

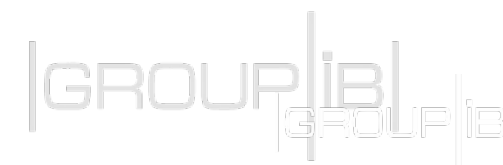


Управление рисками противоправных и мошеннических действий в системах ДБО физических и юридических лиц





Статистика хищений из ДБО



Сегмент рынка в России и СНГ	Кол-во групп	Общее число успешных атак в день	Средняя сумма одного хищения	Сколько воруют в день	H2 2016 — H1 2017		H2 2015 — H1 2016		Процент роста к прошлому периоду
					в RUB	в USD	в RUB	в USD	
Хищения в интернет-банкинге у юридических лиц с использованием вредоносных программ	3	2	1 250 000 ₽	2 500 000 ₽	622 500 000 ₽	\$10 375 000	956 160 000 ₽	16 774 737 \$	-35%
Хищения в интернет-банкинге у физических лиц с использованием вредоносных программ	1	1	63 000 ₽	63 000 ₽	15 687 000 ₽	\$261 450	6 424 200 ₽	112 705 \$	144%
Хищения у физических лиц с Android-троянами	10	300	11 000 ₽	3 300 000 ₽	821 700 000 ₽	\$13 695 000	348 600 000 ₽	6 115 789 \$	136%
Целевые атаки на банки	2	—	—	—	1 630 000 000 ₽	\$27 166 667	2 500 000 000 ₽	43 859 649 \$	-35%
Фишинг	15	950	1 000 ₽	950 000 ₽	236 550 000 ₽	\$3 942 500	—	—	—
Обналичивание похищаемых средств	—	—	—	2 638 350 ₽	1 390 449 150 ₽	\$23 174 153	1 715 032 890 ₽	30 088 296 \$	-19%
Итого				6 813 000 ₽	4 716 886 150 ₽	\$78 614 769	5 526 217 090 ₽	96 951 177 \$	-15%

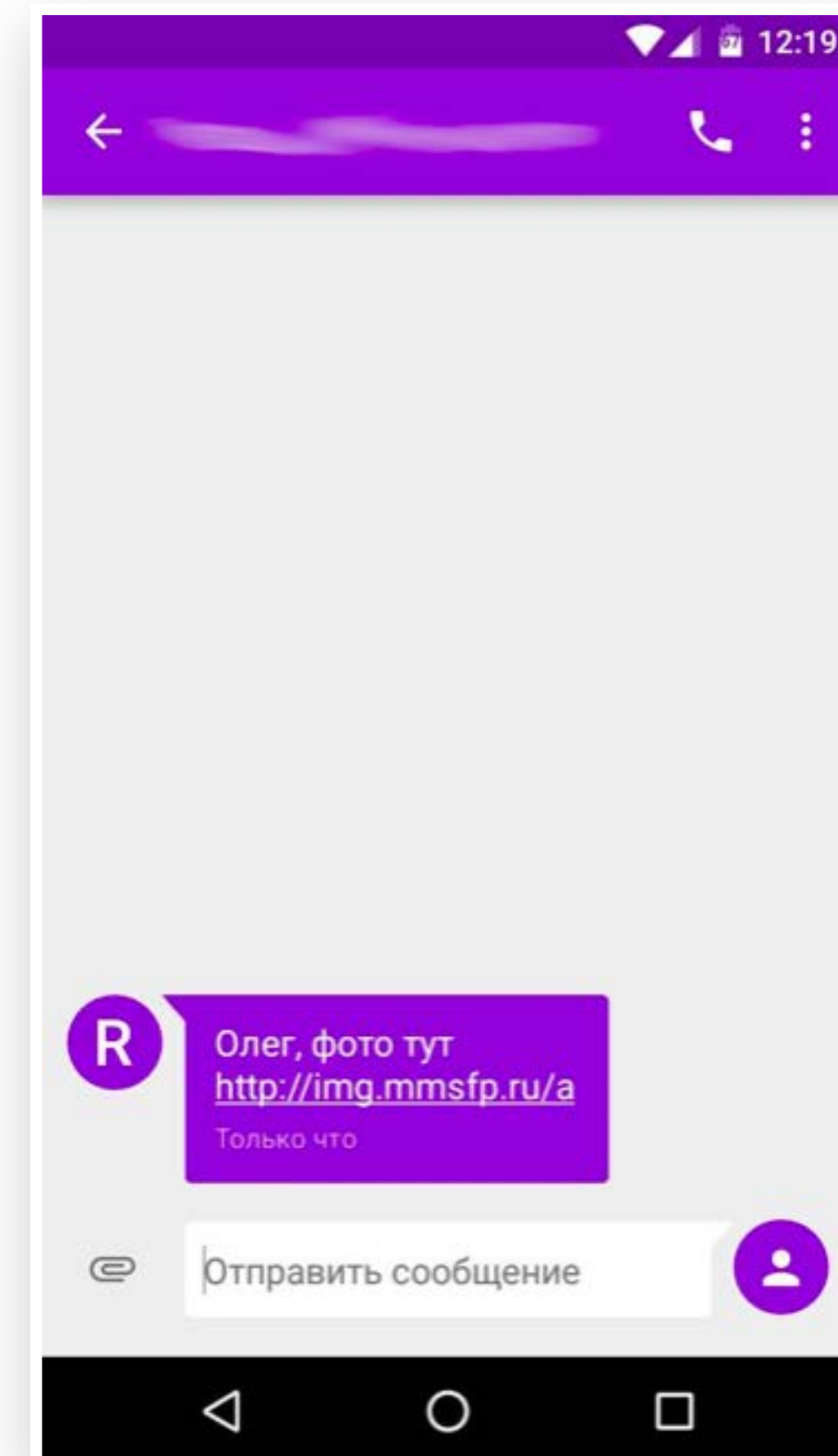
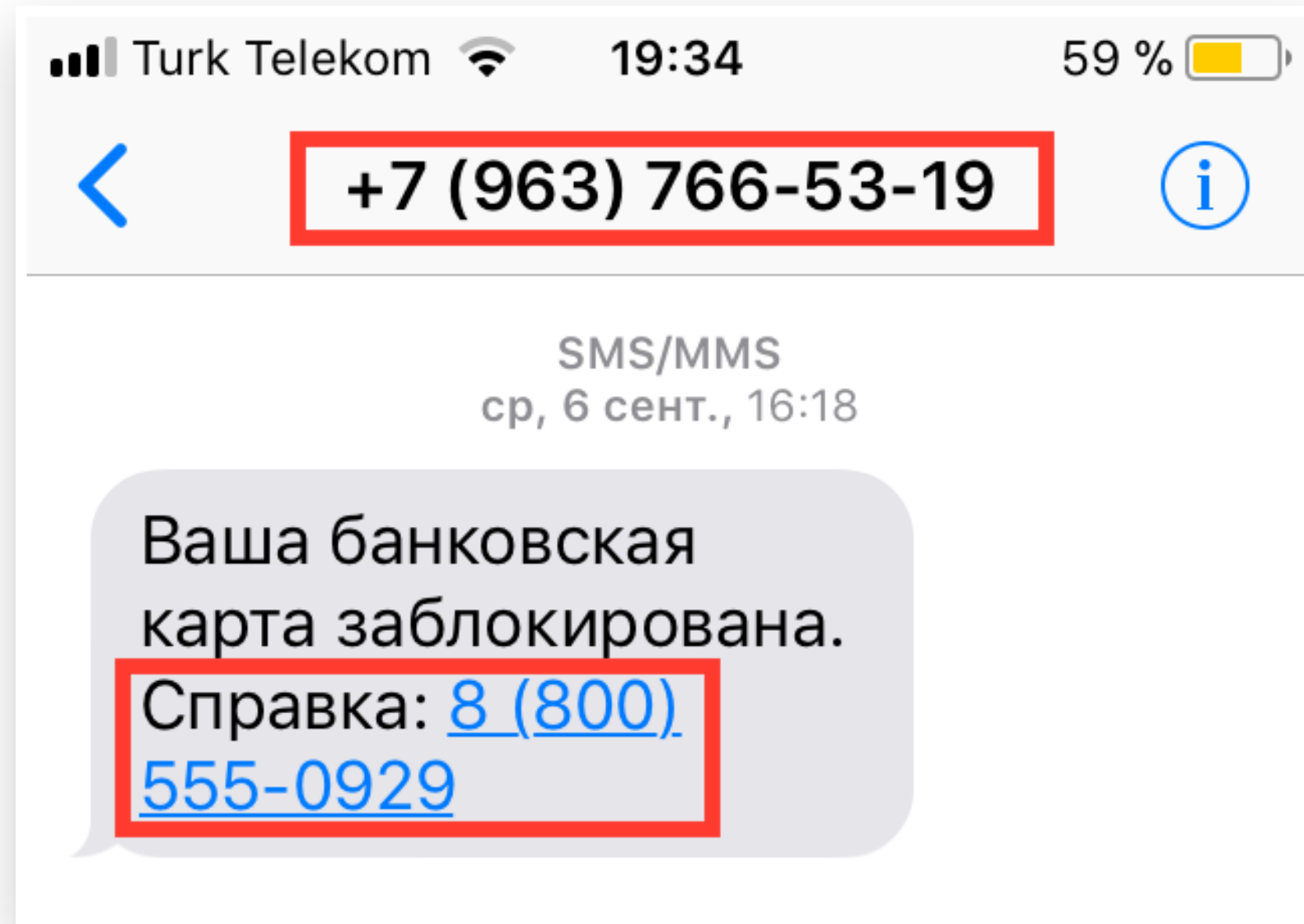
* <https://www.group-ib.ru/2017-report.html>



