XIV конференция «РусКрипто'1012»

Москва. 28-31 марта 2012 года

Основы и пути решения проблем безопасности при дистанционном банковском обслуживании

А.Ф. Беликов

заместитель начальника управления информационной безопасности

ОАО «Россельхозбанк»

Belikovv@rshb.ru

РоссельхозБанк

ОАО «Россельхозбанк»

Доля участия государства в уставном капитале	100%
Долгосрочный кредитный рейтинг	Moody's: Baa1 Fitch: BBB
Специализация	Банк, обслуживающий АПК, агент Правительства
Количество филиалов	78 (все субъекты Российской Федерации, включая Чеченскую республику)
Количество дополнительных офисов	1539
Персонал	Более 30 000

Особенности

- **Хищения происходят в регионах**
- **Вывод похищенных средств в основном - Москва**
- **Атакам подвергаются клиенты использующие Интернет-банк и Банк-Клиент**
- **Злоумышленники территориально располагаются как в Москве, так и в регионах**

Банк и его клиенты ощущают на себе весь спектр инструментария злоумышленников

В чем риски

- **Формирование ощущения безнаказанности и «лёгких денег»**
- **Массовое распространение инструментария и массовое вовлечение в преступную деятельность**
- **Вывод финансовых средств в теневой оборот**
- **Ущерб государству**
- **Повышенные риски**

Организационно-правовая основа взаимодействия

- **Конституционные принципы равенства защиты всех форм собственности (ст.ст. 8, 35, 55 Конституции Российской Федерации)**
- **Нормы международного права**
- **Законодательство Российской Федерации, регулирующее институты банковской, коммерческой и служебной тайны, конфиденциальности персональных данных, тайны связи, средств электронной цифровой подписи, электронных средств платежа и др.:**

Организационно-правовая основа взаимодействия

- институт банковской тайны: Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» (ст. 26), Гражданский кодекс Российской Федерации от 30.11.1994 № 51-ФЗ (ст. 857), Конституция Российской Федерации (ст. 2, 17, 22);

- институт коммерческой тайны: Федеральный закон от № 98-ФЗ «О коммерческой тайне»;

- институт конфиденциальности персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ст. 5-7, 9), Гражданский кодекс Российской Федерации (ст. 150), Конституция Российской Федерации (ст. 2, 17, 22, 23);

- институт тайны связи: Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» (ст. 7, 17, 18, 44, 53, 62-64), Конституция Российской Федерации (ст. 23);

Организационно-правовая основа взаимодействия

- институт служебной тайны: Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», Конституция Российской Федерации (ст. 2, 17);

- институт конфиденциальности средств электронной цифровой подписи: Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи», Федеральный закон от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи»;

- институт конфиденциальности электронных средств платежа: Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (ст. 7, 8, 9, 10).

Организационно-правовая основа взаимодействия

- **Законодательные акты России, регулирующие деятельность правоохранительных органов:**
  - **Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции» (ст. 13);**
  - **Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» (ст. 5-7, 11);**
  - **Федеральный закон от 03.04.1995 № 40-ФЗ «О Федеральной службе безопасности» (ст. 12-13);**
  - **Федеральный закон от 17.01.1992 № 2202-1 «О прокуратуре Российской Федерации» (ст. 6, 10, 21-22);**
  - **другие правовые и нормативные акты.**
- **Соглашение между Управлением «К» Бюро специальных технических мероприятий МВД России (подразделениями «К» территориальных подразделений органов внутренних дел) и кредитными организациями о взаимодействии в области обеспечения банковской безопасности.**

Организация взаимодействия

- Организовано взаимодействие служб и специалистов информационной безопасности банков
- Ряд НБ и ГУ ЦБ РФ активно поддерживают усилия банковского сообщества по противодействию преступности с использованием ДБО
- ЦБ на уровне надзора и регулирования платежной системы начинает осознавать неизбежность вовлечения в проблему
- МВД предоставило ряд рекомендаций по сопровождению уголовных дел по хищениям через ДБО

