



**Компьютерные преступления
в финансовом секторе**



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





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. \$

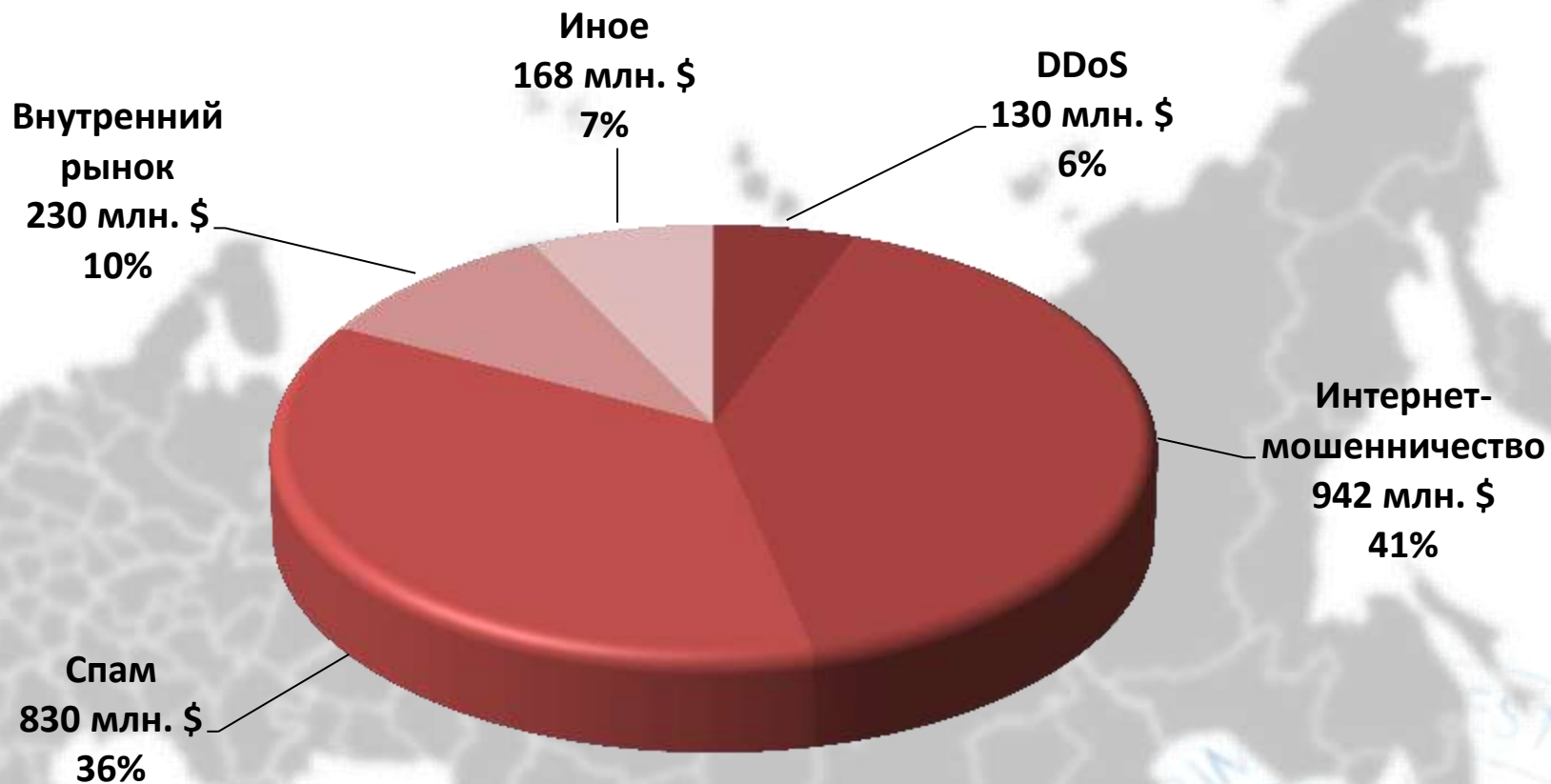
Мировой рынок

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.

