Компьютерные преступления в финансовом секторе

Group-IB

Этапы развития

Российский лидер в сфере РКП
Первая и единственная компания в СНГ, предоставляющая весь спектр услуг в области расследования инцидентов ИБ.

Комплекс услуг
Прединцидентный консалтинг;
Реагирование;
Криминалистика;
Расследование;
Юридическое сопровождение;
Постинцидентный консалтинг.

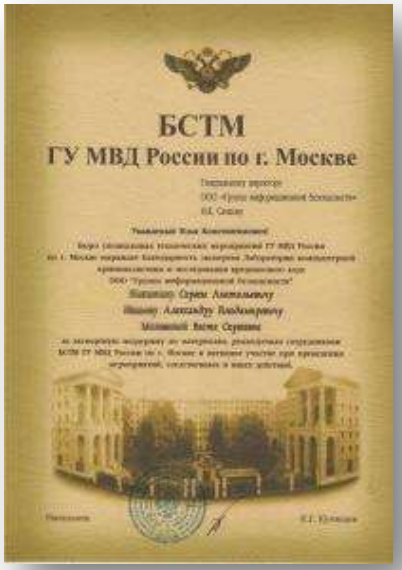
Резидент Сколково
Проект — комплексная система противодействия киберпреступности CyberCop.

Первый 24/7 CERT в Восточной Европе
CERT-GIB — первый частный круглосуточный центр реагирования на инциденты ИБ в России.

Group-IB: карта услуг

- Компьютерная криминалистика
- Исследования вредоносного кода
- Расследования инцидентов ИБ
- Защита бренда от интернет-угроз
- Защита от DDoS-атак
- Мониторинг бот-сетей
- Юридическое сопровождение
- Аудиты информационной безопасности

Наши награды



Киберпреступность

Рынок киберпреступности

Ежегодный отчет о российском рынке киберпреступности:

- ✓ финансовые показатели;
- ✓ анализ основных угроз и тенденций;
- ✓ обзор основных событий;
- ✓ прогнозы.