Меры по стандартизации действий

- **Формирование единых стандартов (требований) безопасности платежных приложений**
- **Внесение изменений в законодательство**
- **Консолидация государственных органов, правоохранительных органов, операторов связи и банковского сообщества**
- **Повышение осведомленности в области информационной безопасности на государственном уровне**

Риски

- Средняя сумма покушения – 400 т.р.
- Средний «улов» специализированных банковских бот-сетей – 20-40 тыс. аккаунтов
- Средняя стоимость «атаки» – 30 тыс.р.
- Законодательство способствует преступной деятельности
- Нежелание госорганов рассматривать проблему в комплексе

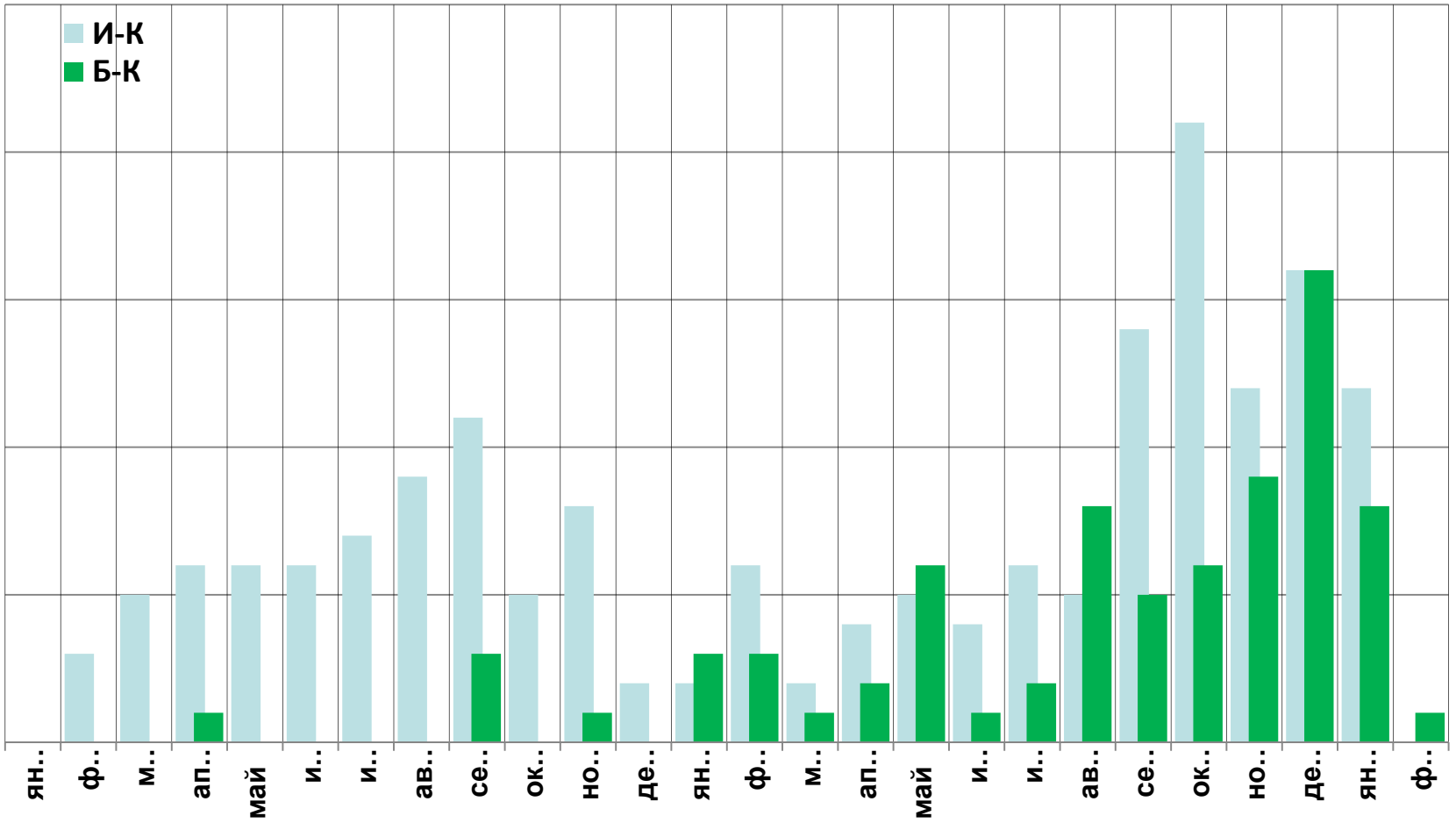
- Формирование ощущения безнаказанности и «лёгких денег»
- Массовое распространение инструментария и массовое вовлечение в преступную деятельность
- Вывод финансовых средств в теневой оборот
- Ущерб государству
- Повышенные риски