Социальная инженерия

Подложные СМС-сообщения

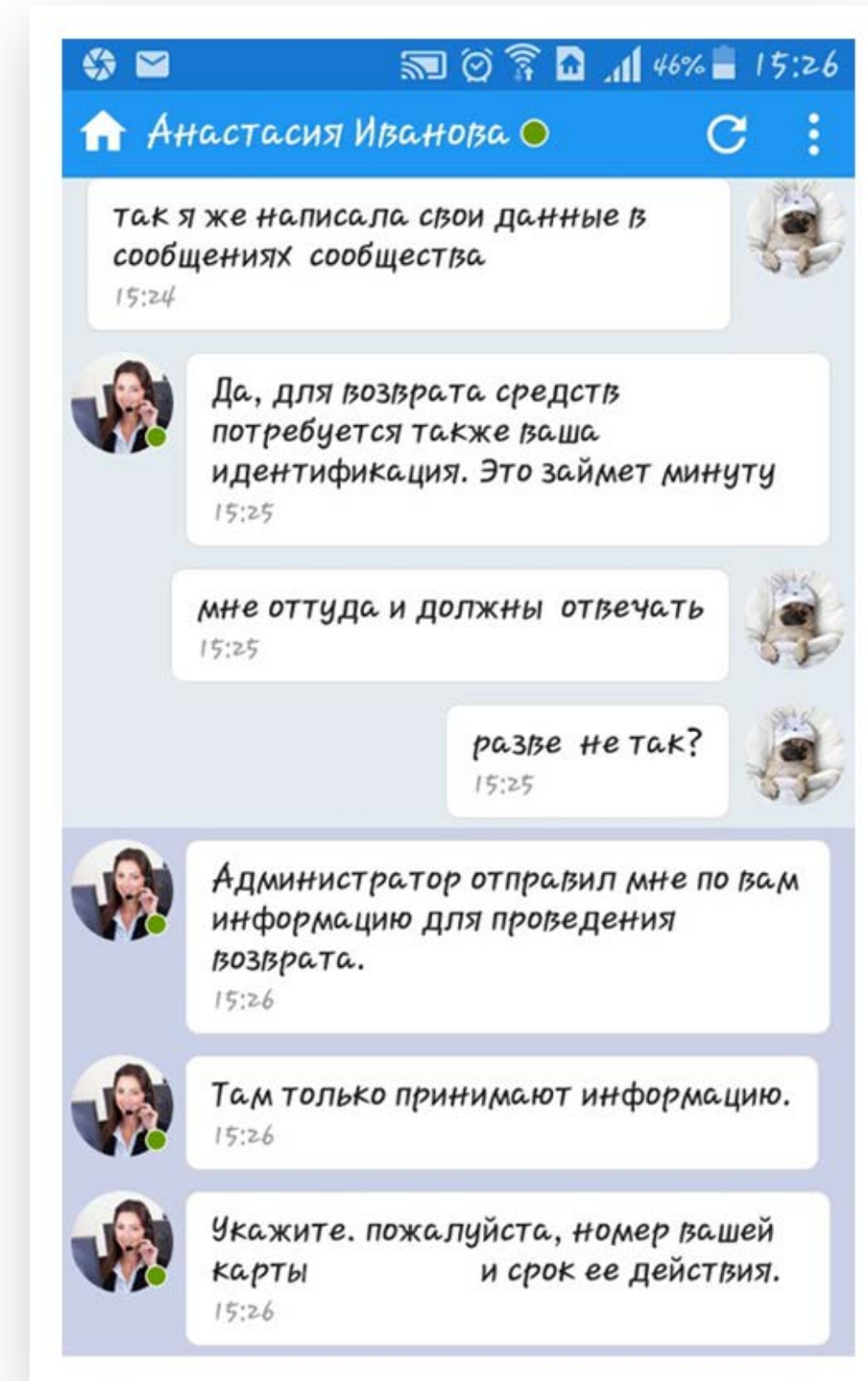
