СЕМИНАР «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ 2010: РАБОТА НА ОПЕРЕЖЕНИЕ»

7 АПРЕЛЯ 2010, МОСКВА, HOLIDAY INN SUSCHEVSKY

Код Безопасности
ГК «Информзащита»

Информационная безопасность виртуальных инфраструктур. Наш ответ на новые вызовы

КОНСТАНТИН ПИЧУГОВ

Менеджер по развитию продуктов

Виртуализация в России и мире
Немного статистики и прогнозов

Код Безопасности
ГК «Информзащита»

Виртуализация в России и мире

Результаты опроса Garther **“Top 10 Technology Priorities in 2010”**:

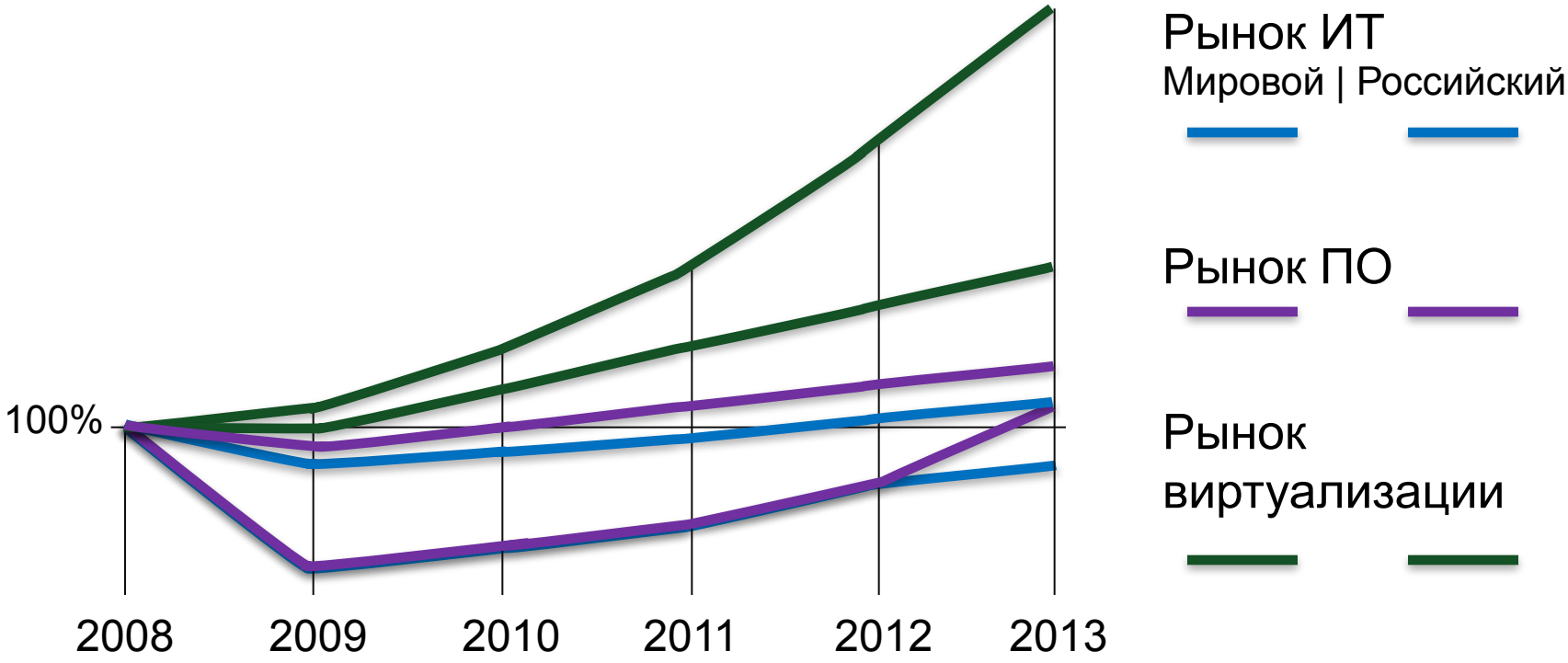
1. Virtualization
2. Cloud computing
3. Web 2.0
4. Networking, voice and data communications
5. Business Intelligence
6. Mobile technologies
7. Data/document management and storage
8. Service-oriented applications and architecture
9. Security technologies
10. IT management