Особенности

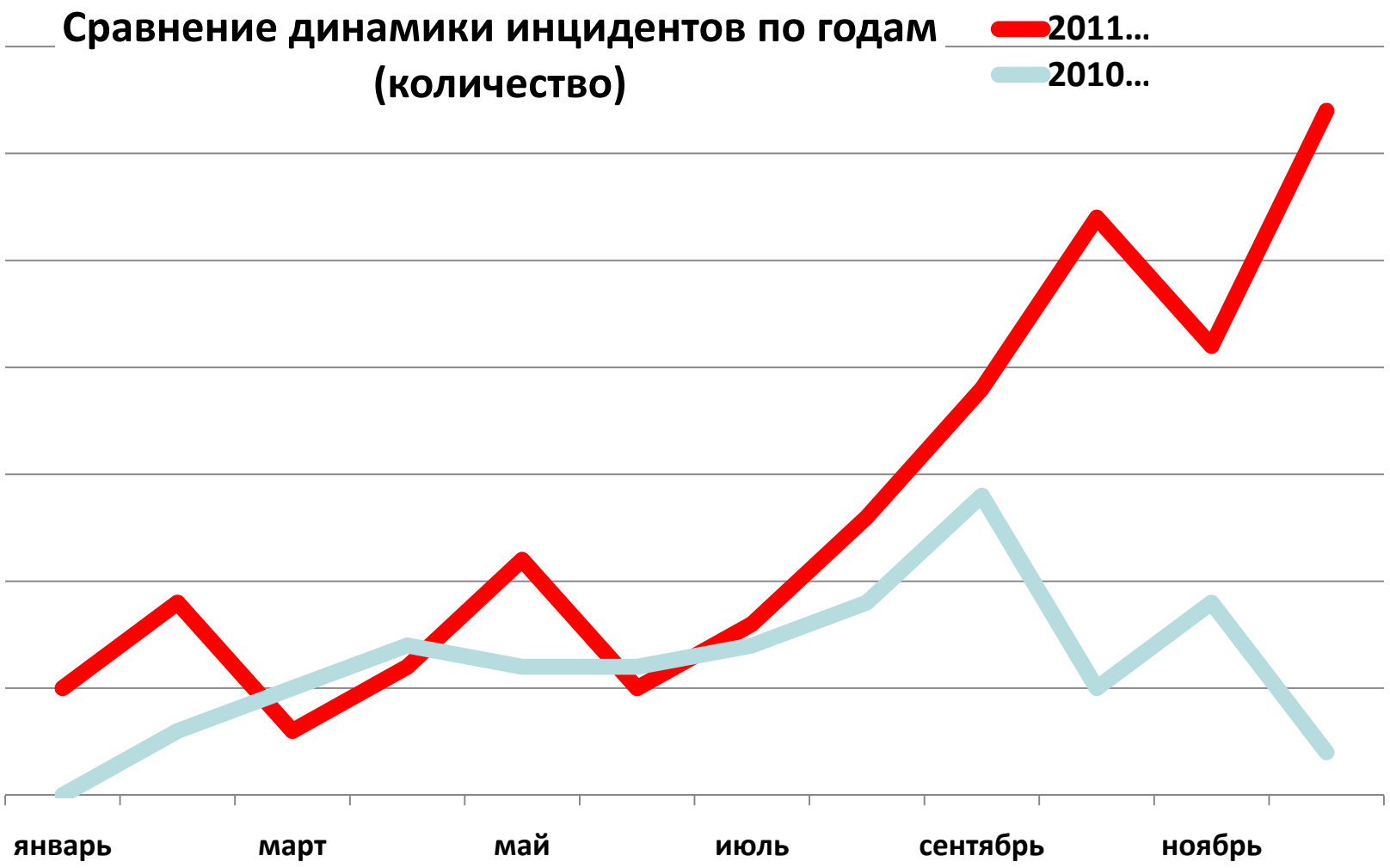
- Хищения и вывод средств происходят в разных регионах
- Вывод похищенных средств через средства мобильного управления счетом
- Трансграничность преступного сообщества
- Увеличение количества хищений со счетов физических лиц
- Отсутствие единых стандартов и требований к платежным приложениям

