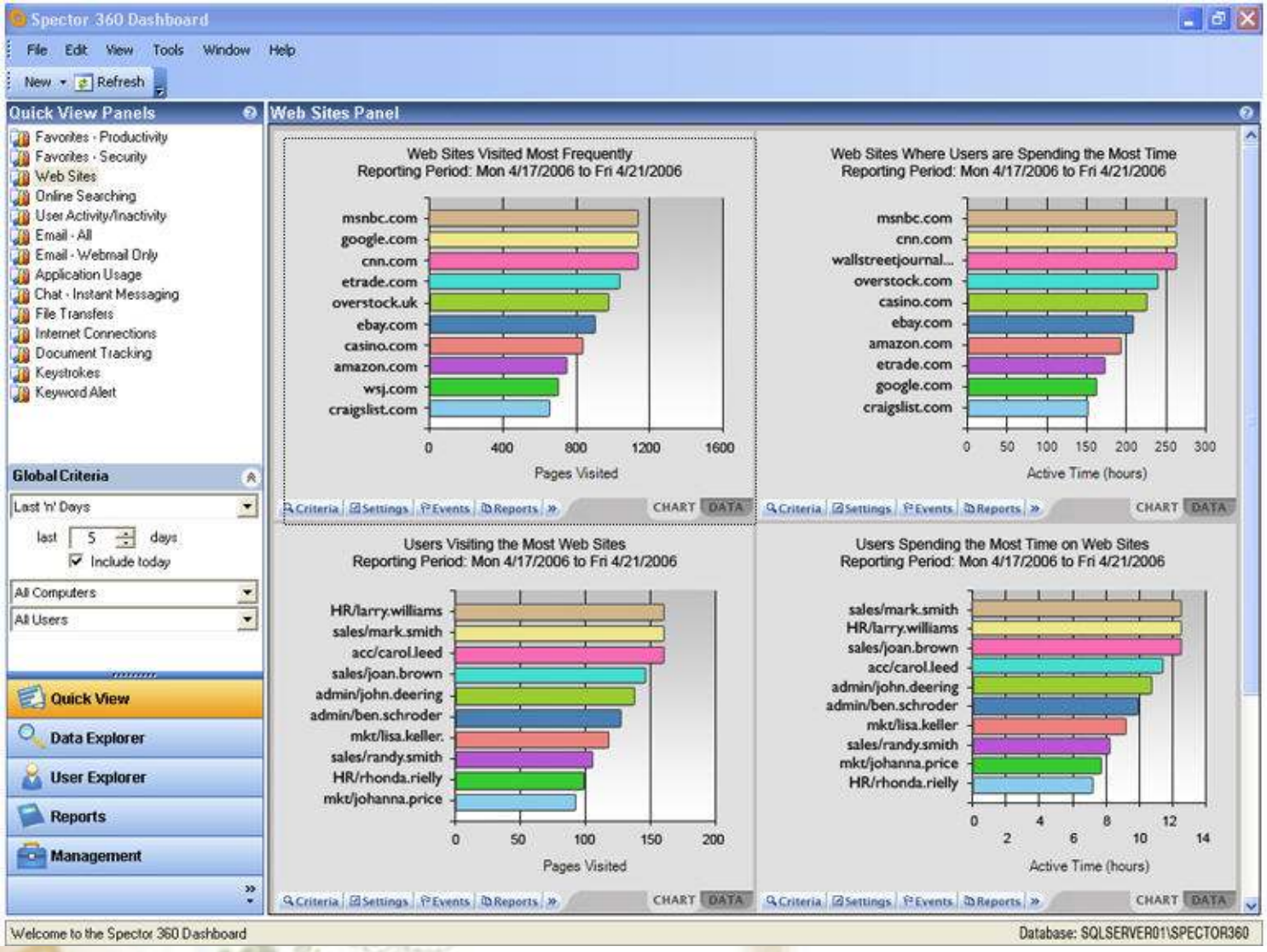
Global Trust Solutions

Технические мероприятия по расследованию инцидента

- Выявление активных пользователей
- Выявление подозрительных процессов
- Анализ системных журналов
- Анализ журналов сетевого оборудования
- Анализ конфигурации системного ПО, оборудования и сетевых адаптеров
- Поиск подозрительных файлов и других следов атаки (антивирусное сканирование, контроль целостности, контроль изменений)