Источник: Gartner, 2009

Код Безопасности
ГК «Информзащита»

Виртуализация в России и мире

Развития рынков информационных технологий с учетом кризиса

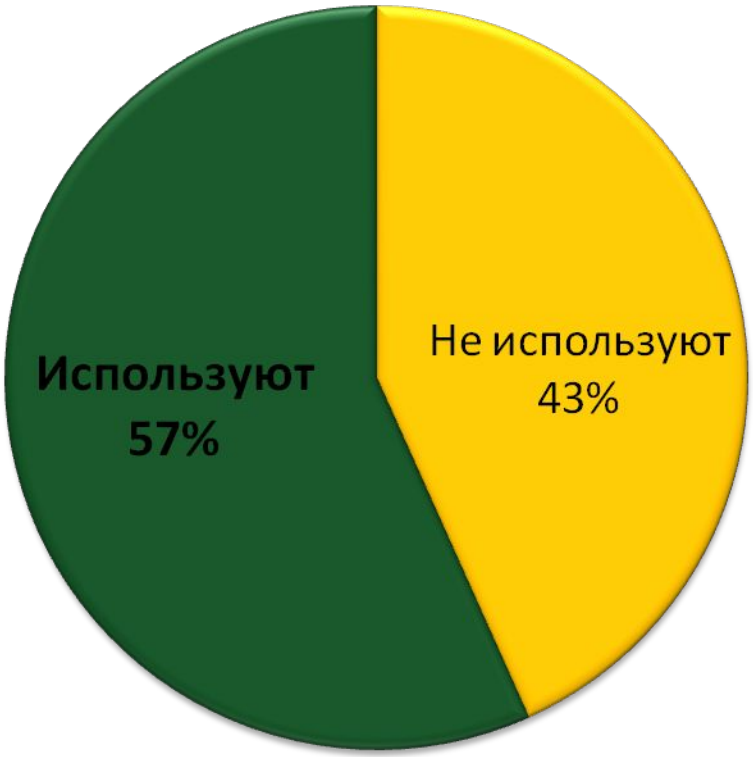


Источник: IDC, октябрь 2009

Код Безопасности
ГК «Информзащита»

Виртуализация в России

Использование технологий виртуализации в российском бизнесе 2009



Источник: CNews Analytics, 2009

Код Безопасности
ГК «Информзащита»

Виртуализация в России

Источник: CNews Analytics, 2009

Код Безопасности
ГК «Информзащита»

Виртуализация в России

Источник: CNews Analytics, 2009

Код Безопасности
ГК «Информзащита»

Виртуализация в России

Источник: CNews Analytics, 2009

Код Безопасности
ГК «Информзащита»

Виртуализация
Вопросы безопасности

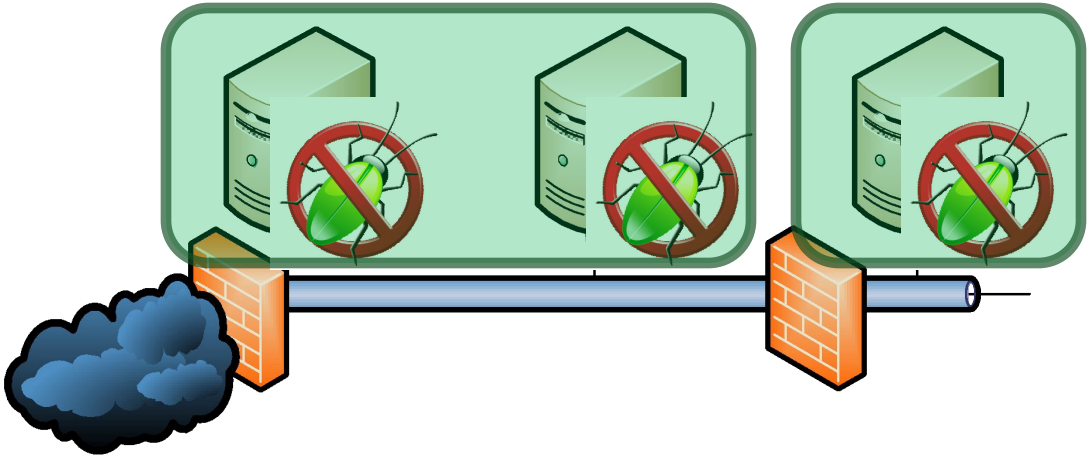
Код Безопасности
ГК «Информзащита»