Динамика атак

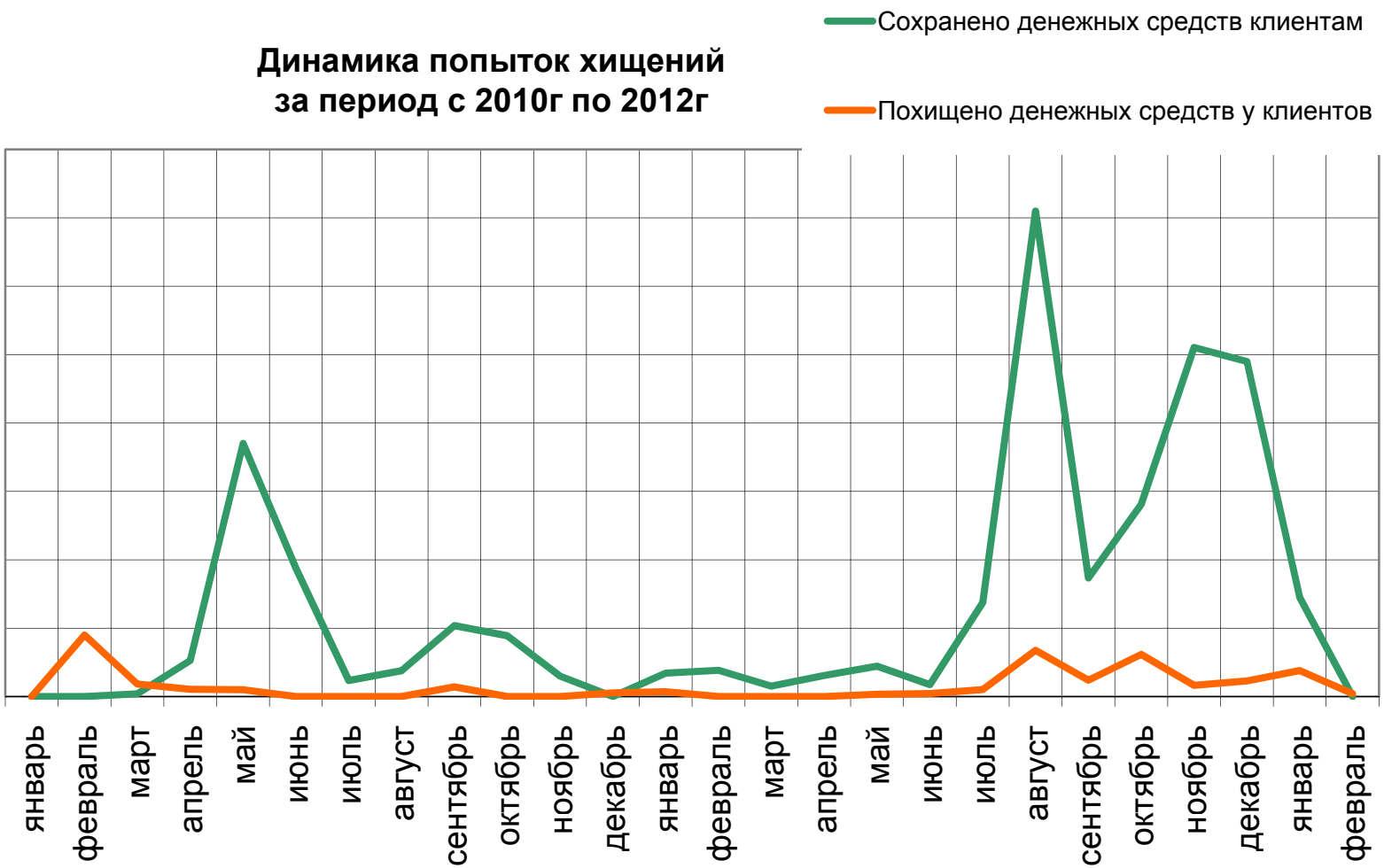
Атакам подвергаются пользователи «толстого» и «тонкого» клиента