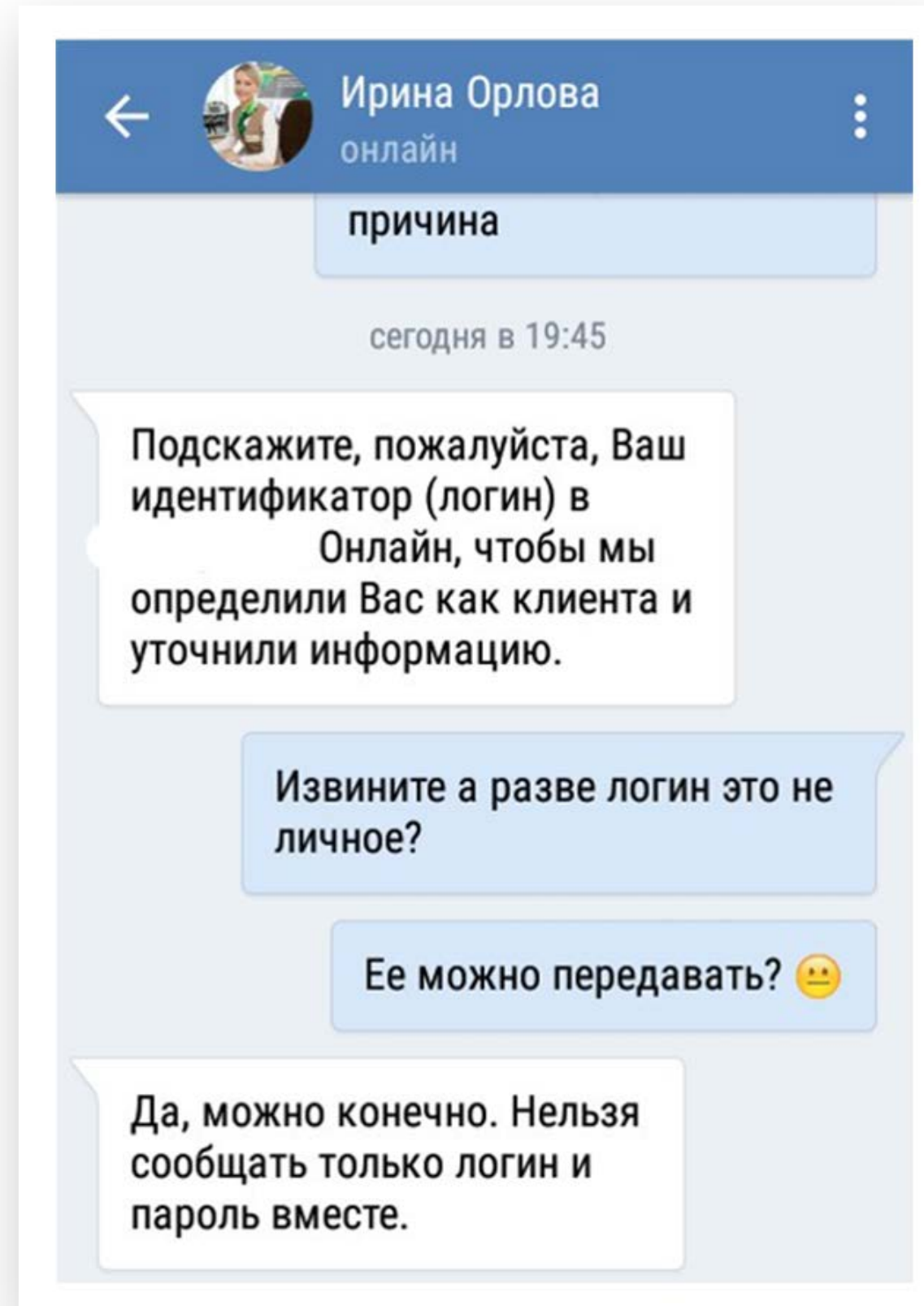
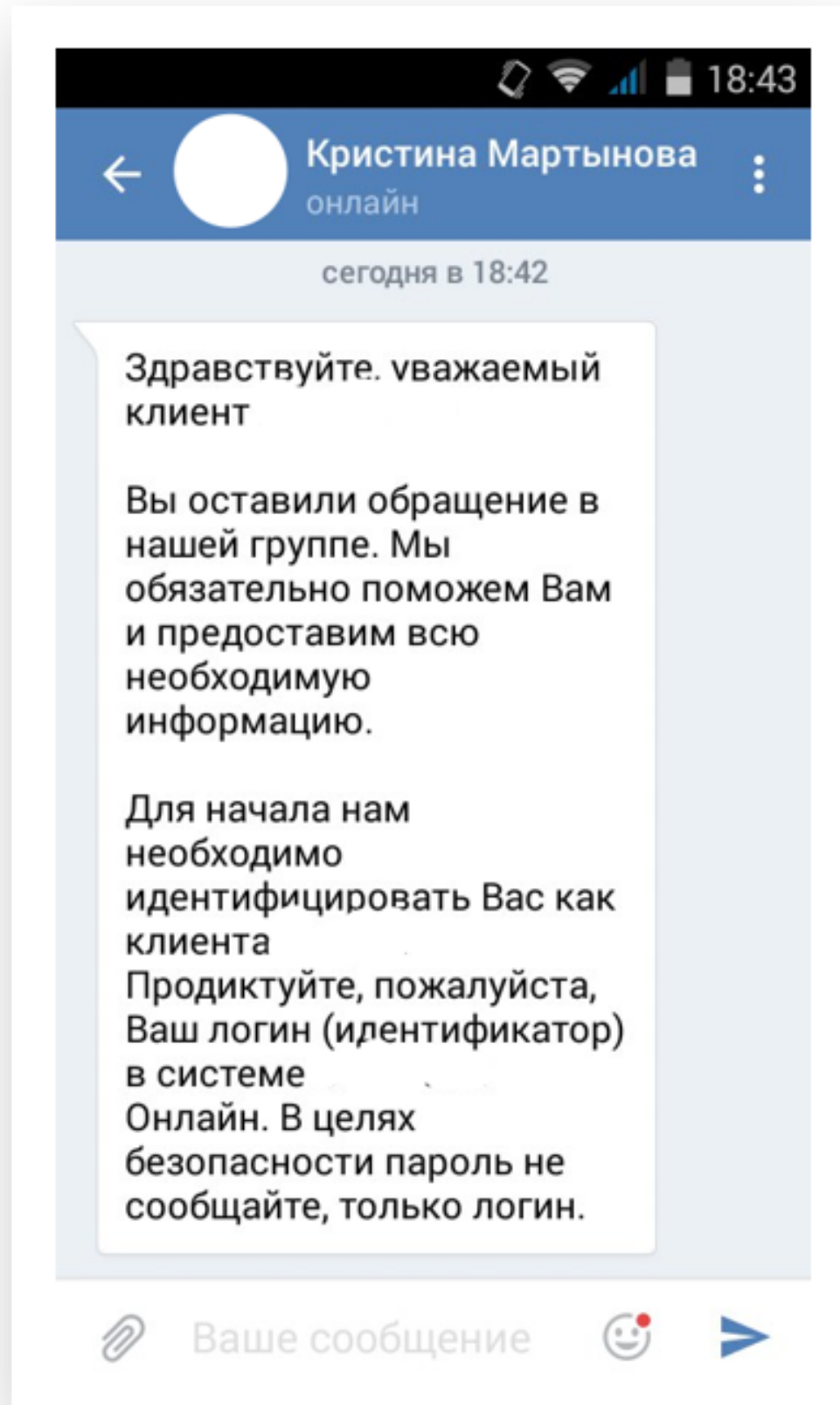
GROUP IB
GROUP ID