ИБ виртуализации. Постулаты

- Виртуальные машины подвержены тем же угрозам безопасности, что и реальные компьютеры.
- Виртуализация дает весьма эффективные методы борьбы с некоторыми видами угроз (например, Sandboxing).
- Но и приносит новые угрозы и проблемы безопасности…

Код Безопасности
ГК «Информзащита»

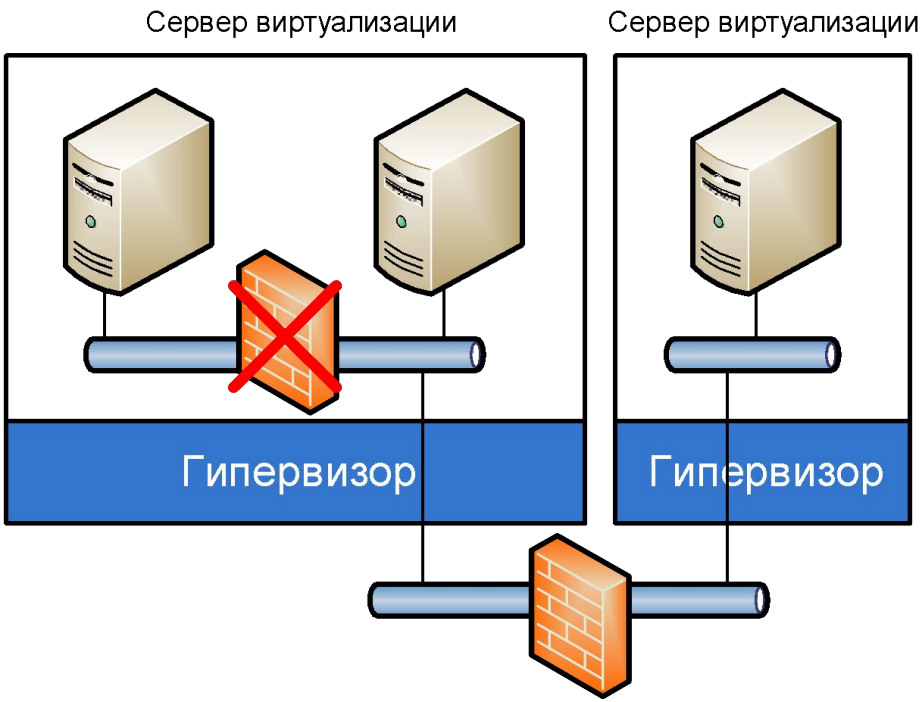
Традиционные средства защиты в физической инфраструктуре



- Управление доступом
- Firewall, VPN
- Криптография
- Антивирусы
- IDS/IPS
- Другие средства защиты

Код Безопасности
ГК «Информзащита»

Виртуализация меняет свойства сетей



- Часть физической локальной сети виртуализируется
- Межсетевые экраны становятся не везде применимы

Код Безопасности
ГК «Информзащита»

Гипервизор — отдельный слой

- Гипервизор управляет основными ресурсами
- Гипервизор играет роль «человек в середине»