Темпы инцидентов



Соотношения сохраненных и похищенных денежных средств

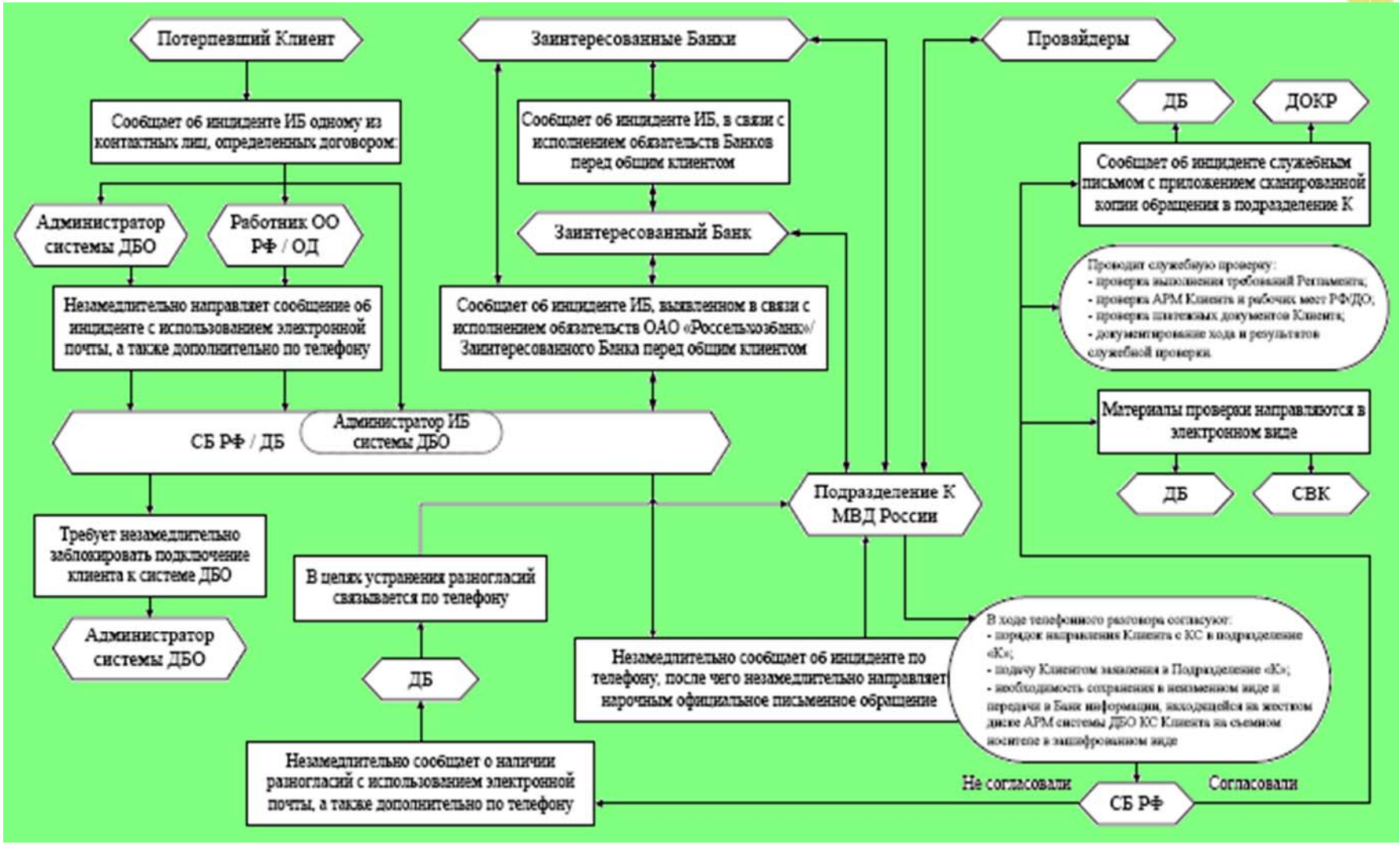


Основания и принципы осуществления неотложных мероприятий кредитной организации при инцидентах в ДБО

В соответствии с федеральным законодательством, противоправные действия злоумышленников, направленные на хищение денежных средств клиентов коммерческой организации при дистанционном банковском обслуживании, подпадают под признаки состава преступлений, предусмотренных нормами статей 158, 272, 273 Уголовного кодекса Российской Федерации

При разборе инцидентов, связанных с хищением денежных средств клиентов при ДБО, установлена примерная схема неотложных организационных действий, основанная на анализе попыток хищения

Примерная схема неотложных мероприятий



Заинтересованные стороны

Неотложные организационные мероприятия должны осуществляться следующими заинтересованными сторонами

- **Взаимодействие кредитной организации с потерпевшим клиентом**
- **Взаимодействие между заинтересованными внутренними подразделениями кредитной организации**