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



- ✓ 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



- ✓ 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



- ✓ 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



Serbia	40	5
Russian Federation	1443642	64750
Saudi Arabia	27	0

CRIME INVESTIGATION

Противодействие фишингу



Братья Попелыш

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



CERT-GIB
Нью Йорк:
GMT-5

CERT-GIB
Москва:
GMT+4

CERT-GIB
Владивосток:
GMT+10

CERT-GIB: Европа, Северная Америка, Азия

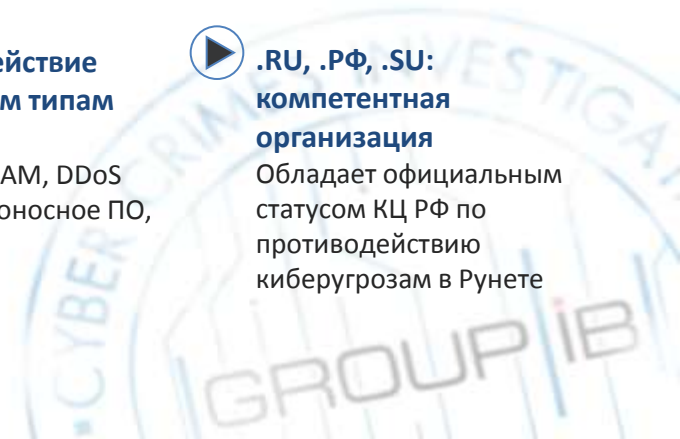


▶ **Первый 24/7 CERT в Восточной Европе**
CERT-GIB первый в Восточной Европе круглосуточный центр реагирования на инциденты ИБ.

▶ **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





Координационный центр
национального домена сети Интернет

WHOIS

.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](#)

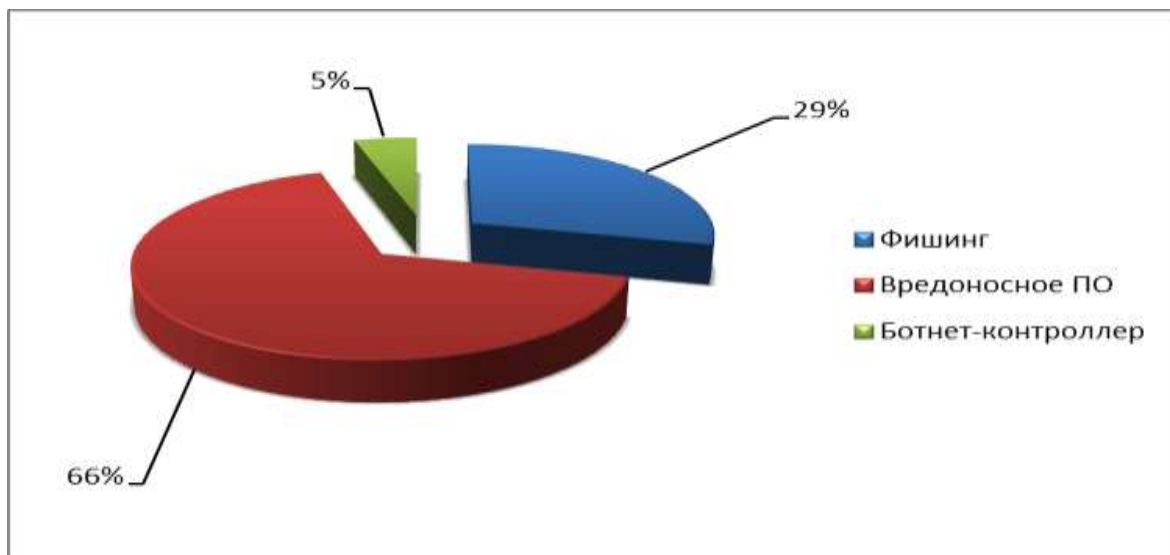
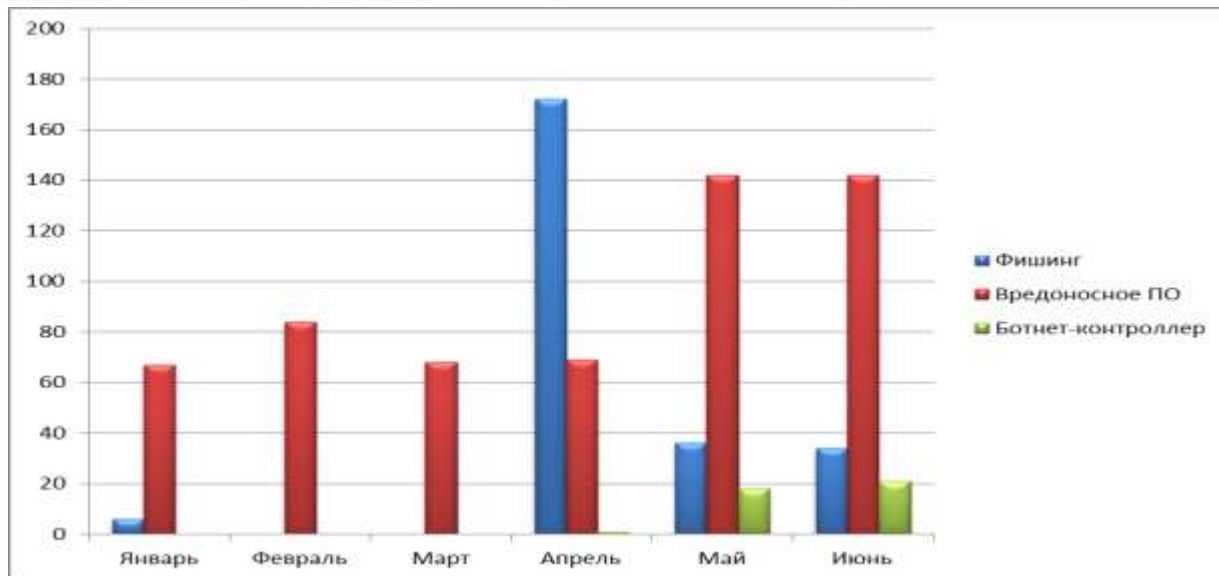
[Group-IB](#) (Группа информационной безопасности)