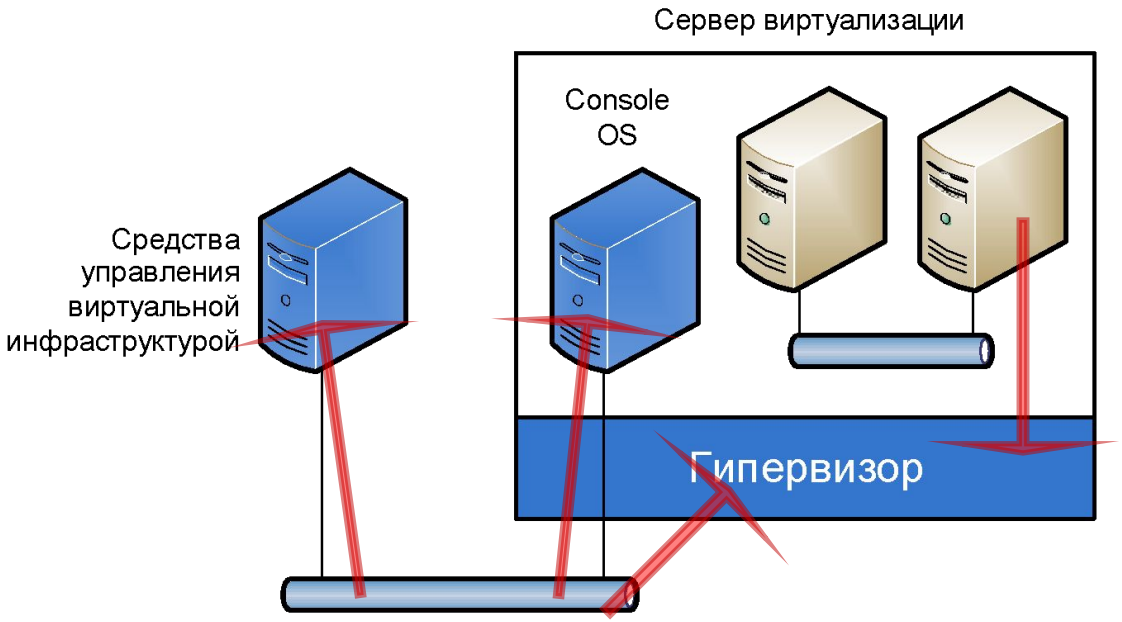
Код Безопасности
ГК «Информзащита»

Гипервизор и данные виртуальных машин

- Гипервизор может читать и изменять данные виртуальных машин, когда они не работают

Код Безопасности
ГК «Информзащита»

Варианты атаки на гипервизор



- Есть множество вариантов НСД к гипервизору через различные элементы виртуальной инфраструктуры

Код Безопасности
ГК «Информзащита»

Традиционные средства защиты в виртуальной среде подвержены компрометации

Если:

- Чувствительны к угрозам **Man in The Middle** (LAN, RAM, HDD, другой ввод/вывод).
- Чувствительны к **несанкционированному изменению данных** в то время, когда виртуальная машина **выключена**.

Код Безопасности
ГК «Информзащита»

Аппаратные средства защиты в виртуальной среде

В виртуальной среде не всегда возможно применять аппаратные средства защиты.

- Не работают традиционные средства доверенной загрузки.
- Во многих случаях аппаратное средство нельзя «пробросить» в виртуальную машину.

Код Безопасности
ГК «Информзащита»

Каким путем пойти?

Использовать только специализированные нечувствительные к угрозам виртуализации средства защиты

Использовать традиционные средства

+

специализированное решение, закрывающее угрозы виртуализации

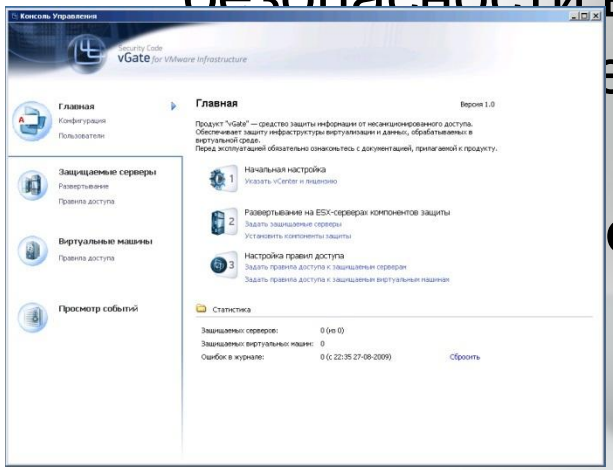
Код Безопасности
ГК «Информзащита»