- **Взаимодействие между заинтересованными кредитными организациями**
- **Взаимодействие кредитной организации (кредитных организаций) с правоохранительными органами**
- **Взаимодействие правоохранительных органов с провайдерами**

Типовое обращение в территориальные органы МВД

Приложение
к Порядку разбора инцидентов при дистанционном
банковском обслуживании, связанных с использованием
в ОАО «Россельхозбанк» системы «Банк-Клиент» («Интернет-Клиент») № 296-П
(приказ ОАО «Россельхозбанк» от 25.06.2009 № 244-ОД)
(в редакции приказа ОАО «Россельхозбанк» от 19.05.2010 № 172-ОД)

Открытое акционерное общество "Российский Сельскохозяйственный банк"
N-СКИЙ РЕГИОНАЛЬНЫЙ ФИЛИАЛ
(N-ский РФ ОАО "РОССЕЛЬХОЗБАНК")
ул. N-ская, д.1, г. N-ск, N-ская область, XXXXXX
тел.(300) 999-88-77, факс (000) 222-33-22, E-mail:xxxx@xxxx.ru
ОКПО 59650622, ОГРН 1027700300000
ИНН / КПП 8888888888 / 535555535

_____№ _____

(должность)
(звание)
(ФИО)
(почтовый адрес)

Об оказании содействия

Уважаемый (имя, отчество)!

