8-й Евразийский форум информационной безопасности

ИНФОФОРУМ ЕВРАЗИЯ // СИТИ

Москва, 7 июня 2012 года

Код безопасности

ГК «Информзащита»

Безопасность электронного бизнеса: от пользователя до виртуальной инфраструктуры

Емельянников Михаил Юрьевич

Управляющий партнер
Консалтинговое агентство «Емельянников, Попова и партнеры»

Дистанционное банковское обслуживание

Предоставление банковских услуг на основании распоряжения, передаваемого клиентом по каналам связи (без физического присутствия в банке) с использованием:

- компьютера (личного или находящегося в общем пользовании)
- планшета, коммуникатора, смартфона
- телефона (голосом, путем ввода данных по меню или передачи СМС сообщения)
- банкомата, терминала, инфомата

Очевидные проблемы

- Идентификация (взаимная!)
- Аутентификация (взаимная!)
- Авторизация
- Подтверждение подлинности действий клиента
- Защита от перехвата информации
- Противодействие навязыванию ложной информации (ложных запросов)

Объекты атаки

- Информационная система банка
- Канал связи
- Средства доступа пользователя:
  - контролируемое (банкомат, платежный терминал, инфомат)
  - неконтролируемое (принадлежащее пользователю)
  - доверенное устройство в недоверенной среде

Атака на систему ДБО в банке

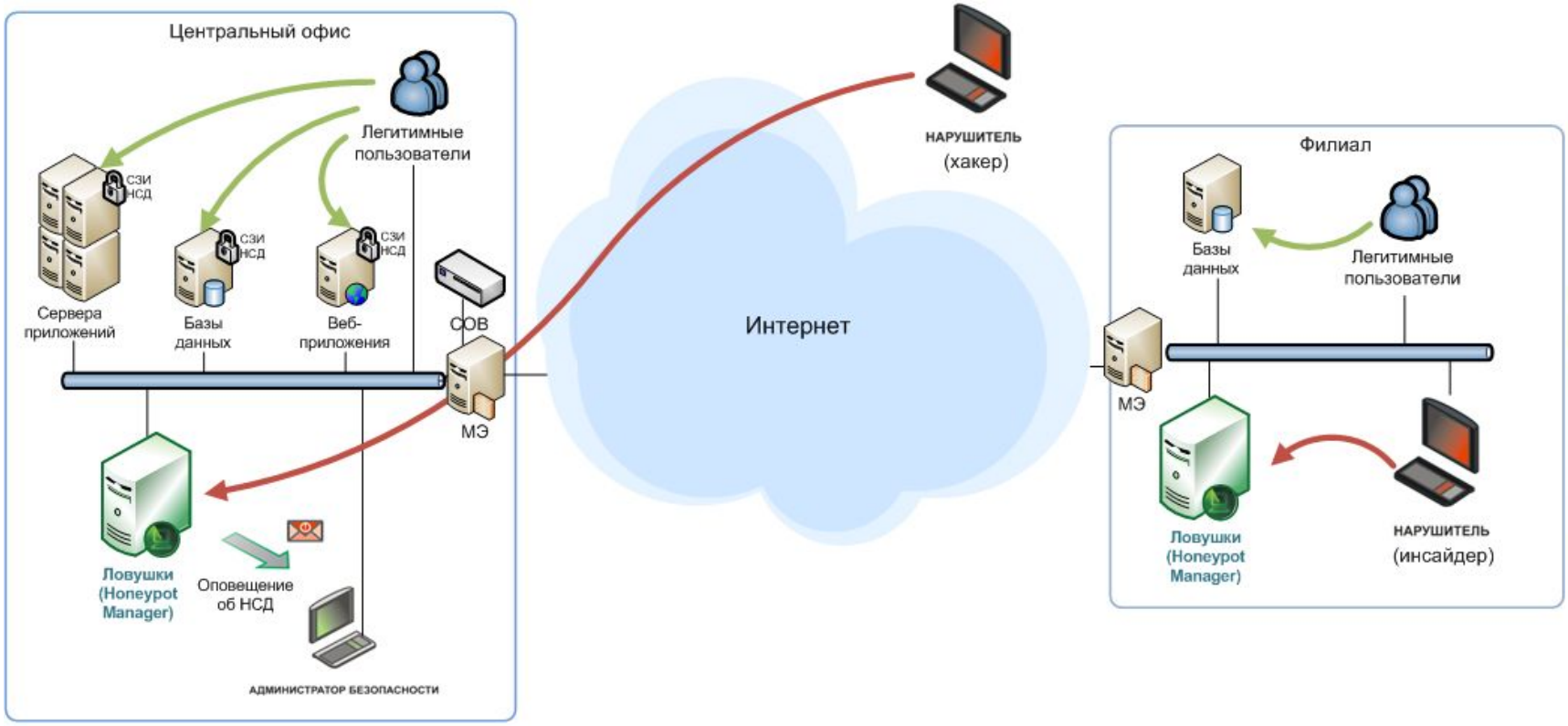
Снаружи
- атакуют от имени клиента
- преодолевают систему защиты