Социальная инженерия

Социальные сети





5 уровней противодействия мошенничеству



Big Data User and Entity Analytics

- Enable analysis of both linkages and relationships across users and other entities and their attributes using data in big data stores to detect fraud

User- and Entity-Centric for Multiple Channels and Products

- Analyzes and correlates users and other entity behavior across different channels and products, and prioritizes alerts using rules or statistical models

User- and Entity-Centric for Specific Channel

- Monitors and analyzes user and entity behavior, as well as identifies anomalous behavior using rules or statistical models

Navigation- and Network-Centric

- Analyzes session or network behavior and compares it to what is expected

End-point centric

- Malware detection, end-point behavior and location correlation
- Device fingerprinting, phone printing and “bloprinting”





Нужно видеть полную картину Что делает клиент...



Secure Bank

Secure Bank

Secure Bank

Secure Bank

SB

Secure Bank

Сессиями

Единичное

Вернуться

Время события:

2017-11-08 08:18:23 - 2017-11-08 08:18:23

IP адреса:

83.239.96.116

Уровни риска:

HIGH

Тип риска:

Социальная инженерия - высокий уровень

URL Адреса:

https://.../priva

Обновить информацию

Логин:

f8d71b1159b7994973061ed30c9a7eb8df865d01

Активность

Устройства

Пользователи

Местоположение

Скрипты

Формы

URL

Выбрать колонки

Выгрузить в CSV

ID сессии	Дата	Логин	IP	URL
613820132006	2017-11-08 08:16:04	f8d71b1159b7994973061ed30c9a7eb8df865d01	83.239.96.116	https://.../private/payments/servicesPayments.do?s...omResource=
613820132006	2017-11-08 08:15:53	f8d71b1159b7994973061ed30c9a7eb8df865d01	83.239.96.116	https://.../private/payments.do
613820132006	2017-11-08 08:15:09	f8d71b1159b7994973061ed30c9a7eb8df865d01	83.239.96.116	https://.../private/cards/list.do#
613820132006	2017-11-08 08:14:57	f8d71b1159b7994973061ed30c9a7eb8df865d01	83.239.96.116	https://.../private/cards/list.do
613820132006	2017-11-08 08:13:35	f8d71b1159b7994973061ed30c9a7eb8df865d01	83.239.96.116	https://.../private/accounts.do
613820132006	2017-11-08 08:13:12	f8d71b1159b7994973061ed30c9a7eb8df865d01	83.239.96.116	https://.../confirm/way4.do
613820132006	2017-11-08 08:06:17	f8d71b1159b7994973061ed30c9a7eb8df865d01	83.239.96.116	https://.../nc/page/registration.do
613820132006	2017-11-08 08:05:49	f8d71b1159b7994973061ed30c9a7eb8df865d01	83.239.96.116	https://...ex.do
613820132006	2017-11-08 08:05:41	f8d71b1159b7994973061ed30c9a7eb8df865d01	83.239.96.116	https://.../nc/page/recover.do
613820132006	2017-11-08	f8d71b1159b7994973061ed30c9a7eb8df865d01	83.239.96.116	https://...

Статистика

Поиск

События

Отчеты

Домены

Скрипты

Формы

Проверенные клиенты

Белый список

Сборщик

/private/payments.do

/private/cards/list.do#

/private/cards/list.do

/private/accounts.do

/confirm/way4.do

/nc/page/registration.do

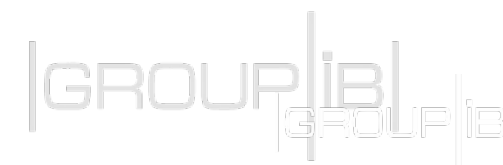
lex.do

/nc/page/recover.do

6



Нужно видеть полную картину Как делает клиент...