Открытое акционерное общество «Российский Сельскохозяйственный банк», являющееся по сути государственным банком, 100% акций которого принадлежат государству, обеспечивающее выполнение государственной программы поддержки сельского хозяйства Российской Федерации, просит оказать содействие в розыске злоумышленников и противодействии преступным группировкам, совершивших хищение денежных средств со счета клиента Банка.

Так, (дата) года с расчетного счета № (номер счета), принадлежащего (наименование клиента), открытом в N-ском региональном филиале ОАО «Россельхозбанк», посредством удаленного доступа к информационным ресурсам клиента с использованием электронной системы «Банк-Клиент» («Интернет-Клиент») неизвестными лицами незаконно осуществлено списание денежных средств в сумме (сумма) руб. на счет № (номер счета)
принадлежащий (наименование клиента), открытый в (наименование Банка, адрес).

Клиент N-ского регионального филиала ОАО «Россельхозбанк», (наименование клиента), был вынужден обратиться в правоохранительные органы (отдел «К») по месту регистрации.

Указанные противоправные действия злоумышленников подпадают под признаки состава преступлений, предусмотренных нормами статей 158, 272 Уголовного кодекса Российской Федерации, и были совершены с использованием инновационных технологий.

В данных обстоятельствах проблема хищения денежных средств со счета клиента N-ского регионального филиала ОАО «Россельхозбанк» посредством инновационных технологий касается не только защиты клиентов Банка, а затрагивает безопасность государства в целом, и отсутствие консолидированного противодействия государственных органов преступным группировкам, деятельность которых направлена на совершение преступлений в сфере охраняемой законом компьютерной информации, в условиях кризиса может привести к дестабилизации банковской системы Российской Федерации.

Для сведения направляем имеющиеся материалы.

Директор филиала **(инициалы, фамилия)**

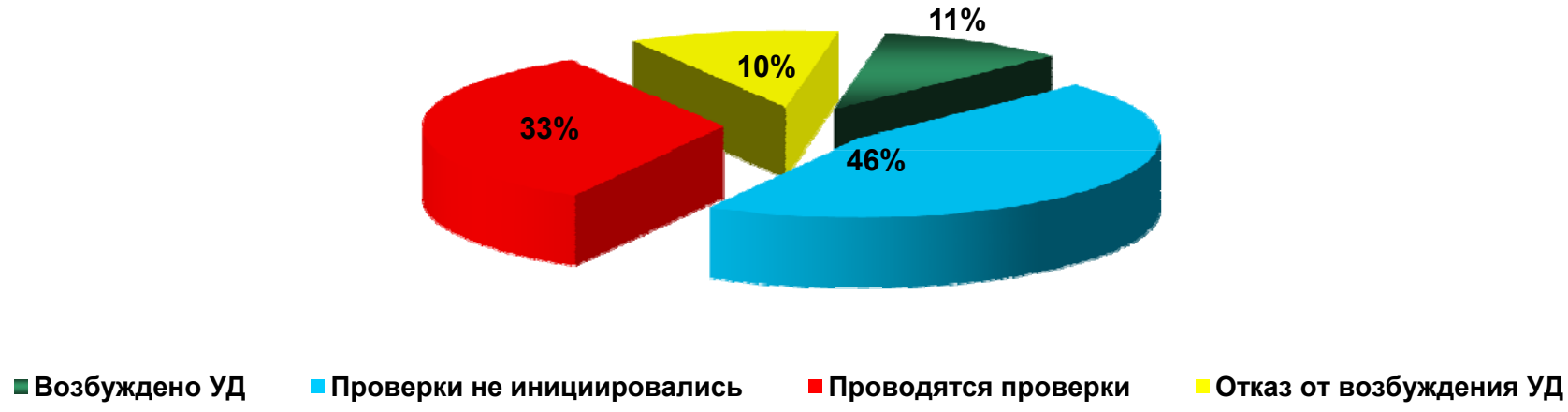
Исп. **(ФИО)**
тел.: (___) _

Разработка совместных мер

- **Распределение «зон ответственности»:**
  - **«Зона ответственности кредитной организации»**
  - **«Зона ответственности правоохранительных органов»**
- **Меры по противодействию предполагаемым или реальным фактам общеуголовных проявлений в банковской системе**
- **Меры по созданию так называемой «прямой/горячей линии» между кредитной организацией и органами внутренних дел**
- **Участие в формировании централизованного/регионального «банка данных» о физических лицах и организациях различных форм собственности, недобросовестных участниках кредитно-денежных отношений**