Изнутри
- обычный пользователь-нарушитель или в сговоре с ним
- привилегированный пользователь
- администратор

Нейтрализация внешних атак

- Межсетевое экранирование
- Системы обнаружения/ предупреждения вторжений
- Системы защиты от проникновения вредоносного контента
- Ловушки для нарушителей, использующих неизвестные способы и методы атак

Противодействие неизвестным атакам Security Studio Honeypot Manager



Код Безопасности

Ключевые возможности Security Studio Honeypot Manager

Проактивное средство обнаружения хакерских вторжений и НСД к информации

- Имитация работы бизнес-приложений
- Регистрация попыток НСД к информации
- Уведомление о фактах НСД
- Отчеты об активности нарушителей
- Централизованное управление

Достоинства систем данного класса

Security Studio Honeypot Manager

Проактивное средство обнаружения хакерских вторжений и НСД к информации

- Низкое количество ложных срабатываний
- Обнаружение атаки по небольшому количеству данных
- Обнаружение новых типов атак
- Возможность понять цели, методы и средства нарушителя
- Невысокие требования к обслуживанию

Уникальные особенности

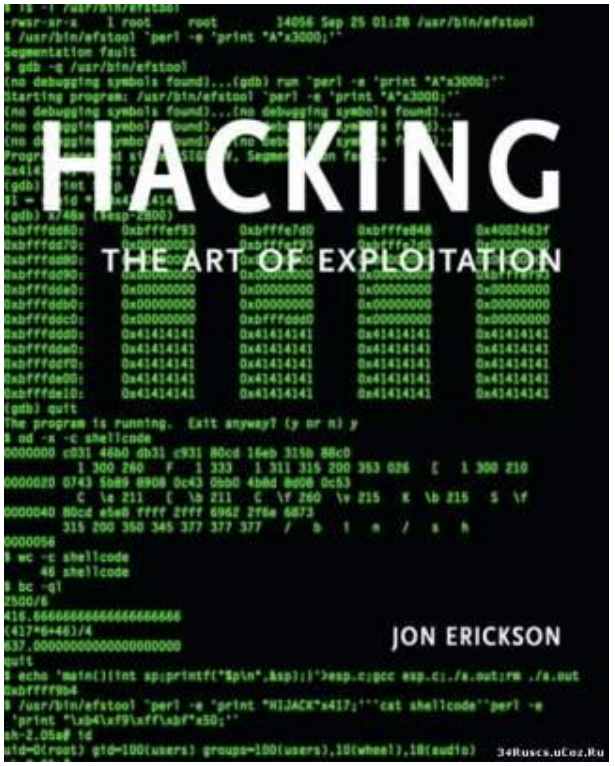
Security Studio Honeypot Manager

Проактивное средство обнаружения хакерских вторжений и НСД к информации

- Единственное СОВ на основе имитации данных
- Высокая реалистичность имитации
- Возможность оценить реальный уровень угроз и эффективность применения средств защиты
- Возможность интеграции с системой безопасности
- Наличие сертификата ФСТЭК (ТУ, НДВ-4, 1Г, К1)