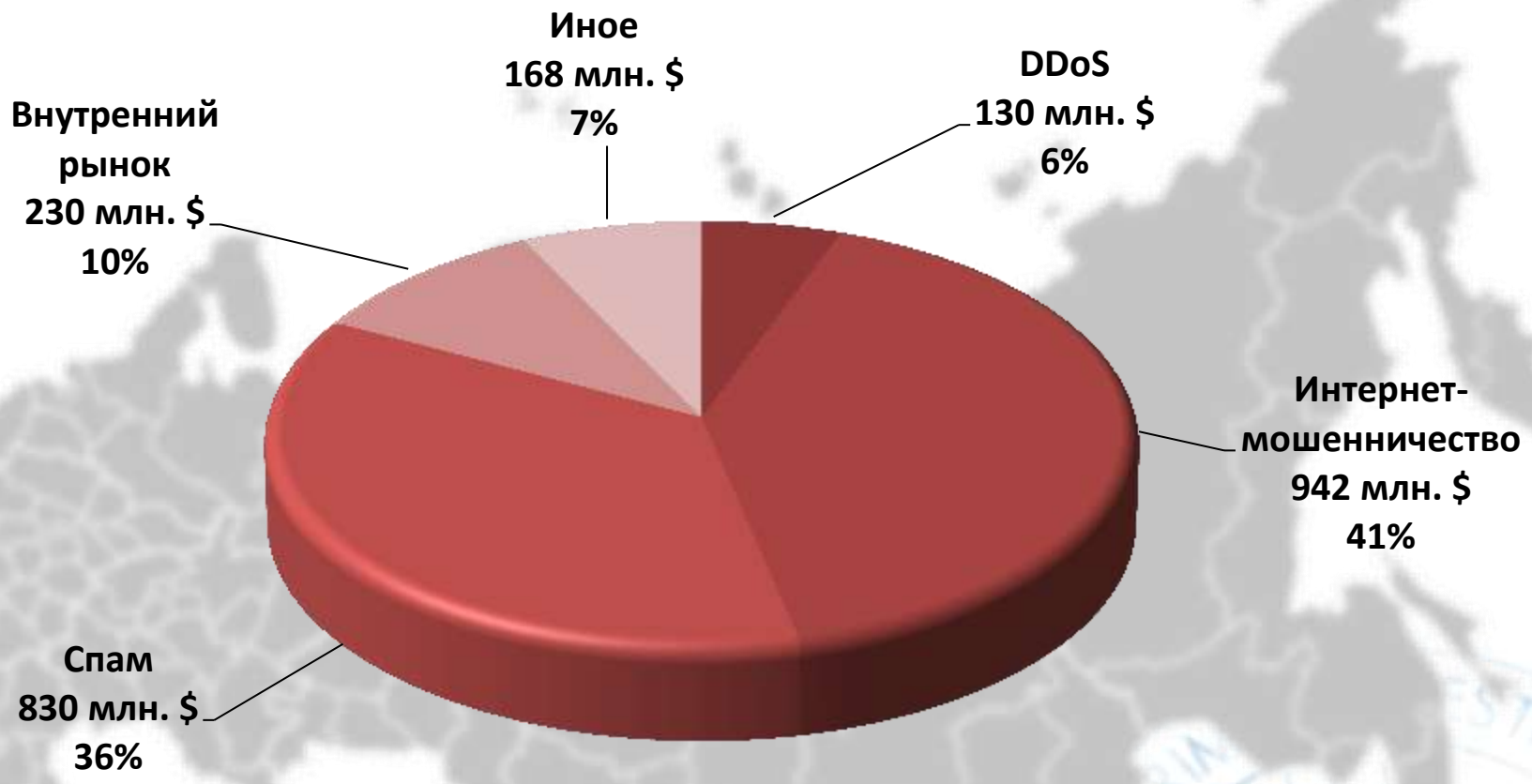
Рынок киберпреступности

Финансовые показатели*

Российский рынок	2,3 млрд. $
Русский рынок	4,5 млрд. $
Мировой рынок	12,5 млрд. $

* - отчет Group-IB “Русский рынок компьютерных преступлений. Состояние и тенденции.” 2011 г.

Киберпреступность в РФ



* - отчет Group-IB “Русский рынок компьютерных преступлений. Состояние и тенденции.” 2011 г.

Тенденции 2011

- ✓ Рост количества хищений
- ✓ Физические лица
- ✓ Удаленный доступ
- ✓ Автоподмена и автозалив
- ✓ Благотворительность
- ✓ Веб-инжекты
- ✓ Новые игроки

Тенденции 2012

- ✓ Снижение количества хищений до июня
- ✓ Общий рост количества хищений
- ✓ Работа со смарт-картами
- ✓ Атаки на мобильные платформы
- ✓ Автоподмена и автозалив
- ✓ Рост фишинга

Противодействие хищениям в ДБО

Группа Carberp

- ✓ В тесном сотрудничестве с **ФСБ** и **МВД России** при содействии **Сбербанка России** и **FOX-IT**
- ✓ Результат расследования – задержана преступная группа из 8 человек
- ✓ Первый в российской практике случай задержания всех фигурантов группы онлайн-мошенников

Группа Hodprot

- ✓ В тесном сотрудничестве с **ФСБ** и **МВД России** при содействии **Сбербанка России** и **ESET**
- ✓ Результат расследования – задержана преступная группа из 7 человек
- ✓ Мероприятия проводились в нескольких регионах России

Группа Гермеса

- ✓ В тесном сотрудничестве с **ФСБ** и **МВД России**
- ✓ Результат расследования – арестован организатор преступной группы
- ✓ Ликвидирована крупнейшая банковская бот-сеть России

Противодействие фишингу

Братья Попелыш

- ✓ Хищение **13 млн рублей**
- ✓ **Первое** уголовное дело по фишингу в России
- ✓ Результат – условные сроки и штрафы