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

Оформление карты «Тинькофф»

tsk-bank.ru

Тинькофф
Кредитные Системы

Банк работает здесь:
[г. Москва](#)

Кредитные карты | Вклады | О банке | Контакты | Интернет-банк

Наши карты | Услуги и сервис | Использование карты | Пополнение | Вопросы?

Заполните анкету за 5 минут и получите кредитную карту в г. Москва

- ✓ Сумма кредита до 300 000 рублей
- ✓ Без справок и визита в банк
- ✓ Решение сразу после заполнения
- ✓ Бесплатный интернет-банк

1 Вы заполняете онлайн-заявку - вам не нужно посещать офис

2 Банк принимает и сообщает решение и кредитный лимит

3 Представитель банка бесплатно доставит вам карту в г. Москва

Старт | Паспортные данные | Место работы | Личная информация

Фамилия *

Имя *

Отчество *

Мобильный телефон *

Путь к противодействию

response@cert-gib.ru



+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](#)



Computer Security Incident Response Team
Мы работаем круглосуточно

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/...](http://cctld.ru/ru/activities/)
2 days ago · reply · retweet · favorite



Join the conversation

Профилактика хищений



- ✓ 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

FraudMonitor
Служба контроля мошенничества

Сообщить об ошибке или внести предложение по улучшению:
тел.: +7 (495) 661-55-38, e-mail: support@group-ib.ru

Вы авторизованы: Валерий Дмитрий Александрович,
ИБС
Ваш статус: Администратор
Время: 17 января 2012 12:23

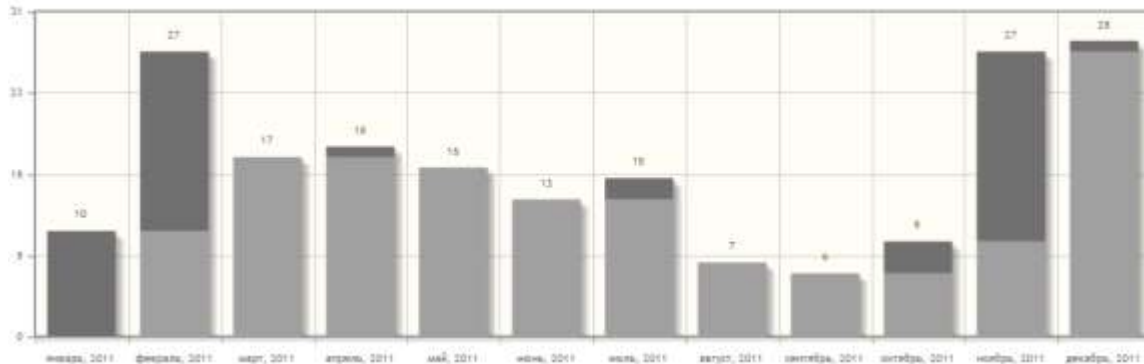
Главная | О нас | Источники данных | Владельцы мошенничества | Источники IP-адресов мошенников | Мошенничества | Заказы | Обратная связь | Поддержка