Барьеры на пути нарушителя, проникшего в сеть

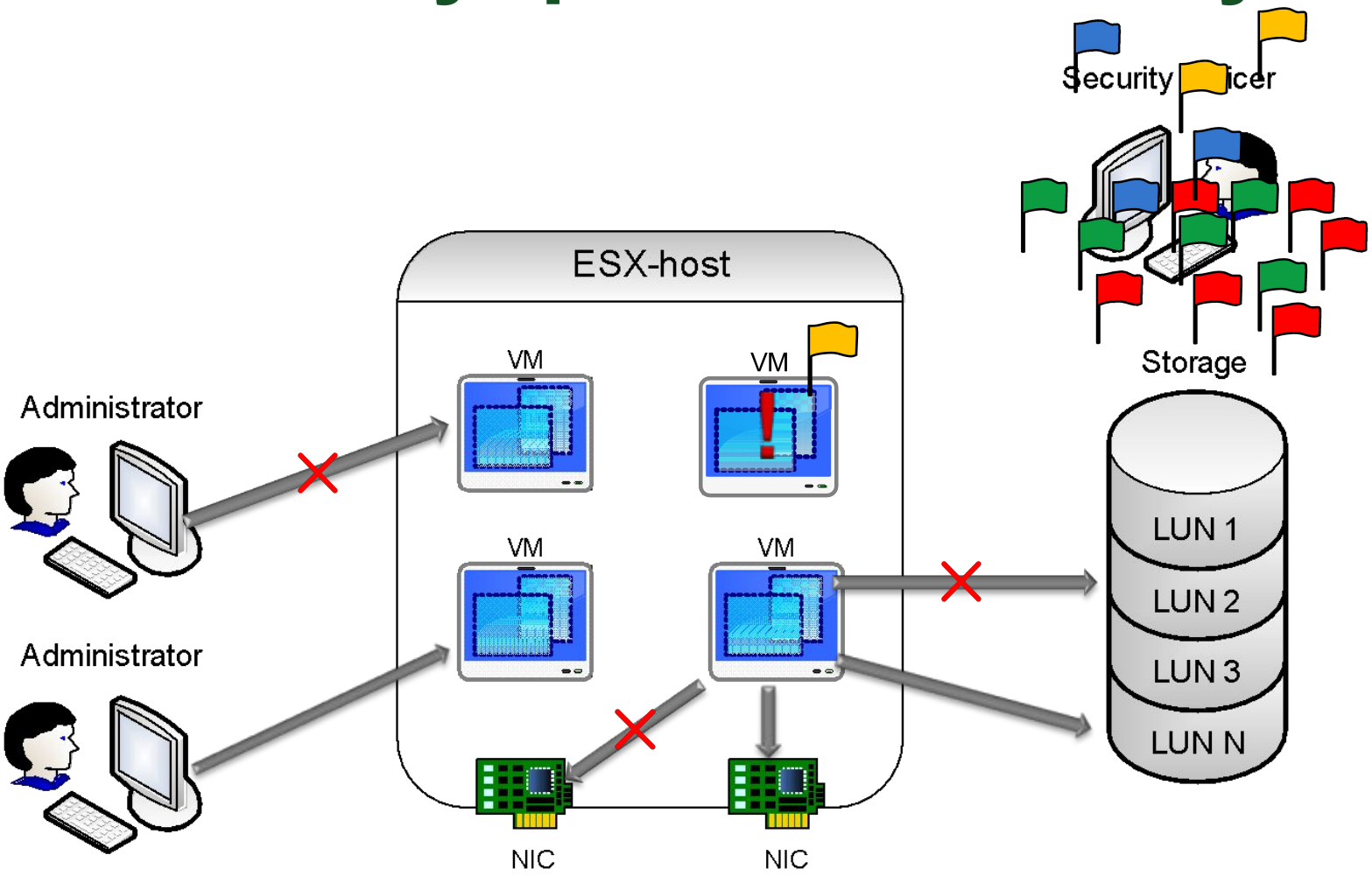
- Сегментация и изоляция
- Усиленная взаимная аутентификация пользователей и оборудования
- Мандатное управление доступом к защищаемым ресурсам
- Ограничение прав привилегированных и супер-пользователей