CERT-GIB

CERT-GIB: Европа, Северная Америка, Азия

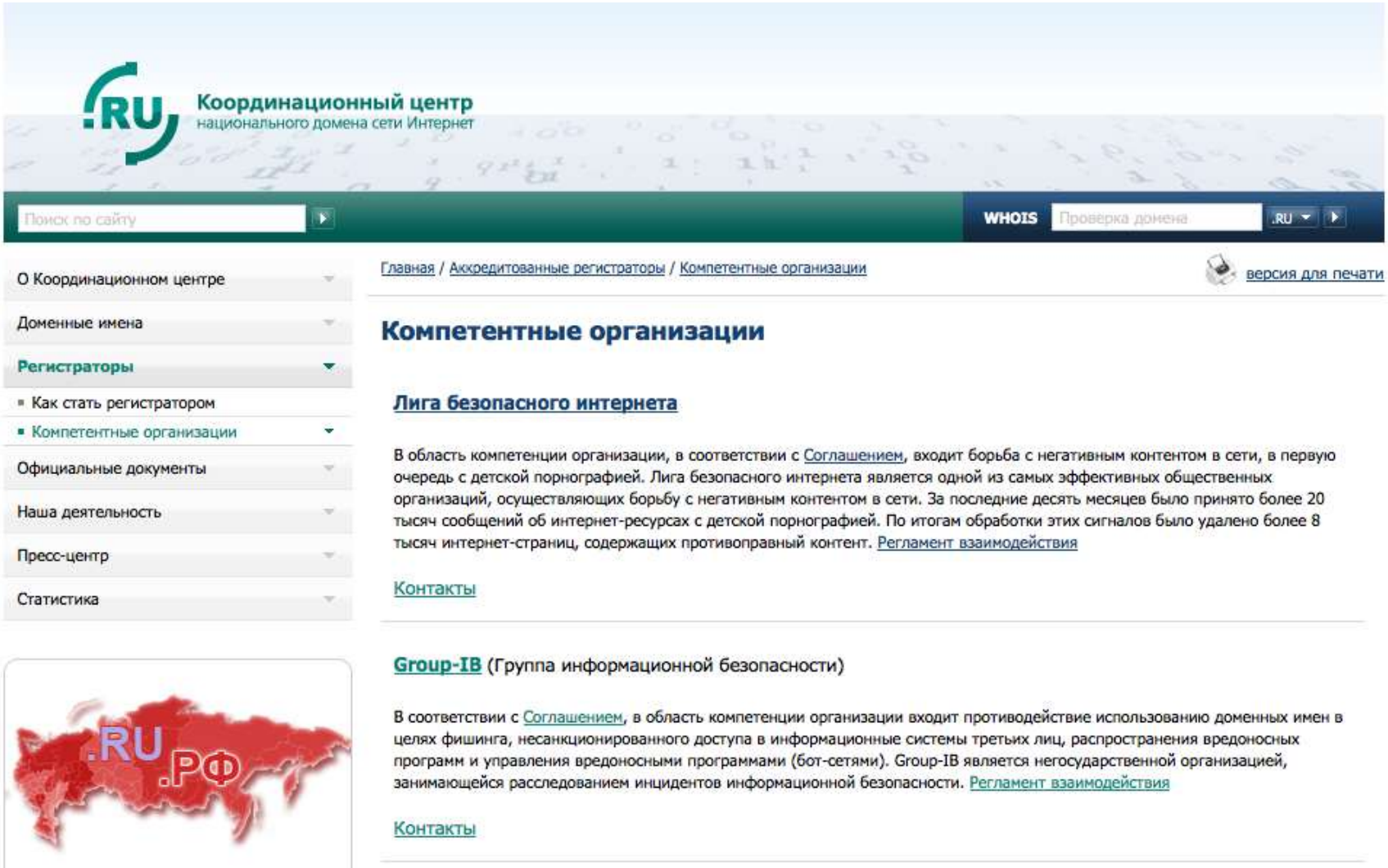
Первый 24/7 CERT в Восточной Европе
CERT-GIB первый в Восточной Европе круглосуточный центр реагирования на инциденты ИБ.

Трансконтинентальная поддержка
Группы мониторинга и реагирования присутствуют в разных частях земного шара: Европа ➔ Северная Америка ➔ Азия

Противодействие следующим типам угроз:
Фишинг, СПАМ, DDoS атаки, вредоносное ПО, бот-сети

.RU, .РФ, .SU: компетентная организация
Обладает официальным статусом КЦ РФ по противодействию киберугрозам в Рунете

Уникальные компетенции



Координационный центр национального домена сети Интернет

Поиск по сайту

WHOIS Проверка домена .RU

О Координационном центре
Доменные имена
Регистраторы
- Как стать регистратором
- Компетентные организации

Официальные документы
Наша деятельность
Пресс-центр
Статистика

Главная / Аккредитованные регистраторы / Компетентные организации

версия для печати

Компетентные организации

Лига безопасного интернета

В область компетенции организации, в соответствии с Соглашением, входит борьба с негативным контентом в сети, в первую очередь с детской порнографией. Лига безопасного интернета является одной из самых эффективных общественных организаций, осуществляющих борьбу с негативным контентом в сети. За последние десять месяцев было принято более 20 тысяч сообщений об интернет-ресурсах с детской порнографией. По итогам обработки этих сигналов было удалено более 8 тысяч интернет-страниц, содержащих противоправный контент. Регламент взаимодействия