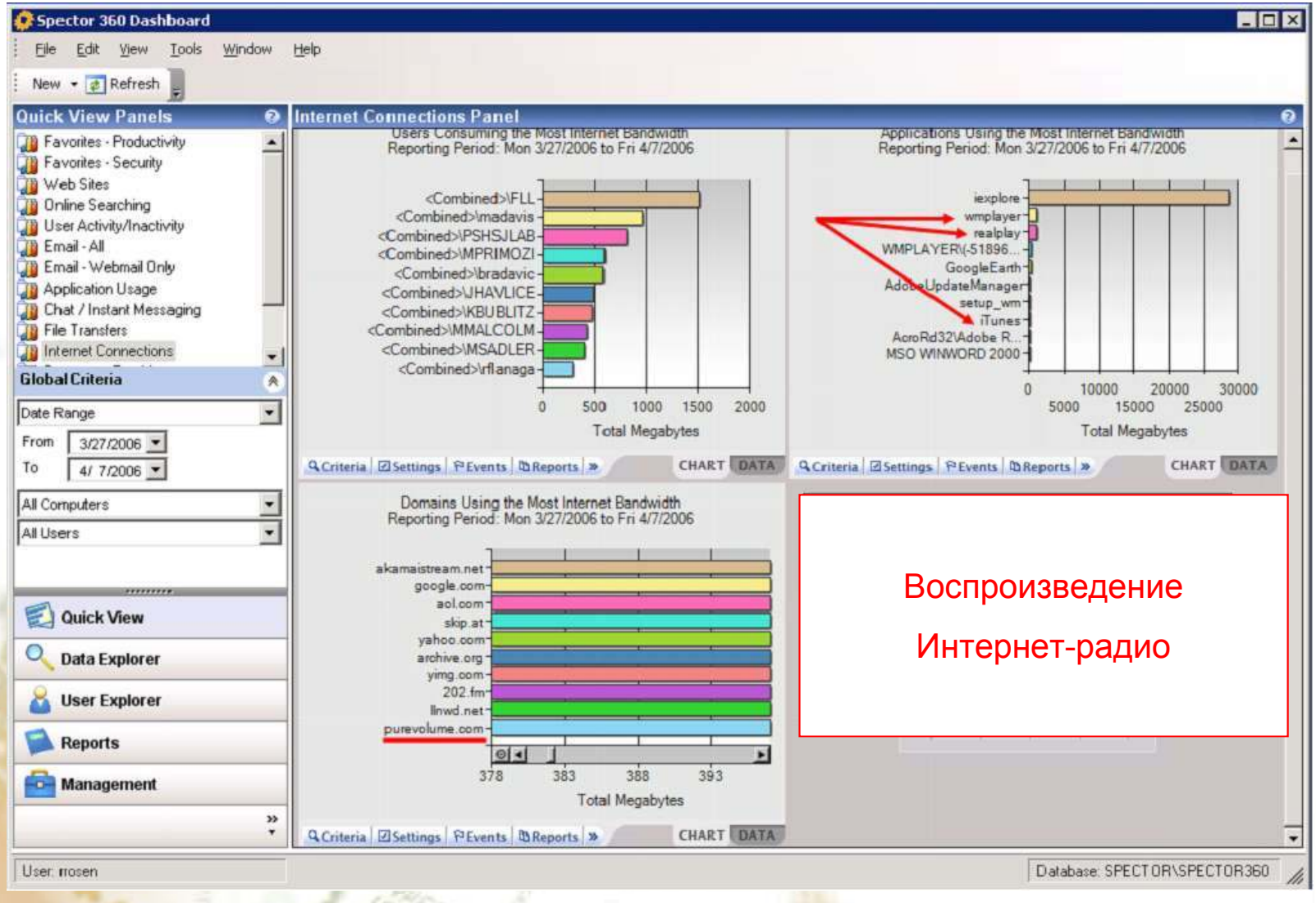
Global Trust Solutions

Анализ посещений веб-сайтов



Global Trust Solutions

Анализ сетевой активности пользователей



Воспроизведение

Интернет-радио

Global Trust Solutions

Ликвидация последствий инцидента

- Планирование восстановительных работ и распределение обязанностей
- Антивирусные мероприятия
- Восстановление данных с резервных копий
- Смена паролей на скомпроментированных системах
- Анализ выявленных уязвимостей и причин инцидента
- Ликвидация уязвимостей, установка программных коррекций
- Воспроизведение картины событий и документирование инцидента
- Подготовка свидетельств нарушения, привлечение правоохранительных органов

Global Trust Solutions

Incident Management Workflow

Регистрация и отчетность по инцидентам может быть реализована на базе:

- HelpDesk-систем
- GRC-систем
- Систем мониторинга ИБ (SIEM-системы, системы класса Security Manager)

Global Trust Solutions

Спасибо за внимание!

Global Trust Solutions

ООО «ГлобалТраст Солюшинс»

Продукты и услуги в области информационной безопасности

Астахов Александр Михайлович

генеральный директор

123317, Россия, Москва,
Пресненская наб., 10, блок С,
Бизнес-центр «Регус»
www.globaltrust.ru

Тел.: +7 (495) 651-66-17
Моб.: +7 (495) 991-80-37
Факс: +7 (495) 967-76-00
E-mail: AlexAstahov@globaltrust.ru