Безопасность виртуальной инфраструктуры – vGate R2/S-R2

- Усиленная аутентификация администраторов виртуальной инфраструктуры и администраторов информационной безопасности
- Защита средств управления виртуальной инфраструктурой и ESX-серверов от НСД
- Мандатное управление доступом
- Контроль целостности и доверенная загрузка ESX-серверов, а также виртуальных машин
- Контроль целостности и защита от НСД компонентов СЗИ
- Контроль доступа администраторов ВИ к данным виртуальных машин
- Регистрация событий, связанных с информационной безопасностью
- Централизованное управление и мониторинг

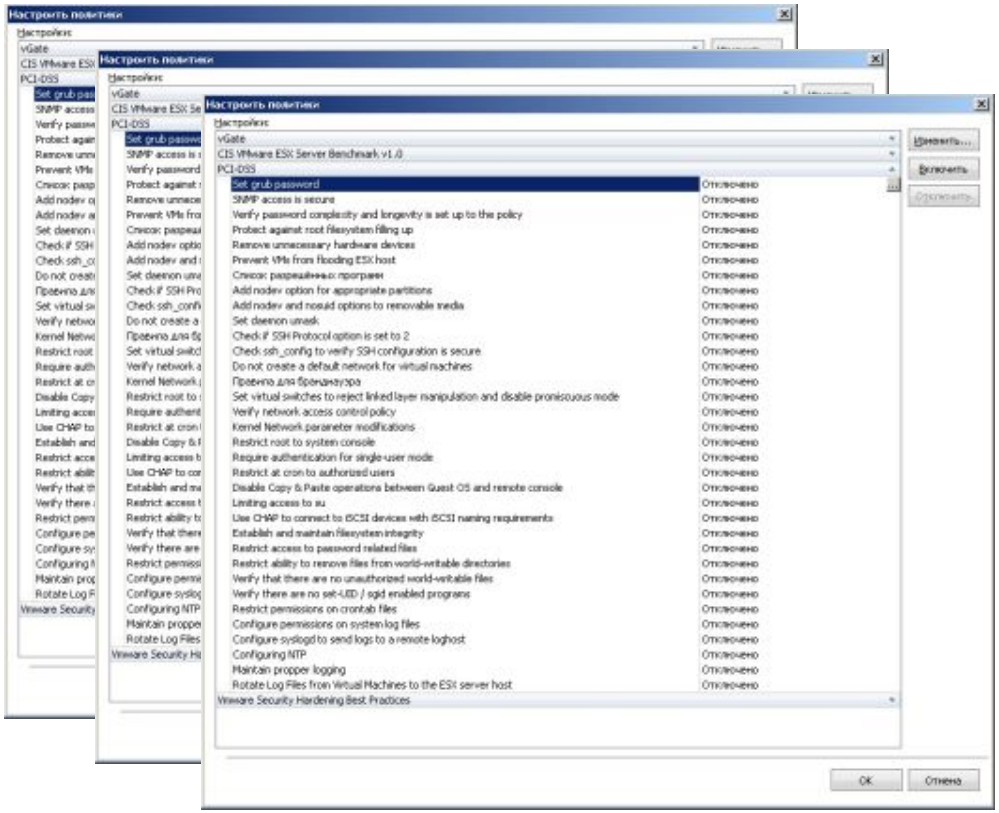
Мандатное управление доступом



Приведение в соответствие

Приведение инфраструктуры в соответствие с требованиями и постоянный контроль соответствия