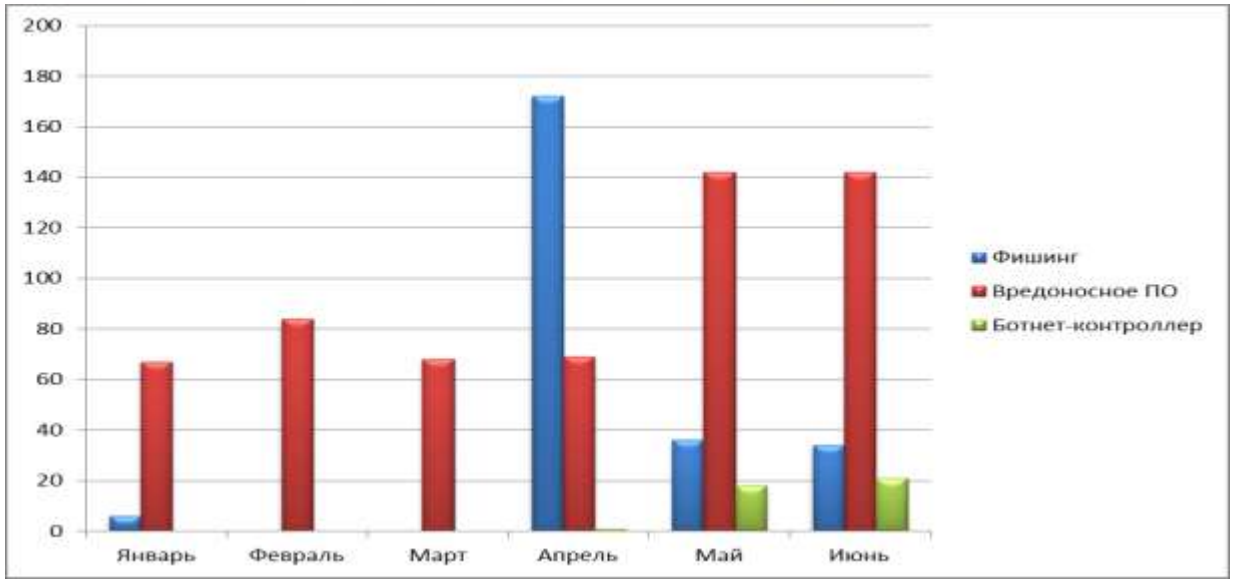
Контакты

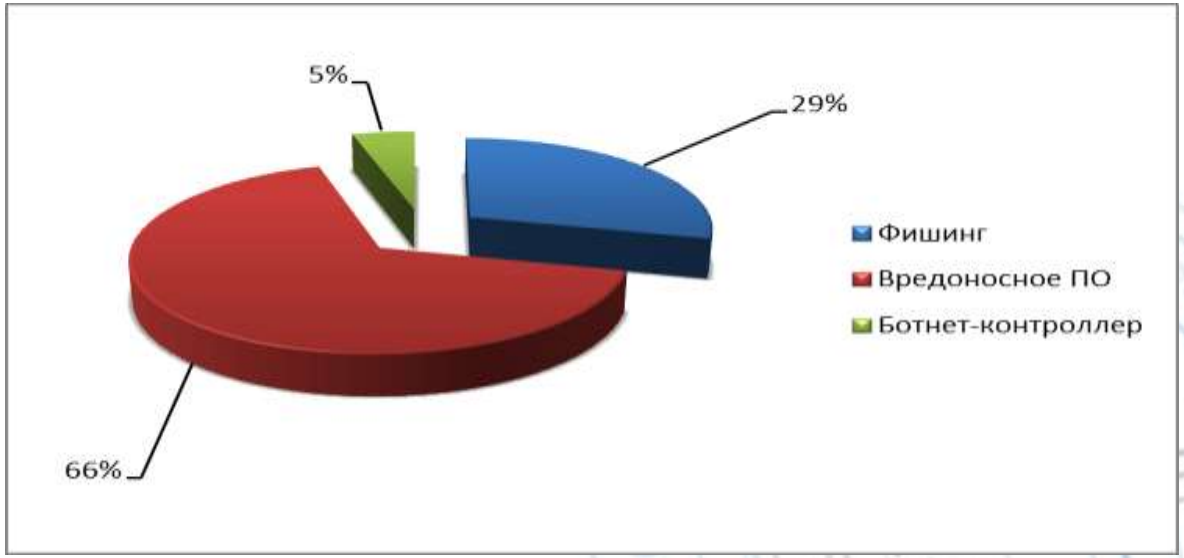
Group-IB (Группа информационной безопасности)