Вход легального пользователя

```
2017-11-16 16:15:50; mouse_click; {"id":null,"name":null,"tag":"A","pageX":777,"pageY":212};
2017-11-16 16:15:47; base_number; {"id":"j_password","name":"j_password","tag":"INPUT"};
2017-11-16 16:15:35; mouse_click; {"id":"j_password","name":"j_password","tag":"INPUT","pageX":573,"pageY":175};
2017-11-16 16:15:28; base_number; {"id":"j_username","name":"j_username","tag":"INPUT"};
2017-11-16 16:15:25; mouse_click; {"id":"j_username","name":"j_username","tag":"INPUT","pageX":558,"pageY":119};
```

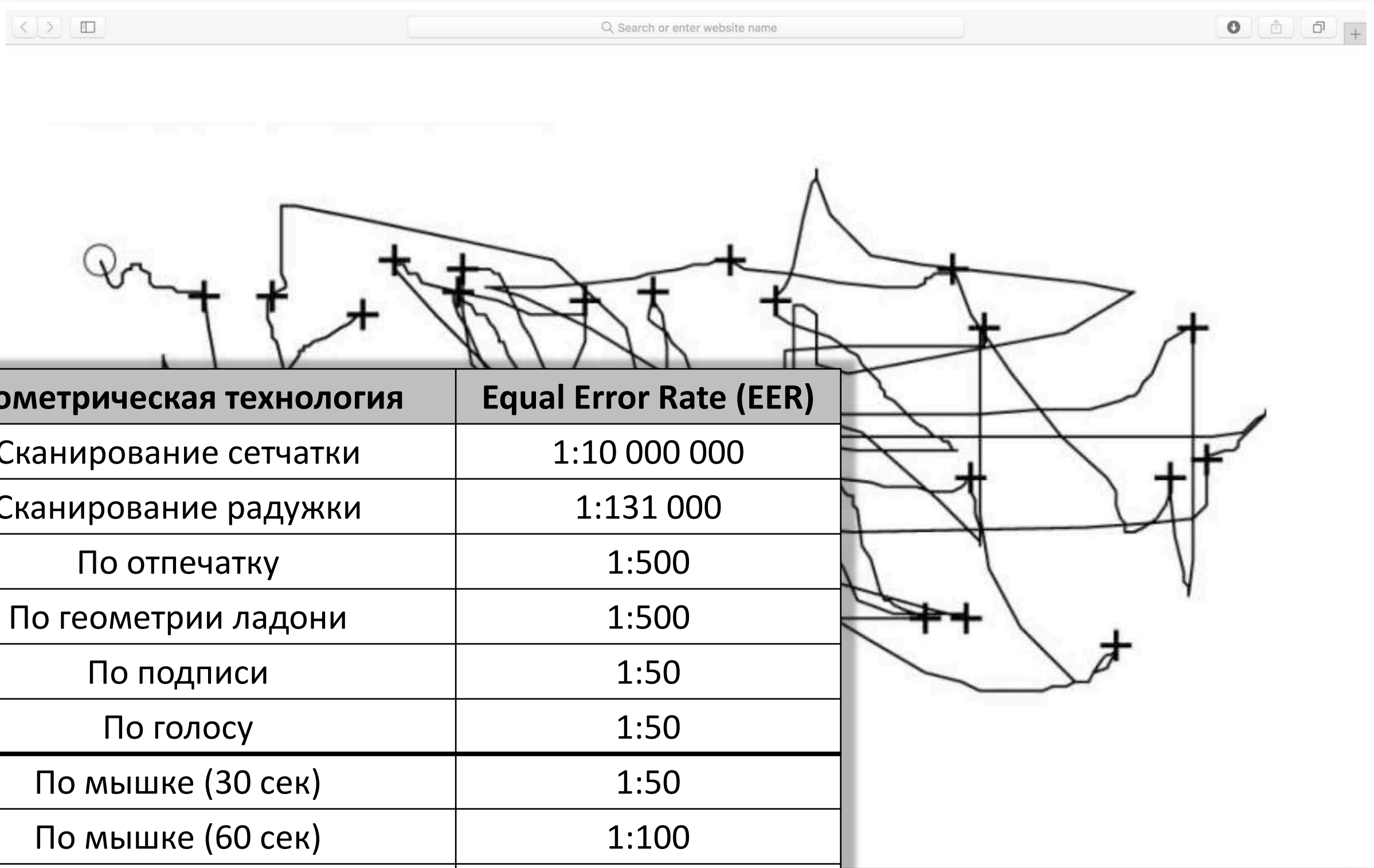
Вход мошенника

```
2017-06-20 10:11:31; mouse_click; {"id":null,"name":null,"tag":"TD","pageX":210,"pageY":352};
2017-06-20 10:11:30; paste_event; {"id":"password","name":"password","tag":"INPUT"};
2017-06-20 10:11:29; mouse_click; {"id":"password","name":"password","tag":"INPUT","pageX":190,"pageY":304};
2017-06-20 10:11:28; active_tab; -;
2017-06-20 10:11:22; not_active_tab; -;
2017-06-20 10:10:41; mouse_click; {"id":"password","name":"password","tag":"INPUT","pageX":226,"pageY":300};
2017-06-20 10:10:39; paste_event; {"id":"login","name":"login","tag":"INPUT"};
2017-06-20 10:10:38; mouse_click; {"id":"login","name":"login","tag":"INPUT","pageX":221,"pageY":244};
2017-06-20 10:10:38; mouse_click; {"id":"login","name":"login","tag":"INPUT","pageX":221,"pageY":244};
2017-06-20 10:10:37; active_tab; -;
2017-06-20 10:10:33; not_active_tab; -;
2017-06-20 10:10:18; current_page; -;
```



Нужно видеть полную картину (ПОД/ФТ)

Клиент ли это...