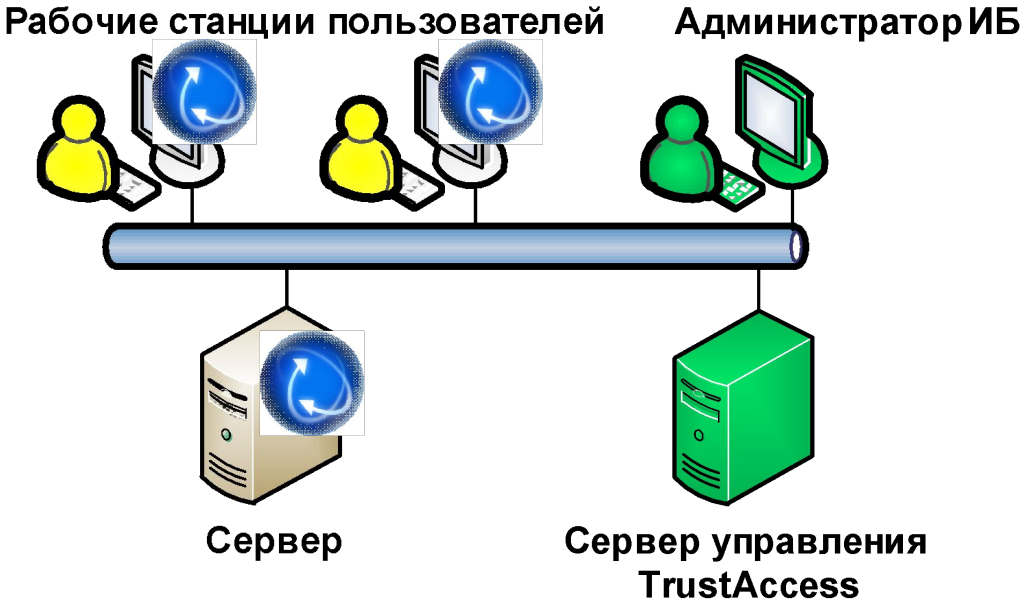
- VMware Security hardening Best Practice
- CIS VMware ESX Server 3.5 Benchmark
- **PCI DSS**
- **СТО БР ИББС**
- ФЗ-152



Код Безопасности
ГК «Информзащита»

Сегментация и изоляция – TrustAccess

Распределенный межсетевой экран с централизованным управлением - сертифицированная защита сетевого доступа к информационным системам



TrustAccess: основные функции

Защита виртуальных машин

Разграничение сетевого доступа

Аутентификация

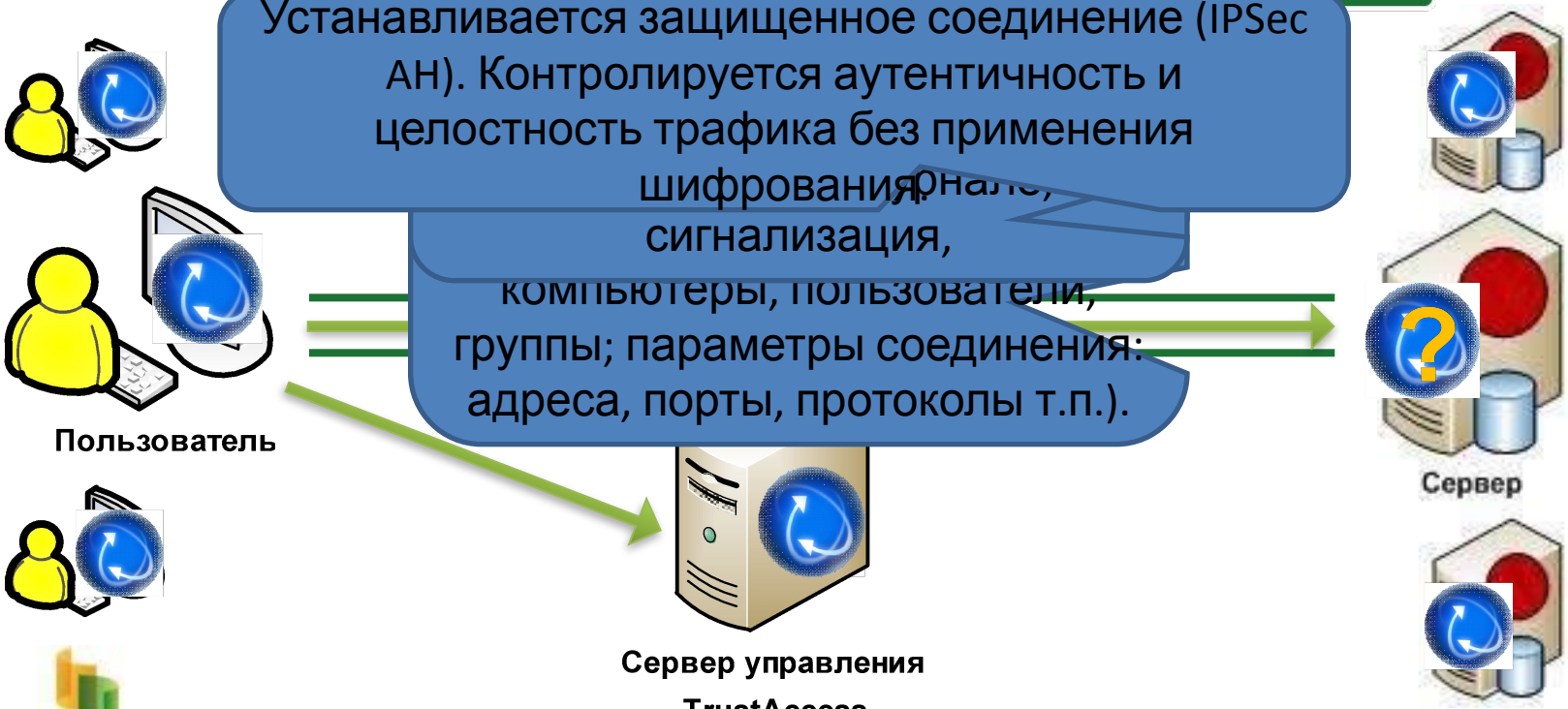
Авторизация (фильтрация соединений)