В соответствии с Соглашением, в область компетенции организации входит противодействие использованию доменных имен в целях фишинга, несанкционированного доступа в информационные системы третьих лиц, распространения вредоносных программ и управления вредоносными программами (бот-сетями). Group-IB является негосударственной организацией, занимающейся расследованием инцидентов информационной безопасности. Регламент взаимодействия

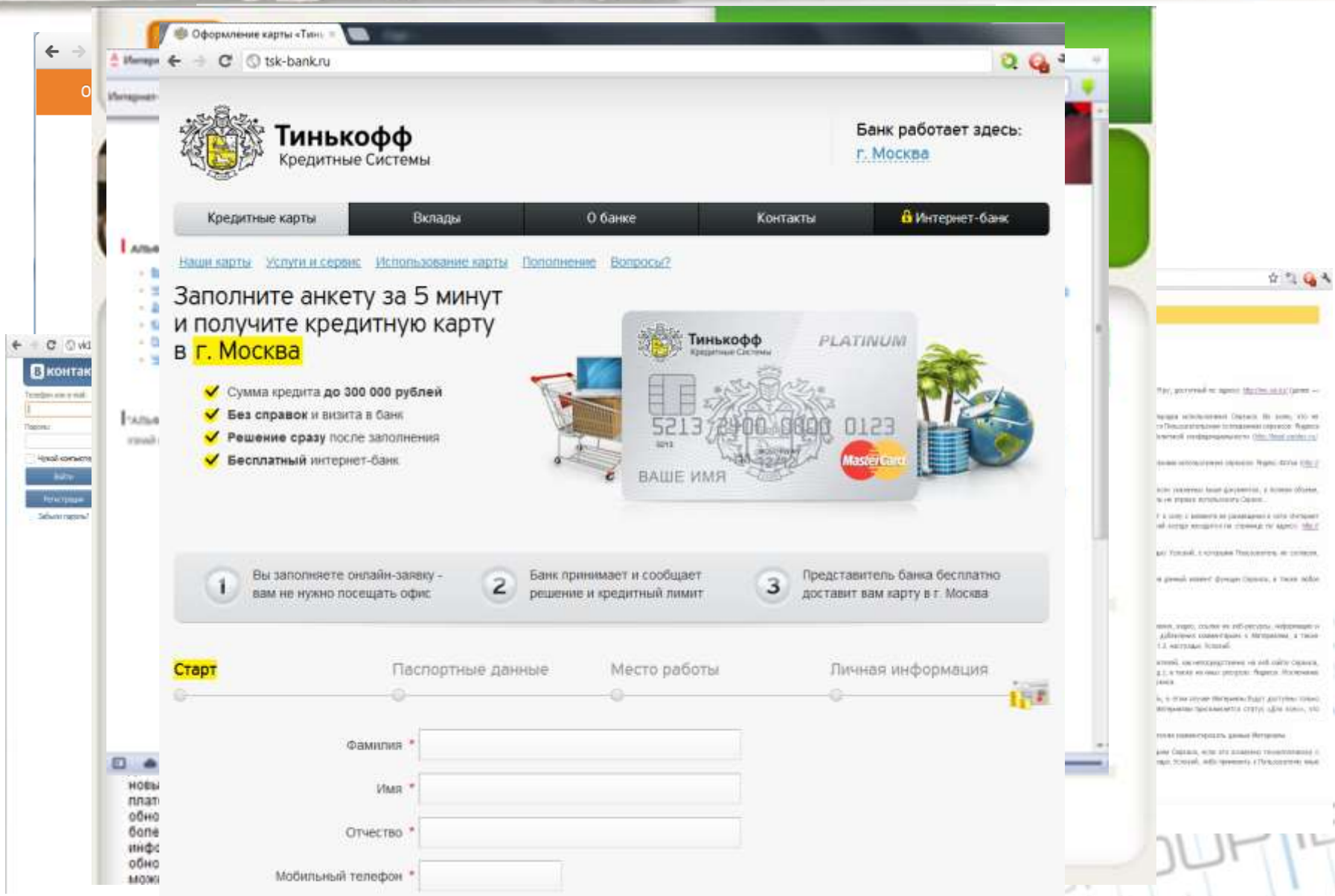
Контакты

Типы угроз в зоне .RU/.РФ





Компрометация и фишинг



Путь к противодействию

response@cert-gib.ru

CERT GIB
Computer Security Incident Response Team

+7 (495) 988-00-40
круглосуточно

CERT-GIB
- Миссия CERT-GIB
- Структура
- CERT-GIB и другие CERTы
- Наши партнеры
- Контактная информация