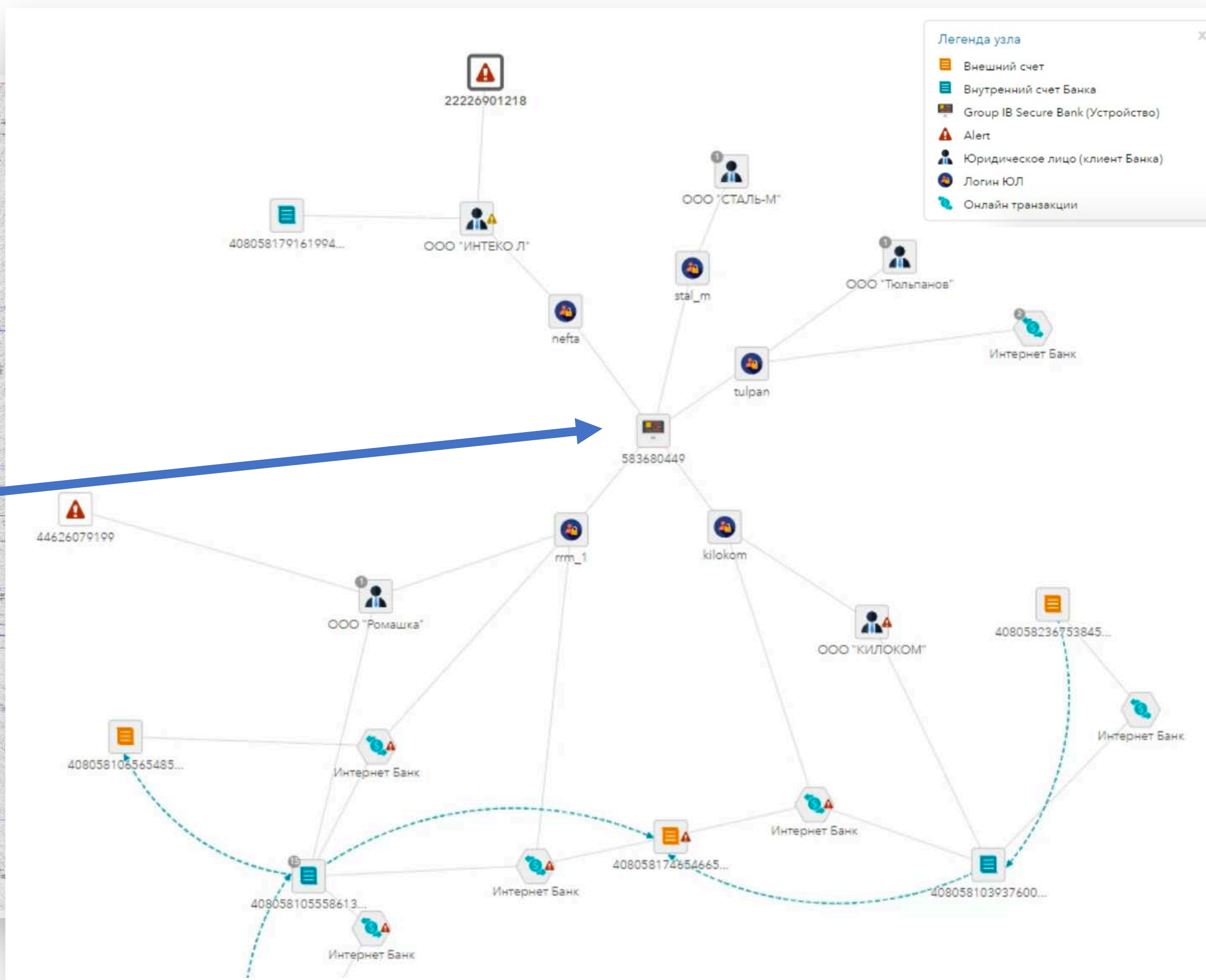
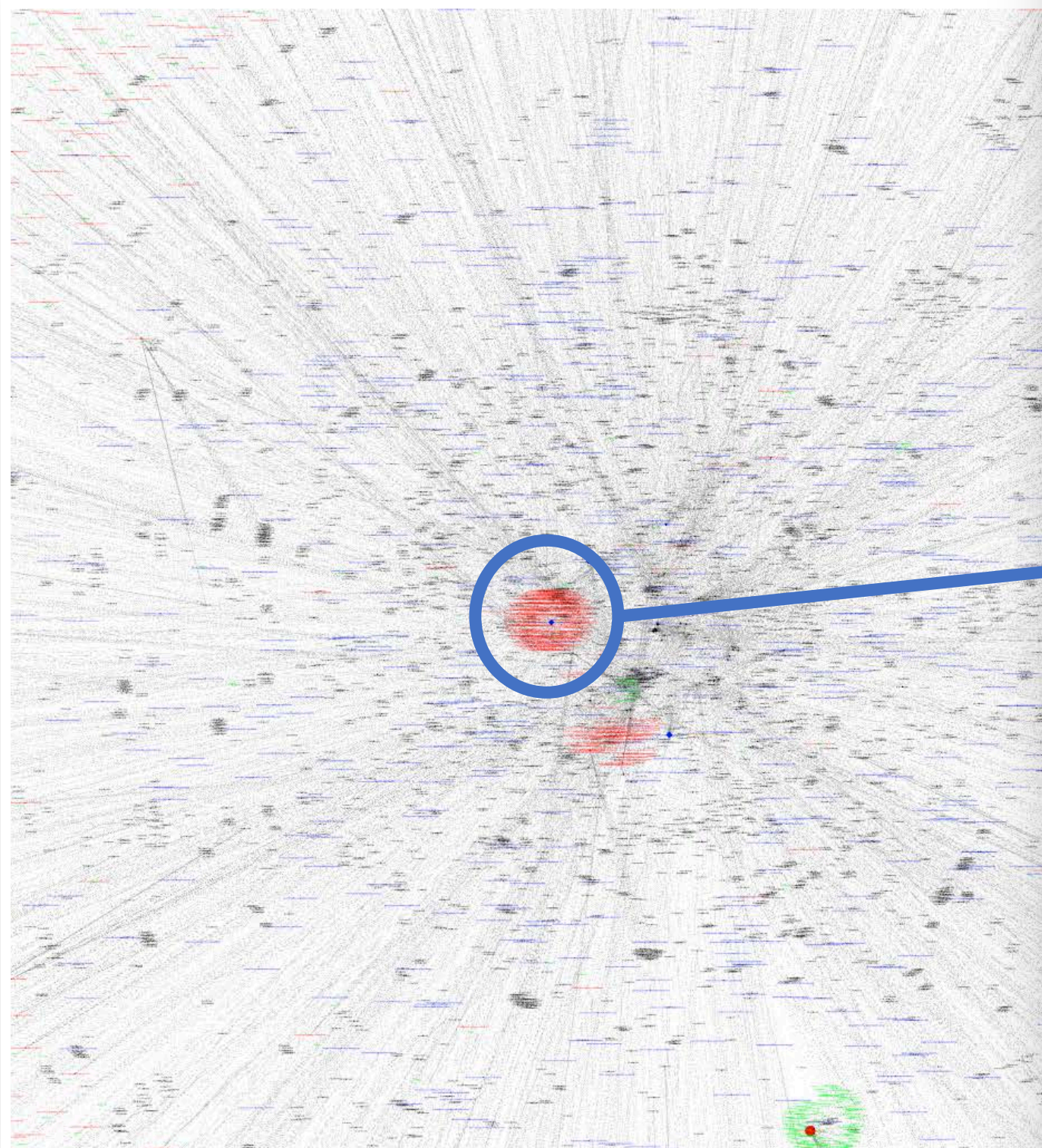
Биометрическая технология	Equal Error Rate (EER)
Сканирование сетчатки	1:10 000 000
Сканирование радужки	1:131 000
По отпечатку	1:500
По геометрии ладони	1:500
По подписи	1:50
По голосу	1:50
По мышке (30 сек)	1:50
По мышке (60 сек)	1:100
По мышке (90 сек)	1:200