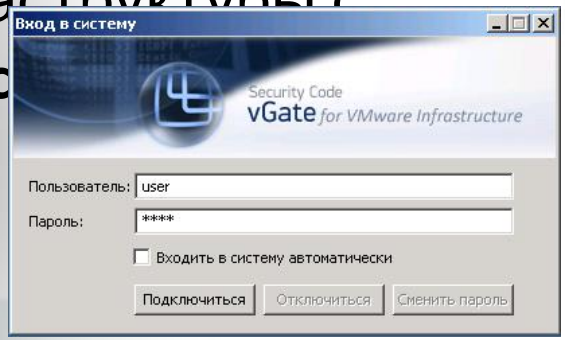
Security Code vGate

for VMware Infrastructure

- Компания «Код Безопасности» представляет новый программный продукт для защиты виртуализации.
- vGate предназначен для обеспечения безопасности виртуальной инфраструктуры с ем **VMware Infrastruc**

ФСТЭК.





Код Безопасности
ГК «Информзащита»

Security Code **vGate**

for VMware Infrastructure

- vGate — первое на рынке России **специализированное** для виртуализации **сертифицированное средство защиты от несанкционированного доступа**.
- Применение vGate дает возможность легитимного использования в виртуальных средах информационных систем, обрабатывающих данные ограниченного доступа, и помогает провести аттестацию таких систем.

Код Безопасности
ГК «Информзащита»

Security Code **vGate**

for VMware Infrastructure

Основные функции:

- Аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности.
- Защита средств управления виртуальной инфраструктурой от несанкционированного доступа.
- Контроль целостности конфигурации виртуальных машин и доверенная загрузка.
- Дискреционный механизм разграничения прав ESX-хостов на исполнение виртуальных машин.
- Регистрация событий, связанных с информационной безопасностью.
- Централизованное управление и мониторинг.