Реагирование на инциденты
- Как сообщить об инциденте
- Политика взаимодействия
- Взаимодействие с органами
- Политика коммуникаций

CERT IS A MARK OWNED BY CARNEGIE MELLON UNIVERSITY
CERT AUTHORIZED TO USE CERT℠

TRUSTED Introducer

CERT-GIB - Команда быстрого реагирования на компьютерные инциденты

CERT-GIB является группой по реагированию на инциденты информационной безопасности, созданной на базе компании Group-IB.

Мы работаем в режиме 24/7

Оказание услуг производится на основе абонентского договора или договора оферты.

Мы оказываем помощь в реагировании на следующие типы инцидентов:

- Отказ в обслуживании (DoS, DDoS);
- Компрометация информации;
- Компрометация актива;
- Внутренний несанкционированный доступ;
- Внешний несанкционированный доступ;
- Создание и распространение вредоносного программного обеспечения;
- Нарушение политик информационной безопасности;
- Фишинг и незаконное использование бренда в сети Интернет;
- Мошеннические действия с системами ДБО и электронными платежными системами.

В соответствии с Соглашением с Координационным Центром Национального Домена Сети Интернет (http://cctld.ru/ru/registrators/competent/) в область компетенции CERT-GIB входит противодействие использованию доменных имен в целях фишинга, несанкционированного доступа в информационные системы третьих лиц, распространения вредоносных программ и управления

Контактная информация
Сообщить об инциденте
Ключ PGP

CERT-GIB
CERTGIB

CERTGIB Android dev smacked with £50k fine over premium rate SMS scam theregister.co.uk/2012/09/04/and...
4 hours ago · reply · retweet · favorite

CERTGIB Московский владелец коротких номеров оштрафован за распространение трояна securitylab.ru/news/429533.php
4 hours ago · reply · retweet · favorite

CERTGIB The virus activity in August 2012: botnets growing, Java vulnerabilities and new threats to Android news.drweb.com/show/?i=2717&l...
21 hours ago · reply · retweet · favorite

CERTGIB Обзор вирусной активности в августе 2012 года: растущие ботнеты, уязвимость Java и новые угрозы для Android news.drweb.com/show/?i=2717&l...
21 hours ago · reply · retweet · favorite

CERTGIB Q&A about domain disputes cctld.ru/ru/activities/...
2 days ago · reply · retweet · favorite