У ~50%
пользователей
высокий уровень
консервативности
курсорного
почерка



Мониторинг выполнения требований ПОД/ФТ (1)

GROUP IB
GROUP ID





Мониторинг выполнения требований ПОД/ФТ (2)



"Заявление на выпуск новых бизнес-карт"

ID сессии	Логин	Пользовательская активность
557227103005	83f3914ce6bfa2147529a688ea7b0c99c717e930	<pre>2017-09-27 18:37:46; base_number; {"id":"yR9Qc50-real","name":null,"tag":"INPUT"}; 2017-09-27 18:37:43; mouse_click; {"id":"yR9Qc50-real","name":null,"tag":"INPUT","pageX":362,"pageY":343}; {"id":"yR9Q130","name":null,"tag":"INPUT","pageX":765,"pageY":264}; {"id":"yR9Q530","name":null,"tag":"INPUT"}; {"id":"yR9Q640","name":null,"tag":"BUTTON","pageX":619,"pageY":207}; {"id":"yR9Q220-real","name":null,"tag":"INPUT"}; 2017-09-27 18:36:24; mouse_click; {"id":"yR9Qq00","name":null,"tag":"INPUT","pageX":443,"pageY":160}; 2017-09-27 18:36:22; mouse_click; {"id":"yR9Q8v","name":null,"tag":"INPUT","pageX":159,"pageY":59}; 2017-09-27 18:36:19; mouse_click; {"id":"yR9Q8s","name":null,"tag":"INPUT","pageX":288,"pageY":352}; 2017-09-27 18:36:18; mouse_click; {"id":"yR9Qxr-real","name":null,"tag":"INPUT","pageX":279,"pageY":327}; 2017-09-27 18:36:17; mouse_click; {"id":"yR9Q0v-cave","name":null,"tag":"DIV","pageX":499,"pageY":314}; 2017-09-27 18:36:16; mouse_click; {"id":"yR9Q9r-real","name":null,"tag":"INPUT","pageX":531,"pageY":270}; 2017-09-27 18:36:12; mouse_click; {"id":"yR9Q5g","name":null,"tag":"INPUT","pageX":289,"pageY":80}; 2017-09-27 18:36:10; current_page; "Заявление на выпуск новых бизнес-карт"; 2017-09-27 18:36:09; mouse_click; {"id":null,"name":null,"tag":"SPAN","pageX":127,"pageY":509}; 2017-09-27 18:36:07; mouse_click; {"id":"yR9Qr1-icon","name":null,"tag":"I","pageX":12,"pageY":118};</pre>
557227103005	88c73ffdf1f76fe59aae2f2ff84d7b38c222bd22	<pre>2017-09-27 18:34:25; mouse_click; {"id":null,"name":null,"tag":"IMG","pageX":1264,"pageY":18}; 2017-09-27 18:34:23; mouse_click; {"id":null,"name":null,"tag":"DIV","pageX":942,"pageY":589}; 2017-09-27 18:33:49; mouse_click; {"id":"u3LQw0","name":null,"tag":"SPAN","pageX":982,"pageY":20}; 2017-09-27 18:33:46; mouse_click; {"id":"u3LQ0n","name":null,"tag":"BUTTON","pageX":625,"pageY":212}; 2017-09-27 18:33:44; current_page; "Список бизнес-карт"; 2017-09-27 18:33:42; mouse_click; {"id":"u3LQ48-cave","name":null,"tag":"DIV","pageX":131,"pageY":485}; 2017-09-27 18:33:36; current_page; "Заявление на выпуск новых бизнес-карт"; 2017-09-27 18:33:35; mouse_click; {"id":null,"name":null,"tag":"SPAN","pageX":95,"pageY":417}; 2017-09-27 18:33:26; mouse_click; {"id":"u3LQa7-icon","name":null,"tag":"I","pageX":29,"pageY":481}; 2017-09-27 18:33:24; mouse_click; {"id":"u3LQr1-icon","name":null,"tag":"I","pageX":11,"pageY":117};</pre>
557227103005	860c24023a68675cffc6c91972e2fd84f338ac6b	<pre>2017-09-27 18:29:49; mouse_click; {"id":"u9xPw0","name":null,"tag":"SPAN","pageX":998,"pageY":14}; 2017-09-27 18:29:42; current_page; "Главная страница"; 2017-09-27 18:29:40; mouse_click; {"id":null,"name":null,"tag":"SPAN","pageX":97,"pageY":96}; 2017-09-27 18:29:34; current_page; "Заявление на выпуск новых бизнес-карт"; 2017-09-27 18:29:33; mouse_click; {"id":null,"name":null,"tag":"SPAN","pageX":107,"pageY":324}; 2017-09-27 18:29:32; mouse_click; {"id":"u9xP4g","name":null,"tag":"BUTTON","pageX":621,"pageY":203}; 2017-09-27 18:29:32; current_page; "Список бизнес-карт"; 2017-09-27 18:29:31; mouse_click; {"id":null,"name":null,"tag":"SPAN","pageX":143,"pageY":401}; 2017-09-27 18:29:30; mouse_click; {"id":"u9xP_8-icon","name":null,"tag":"I","pageX":45,"pageY":467}; 2017-09-27 18:29:28; mouse_click; {"id":"u9xPa7-icon","name":null,"tag":"I","pageX":25,"pageY":483}; 2017-09-27 18:29:26; mouse_click; {"id":"u9xPr1-icon","name":null,"tag":"I","pageX":10,"pageY":114};</pre>