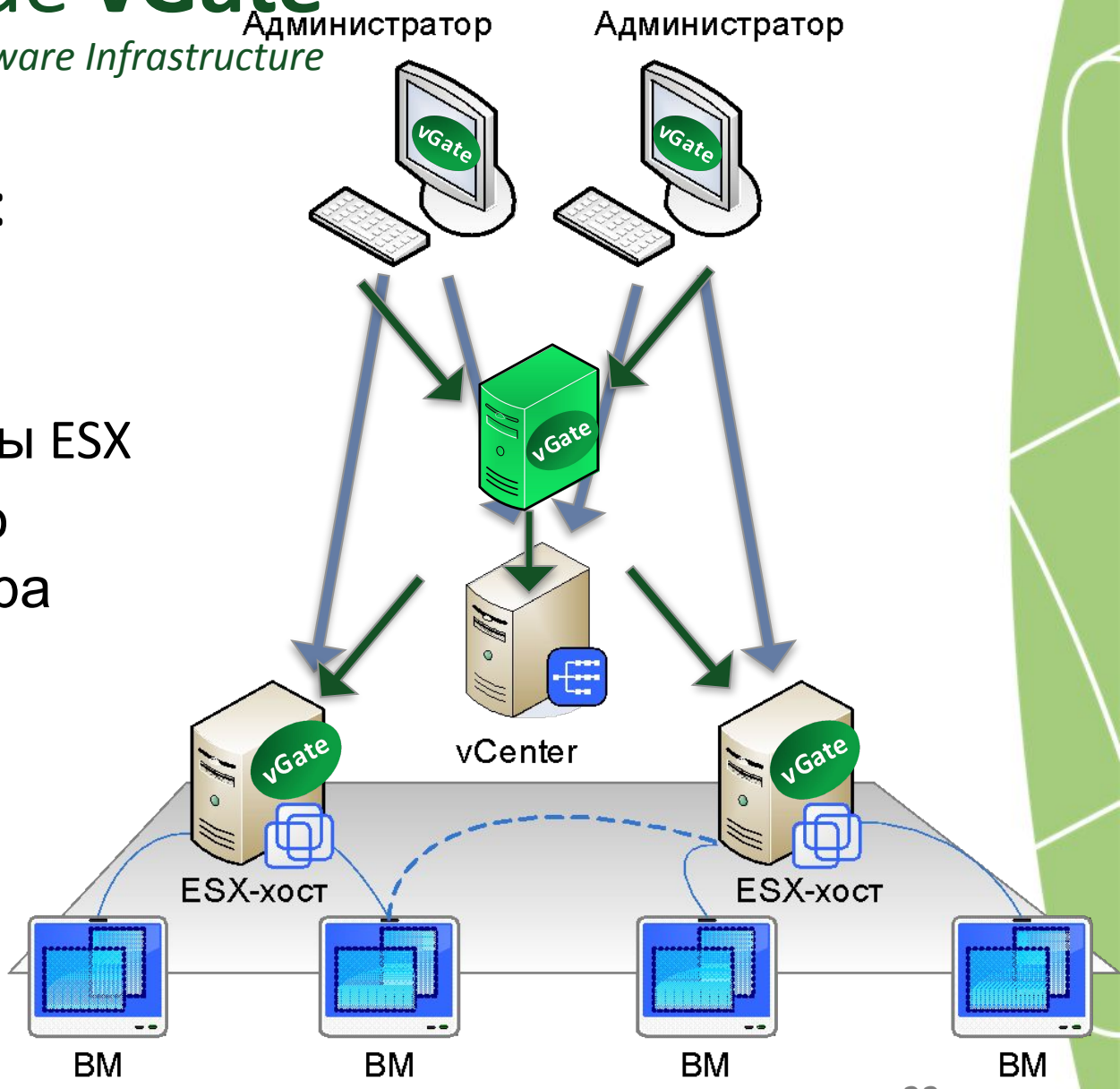
Код Безопасности
ГК «Информзащита»

Security Code **vGate**

for VMware Infrastructure

В СЗИ входят:

- Сервер авторизации
- Модули защиты ESX
- Рабочее место администратора
- Консоль управления



Код Безопасности
ГК «Информзащита»

Security Code **vGate**

for VMware Infrastructure

Лицензирование:

- Право на использование Сервера авторизации vGate
- Право на использование vGate для защиты ESX-хостов

Код Безопасности
ГК «Информзащита»

Security Code **vGate**

for VMware Infrastructure

Уровень сертификации vGate 1.0:

- Сертификация во ФСТЭК по уровню **СВТ 5** и **НДВ 4**
  - дает возможность использовать продукт для защиты автоматизированных систем (**АС**) до класса **1Г** включительно
  - и информационных систем персональных данных (**ИСПДн**) до класса **К1** включительно.

Уровень сертификации vGate 2.0:

- Сертификация во ФСТЭК по уровню **СВТ 3** и **НДВ 2**
  - даст возможность использовать продукт для защиты **АС** до класса **1Б** включительно.

Код Безопасности
ГК «Информзащита»

Security Code **vGate**

for VMware Infrastructure

Подробнее о vGate:

- http://www.securitycode.ru/products/sn_vmware/
- k.pichugov@securitycode.ru

Предоставляем демо-версию vGate:

- http://www.securitycode.ru/products/demo/

Код Безопасности
ГК «Информзащита»

СПАСИБО ЗА ВНИМАНИЕ! ВОПРОСЫ?

КОНСТАНТИН ПИЧУГОВ

Менеджер по развитию продуктов

- +7 (495) 980-2345 (многоканальный)
- k.pichugov@securitycode.ru
- www.securitycode.ru

Код Безопасности
ГК «Информзащита»