Установка защищенного соединения

Устанавливается защищенное соединение (IPSec AH). Контролируется аутентичность и целостность трафика без применения шифрования.

сигнализация,

компьютеры, пользователи, группы; параметры соединения: адреса, порты, протоколы т.п.).



Защита канала связи

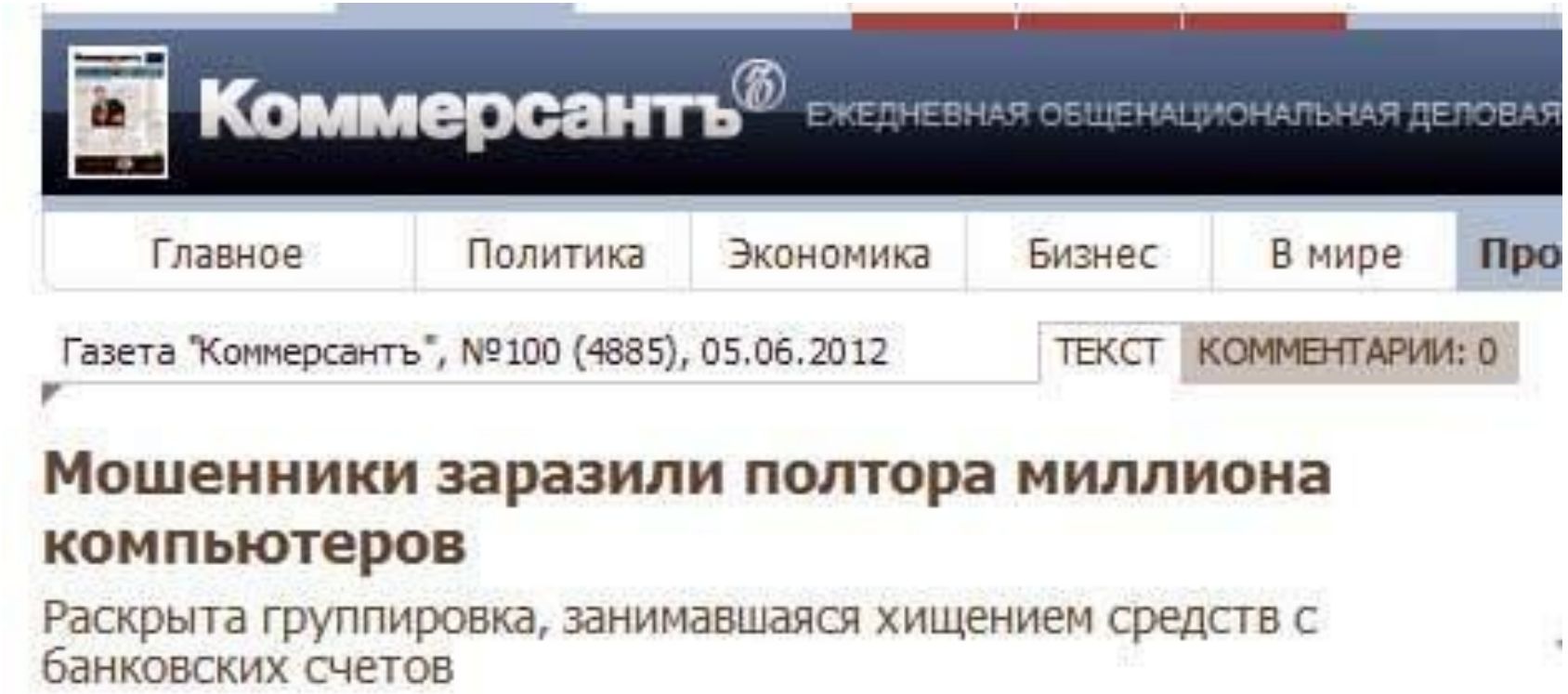
АПКШ «Континент» + Защищенный планшет **«Континент Т-10»** (OS Android) с интегрированными средствами безопасности.