Рядом приватизировать нас как частный ресурс. Если с вами клиентом произошло мошенничество, просим вас максимально оперативно зарегистрировать данный случай. В результате каждой успешной операции с участием денежных средств клиент получает уведомление о мошенничестве без раскрытия клиентской информации, что позволяет предотвратить мошенничество в других компаниях.

Общая статистика по мошенничествам		Суммы мошенничества (руб)		Общая статистика по типу вредоносного ПО	
Идентифицировано мошенничества за 24 часа	4	Общая сумма выявленных мошенничества	465 402 676	Клоны	31
Всего идентифицировано мошенничества	227	Сумма мошенничества за 24 часа	0	Сетевые	16
		Общая сумма зарегистрированных преступлений	482 740 644	Трояны	16
		Общая сумма зарегистрированных мошенничества за 24 часа	0	Трояны	0
				Антивирус	6

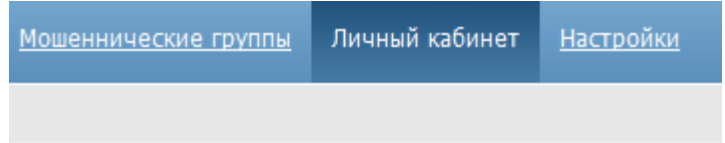
Распределение мошенничества по городам (Топ 5)		Распределение мошенничества по преступным группам		Наиболее часто используемые назначения платежа (Топ 5)	
Москва	10	Группа 1	27	Средства для оплаты товаров	31
Санкт-Петербург	27	Группа 2	18	Средства для оплаты услуг	16
Новосибирск	17	Группа 3	9	Средства для оплаты товаров	16
Казань	18	Группа 4	7	Средства для оплаты услуг	0
Самара	16	Группа 5	6	Средства для оплаты товаров	6

График роста мошенничества



Данные для предотвращения

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



[Получить полный список MAC адресов мошенников](#)

[Получить полный список IP адресов мошенников](#)

[Получить полный список нальщиков - физических лиц](#)

[Получить полный список нальщиков - юридических лиц](#)

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

Мошенническая операция ID236

Данные из платежного поручения

Дата совершения:	21.11.2011
Сумма перевода(руб.):	200000
Платежное поручение(ОД):	ОД
Банк плательщика:	АКБ "Авангард" (Г/ОАО)
Сред. получателя(адрес):	Москва
Банк получателя:	ОАО "ОСБ Банк"
БИК Банка-получателя:	044525201
К. Сч. Пл.	30101810300000000000
К. Сч. Пл.	40702810300000000000
Пред. код назначения платежа:	Еврейбург
Получатель:	ООО "Авант"
ИНН:	447662378
ИПЕ:	
Назначение платежа:	Служба за технологическое исследование и идентификация по договору №718 от 19.11.2011
Идентификационный номер:	126

Общие сведения

Метод:	--- неизвестно ---
Мошенничество подтверждено:	Да
Способ кражи (классификация):	--- неизвестно ---
Использованная система:	--- неизвестно ---
Классификация:	Криминальная
Вид мошенничества:	Криминальная
Согласовано ли мошенничество (Одн. статус):	<input checked="" type="checkbox"/> Не банк <input type="checkbox"/> Не клиент

Статус:

Идентификационный номер:

308



- ✓ 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

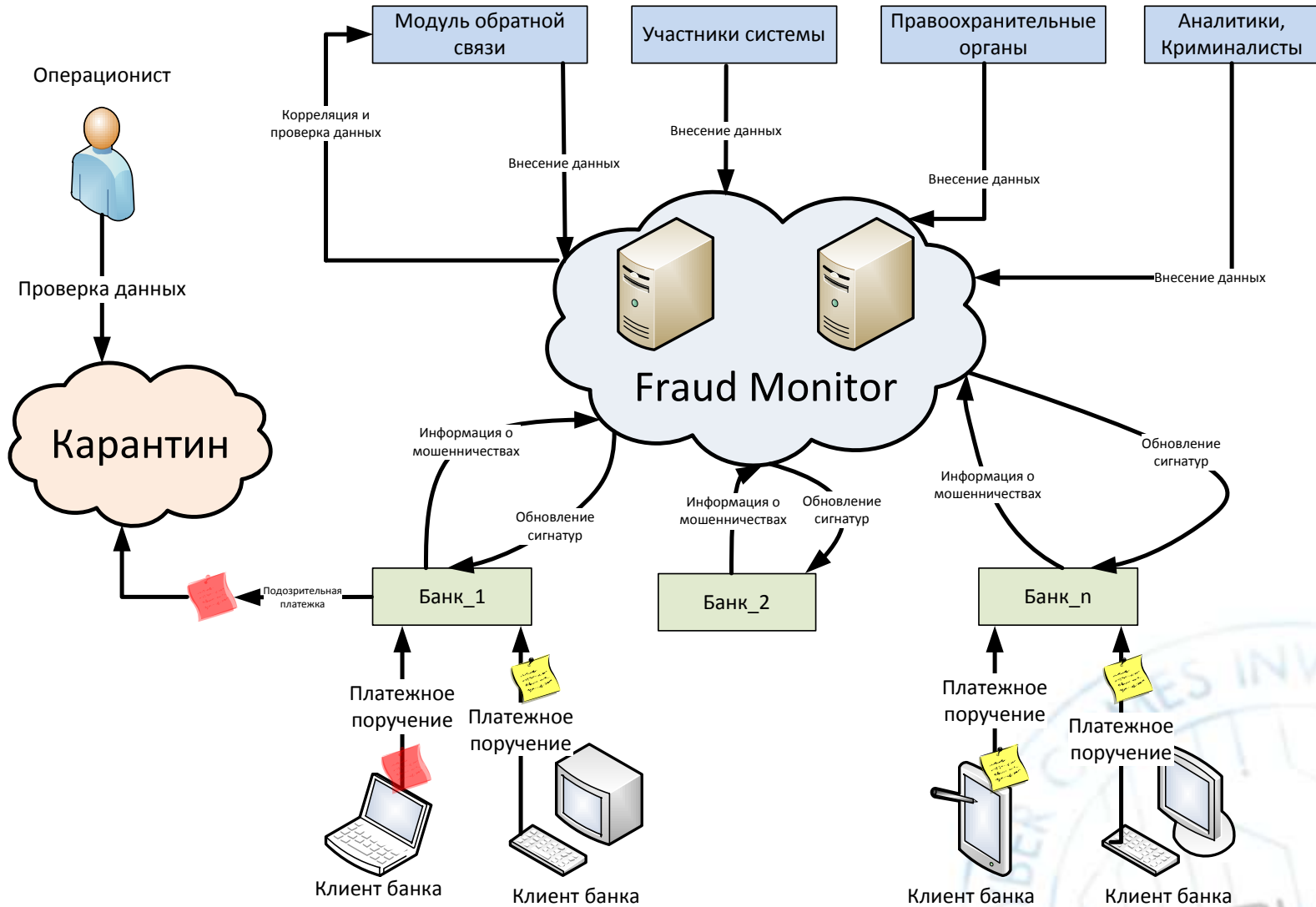


Преимущества

- ✓ 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

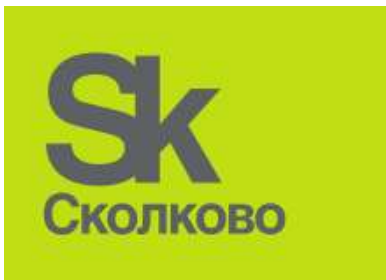


Совместная работа



Дальнейшее развитие

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





+7 495 661 55 38 www.group-ib.ru www.letagroup.ru