Join the conversation

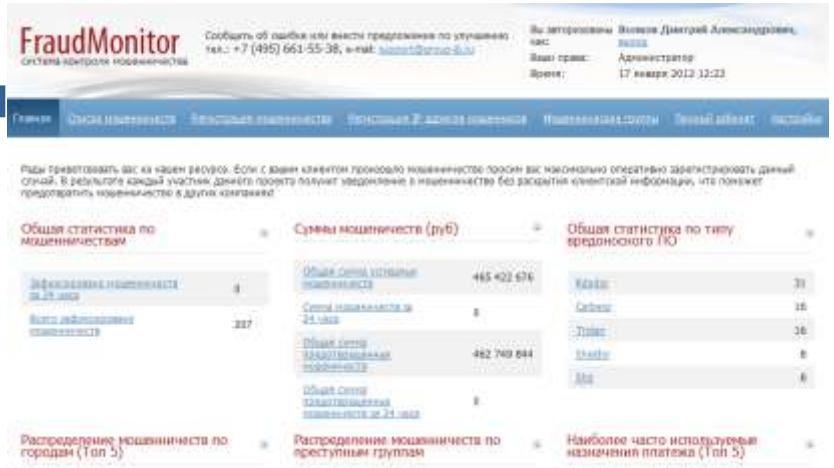
Профилактика хищений

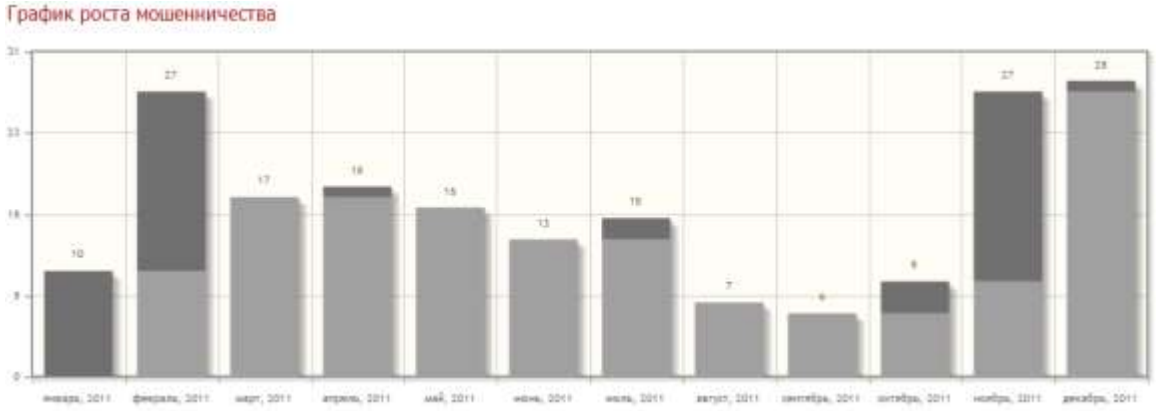
FraudMonitor

- ✓Предоставление единого интерфейса регистрации преступлений
- ✓Консолидация разрозненной информации по мошенничеству в ДБО
- ✓Генерация правил для систем предотвращения мошенничеств
- ✓Оперативное оповещение участников системы
- ✓Снижение уровня преступлений в сфере электронной коммерции
- ✓Ускорение процесс обмена информацией о мошенничестве между банками
- ✓Повышение качества и количества раскрываемых преступлений
- ✓Предоставление прозрачной статистической и аналитической информации

Регистрируемые данные

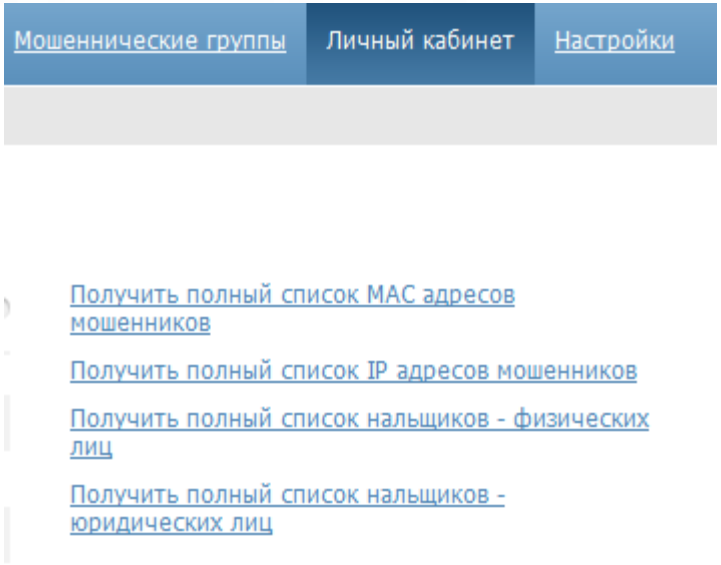
- ✓ Данные из платежного поручения
- ✓ Связи со схемами «обнала»
- ✓ Сведения о вредоносном ПО
- ✓ IP-адреса и MAC-адреса





Данные для предотвращения

- ✓ Списки «нальщиков», включая цепочки
- ✓ IP и MAC-адреса злоумышленников
- ✓ Данные по платежным поручениям



274 fraud create

FraudMonitor@FraudMonitor

Отправлено: Ср 11.01.2012 16:17

Кому: volkov@group-ib.ru

ID	274
дата	16.12.2011
счет получателя	40802810100060010417
банк получателя	ОАО АКБ "Авангард"
БИК банка получателя	044525201
ИНН	771534176630
ФИО(Название) получателя	Щуров Евгений Александрович (ИП)