Код Безопасности
ГК «Информзащита»

ДБО + BYOD

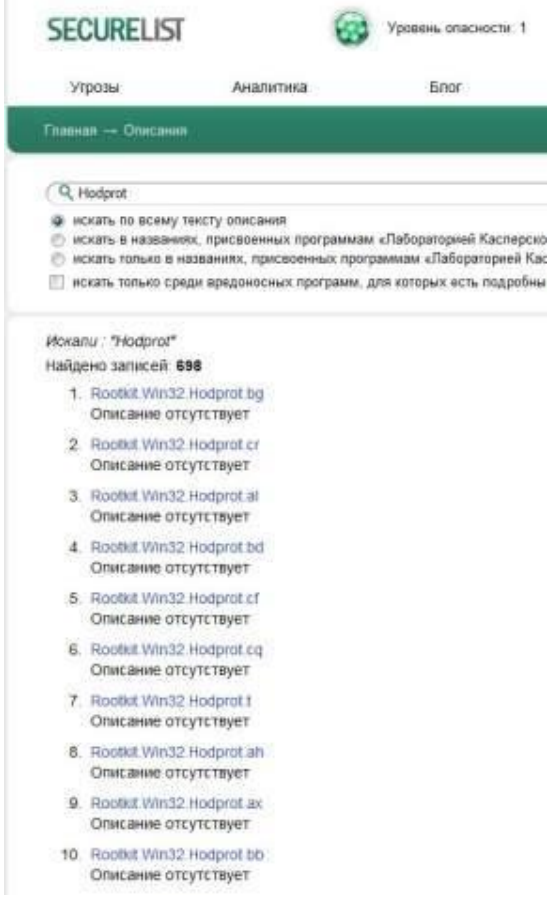
- СКЗИ Континент АП для iOS: программный VPN клиент для устройств iPad
- СКЗИ Континент АП для Android: программный VPN клиент для устройств смартфонов, планшетов и коммуникаторов

Все сложное – чаще всего просто



Группа молодых хакеров, используя сначала вредоносную программу **Hodprot**, а с 2011 года — **Carberp**, размещала их на различных сайтах для незаметного проникновения и установки в компьютерах пользователей. Всего были заражены минимум 1,6 млн. компьютеров.

Полтора миллиона клиентов банков не думали о безопасности. Своей.



Атаки на компьютер клиента – дешево, просто, сердито!

Компьютер клиента:

- Предотвращение НСД: пароль «123» (если есть вообще)
- Антивирус: Он же жутко тормозит!
- Персональный межсетевой экран: Чё?
- HIPS: Чё-чё???

Но и защита компьютера клиента – дешево, просто, сердито

Security Studio Endpoint Protection

Administration Center - централизованное развертывание и обновления Security Studio Endpoint Protection и контроль за безопасностью сети