Также можно определить еще более 50 признаков намеренного или ненамеренного мошенничества или компрометации рабочего места ДБО

1. Выявление удаленного управления только через JS
2. Использование скомпрометированных учетных данных
3. Выявление работы дропперов
4. Профиль пользователя при работе в мобильном приложении
5. Классификация ПО по составу факторов и его поведению
6. Выявление подложных сайтов, нарушение бренда

Скомпрометированный логин
Смена геолокации клиента
Смена геолокации устройства
Смена поддерживаемых языков
Смена провайдера у клиента
Смена провайдера у клиента впервые за 30 дней
Смена провайдера у клиента впервые за 60 дней
Смена провайдера у стационарного устройства
Смена страны у логина
Социальная инженерия - высокий уровень
Социальная инженерия - низкий уровень
Социальная инженерия - средний уровень
У Агента появилась новая группа
Удаленное подключение (LOW)
Удаленное подключение (RDP, TeamViewer, etc.)
Удаленное подключение (VNC, Ammy Admin, etc.)
Удаленное подключение (смена разрешения)
Удаленное управление (тип 5)
Фишинг: более двух клиентов с одного устройства

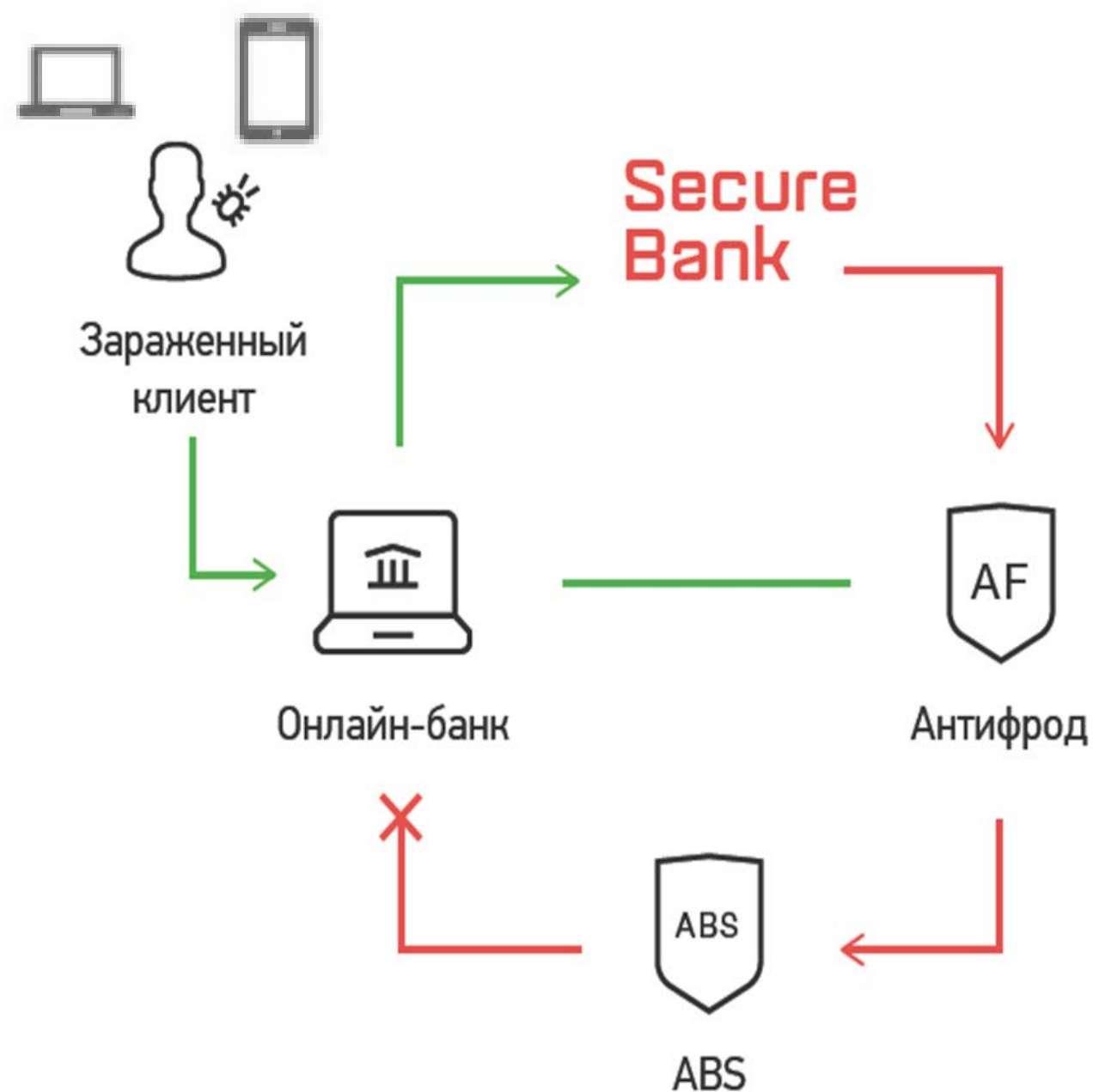


Group-IB Secure Bank

Выявление мошенничества на ранних стадиях и мониторинг соответствия ПОД/ФТ



Secure Bank защищает
«Сбербанк Онлайн»



Бесшовная интеграция с инфраструктурой

ДБО



Антифрод



SIEM



WAF





Российские инновационные
технологии в области предотвращения
и расследования преступлений в
области высоких технологий

www.group-ib.ru

group-ib.ru/blog

info@group-ib.ru

+7 495 984 33 64

twitter.com/groupib

facebook.com/group-ib