ip	mac	user-agent

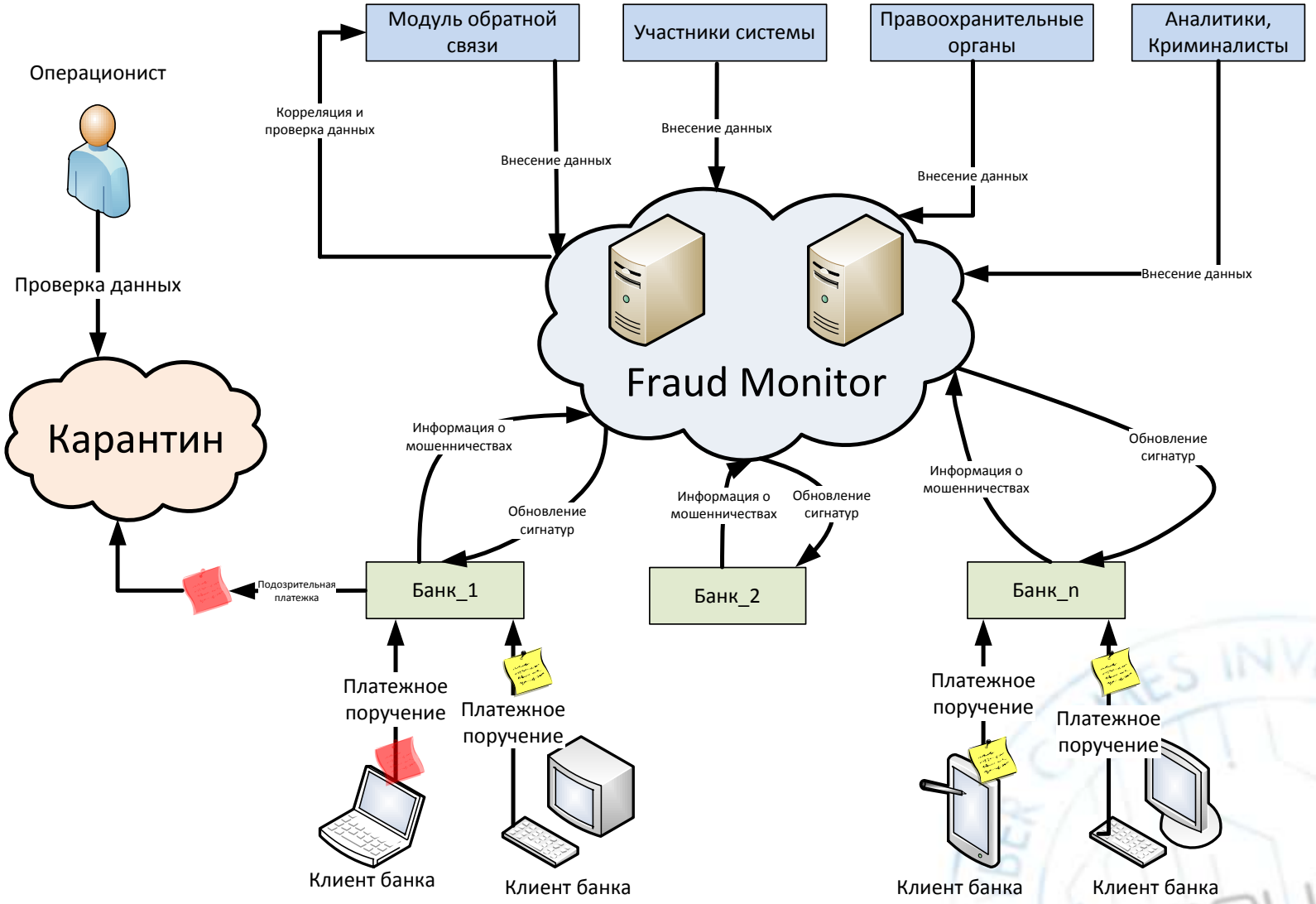
Предоставляемые данные

- ✓Прозрачная статистическая информация
- ✓Возможность поиска по общей базе хищений с удобными фильтрами
- ✓Черные списки IP- и MAC-адресов
- ✓Черные списки юридических и физических лиц
- ✓Результаты криминалистических исследований
- ✓Полная выборка хищений, где клиенты вашего банка участвовали в цепочке обналичивания похищенных денежных средств

Преимущества

- ✓Возможность предотвращать хищения денежных средств со счетов клиентов
- ✓Оперативность и достоверность полученных данных
- ✓ Возможность проведения комплексного расследования
- ✓Сохранение полной истории по хищениям
- ✓Получение прозрачной и достоверной статистической информации

Совместная работа



Дальнейшее развитие

- ✓Встроенный модуль в CyberCop
- ✓Единая площадка совместной работы экспертов и правоохранительных органов
- ✓Платформа для создания центра мониторинга угроз
- ✓Единая система предотвращения хищений

Sk Сколково

Банк России

Министерство финансов

+7 495 66I 55 38 www.group-ib.ru www.letagroup.ru