Персональный межсетевой экран

Антивирус и антишпион

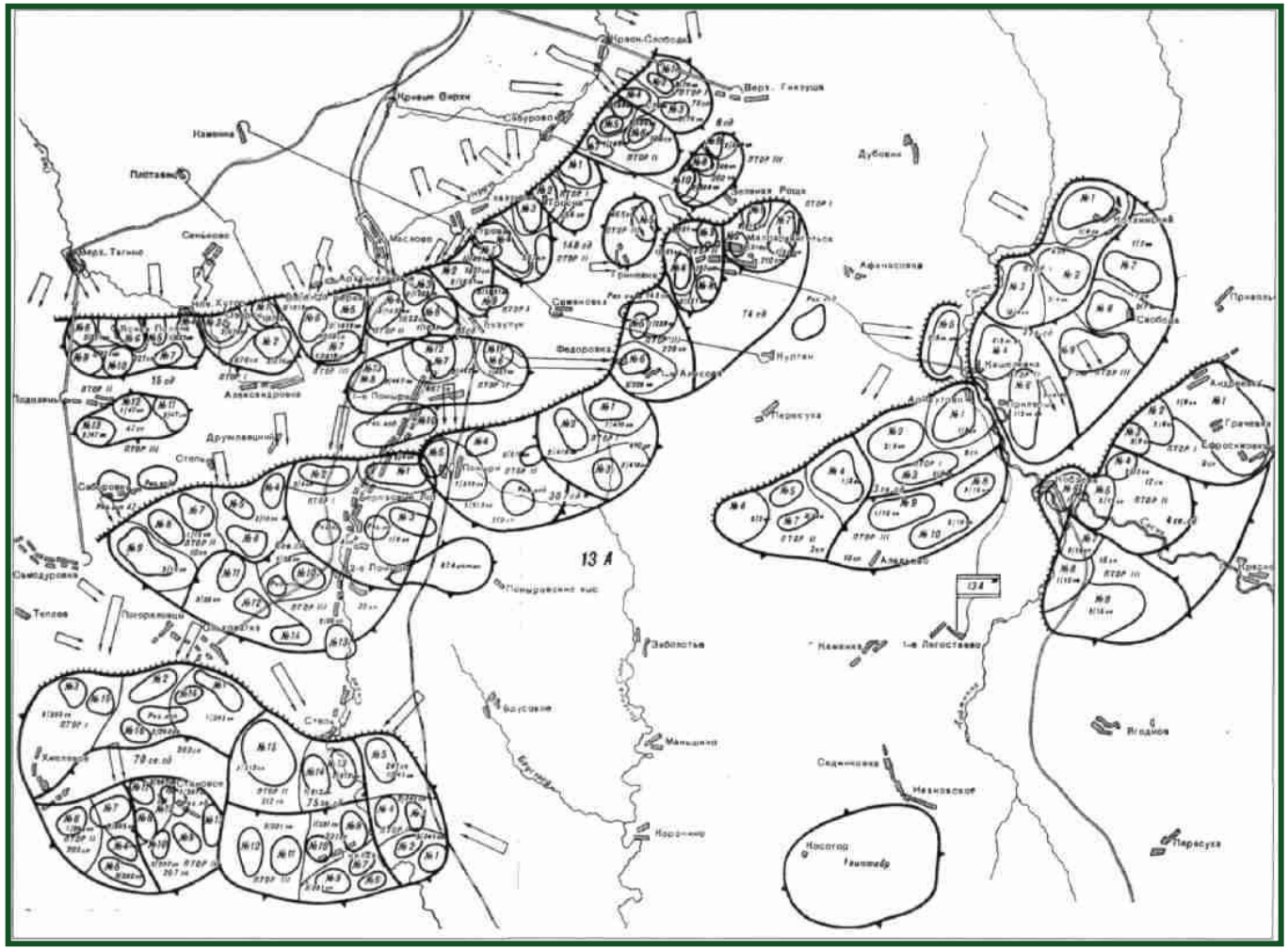
Средство обнаружения вторжений (Модули "Детектор атак" и "Локальная безопасность»)

Веб-контроль за работой интерактивных элементов, встроенных в загружаемые веб-страницы

Антиспам

Код Безопасности
ГК «Информзащита»

Универсальных таблеток нет. Но есть эшелонированная оборона



СПАСИБО ЗА ВНИМАНИЕ!
ВОПРОСЫ?

М.Ю.Емельянников

+7 (916) 659-3474

m.eme@mail.ru

Управляющий партнер

Консалтинговое агентство
«Емельянников, Попова и партнеры»

Компания «Код Безопасности»

+7 (495) 980-2345

info@securitycode.ru

www.securitycode.ru

Код Безопасности
ГК «Информзащита»