Результаты обращений клиентов в органы МВД

Уголовные дела



Результаты обращений клиентов в органы МВД

«УТВЕРЖДАЮ»
Начальник СКМ ОВД по Котельничскому району
майор милиции С. А. Кхххххв

«ХХ» хххххх 20хх г.
«ХХ» часов «ХХ» минут

ПОСТАНОВЛЕНИЕ
об отказе в возбуждении уголовного дела

«ХХ» хххххх 20хх г. г. Котельнич
«ХХ» часов «ХХ» минут

О/У ОБЭП ОВД по Котельничскому району старший лейтенант милиции К. А. Мхххв, рассмотрев материалы проверки КУСП № 3881 от «ХХ» хххх 20хх г., о том, что неизвестное лицо путем мошенничества завладело принадлежащим СКПК «Кхххххй Рхххс» денежными средствами в сумме ХХ.ХХХ рублей, направив «ХХ» хххх 20хх г. в КБ «Рхххххххххк» фиктивное платежное поручение от имени СКПК «Кхххххй Рхххс».

УСТАНОВИЛ

«ХХ» хххх 20хх г. в ОВД по Котельничскому району обратился председатель СКПК «Кхххххй Рхххс» Рххн С. Л. о том, что неизвестное лицо путем мошенничества завладело принадлежащим СКПК «Кхххххй Рхххс» денежными средствами в сумме ХХ.ХХХ рублей, направив «ХХ» хххх 20хх г. в КБ «Рхххххххххк» фиктивное платежное поручение от имени СКПК «Кхххххй Рхххс».

В ходе проверки было установлено, что «ХХ» хххх 20хх г. около 12 часов по интернет сети в системе мобильный банк КБ «Рхххххххххк» поступило платежное поручение № 1ХХ в сумме ХХ.ХХХ рублей от имени СКПК «Кхххххй Рхххс». Бухгалтер КБ «Рхххххххххк» Сххххха О. Э. рассмотрела данное поручение. В это же время в офис КБ «Рхххххххххк» позвонила неизвестная женщина, которая не представилась, она только пояснила, что является сотрудником Кхххххго регионального, а чего именно – не пояснила. Женщина попросила быстрее рассмотреть и направить для перечисления денежных средств платежное поручение № 1ХХ от «ХХ» хххх 20хх г. Бухгалтер офиса КБ «Рхххххххххк» Сххххха О. Э. рассмотрела, направила его, для перечисления денежных средств в Кхххххий региональный офис КБ «Рхххххххххк». Денежные средства были перечислены в ХХХ-24 г. Москва на лицевой счет гр. Нехххко Ахху Охххны. Данное преступление было совершено с использованием системы интернет.

В настоящее время установить лицо, незаконно осуществившее неправомерный доступ в систему данных СКПК «Кхххххй Рхххс», и установить адреса мест, куда перечислены денежные средства, и кто в дальнейшем и каким образом обналичил данные денежные средства, не представляется возможным.

Таким образом, в настоящее время в действиях неизвестного лица отсутствует состав преступления, предусмотренный ст. 159 ч. 3 УК РФ, т.к. оно не установлено и неизвестно его отношение к содеянному.

На основании изложенного и руководствуясь п. 2 ч. 1 ст. 24 и ст. ст. 144, 145 УПК РФ

ПОСТАНОВИЛ

1. Отказать в возбуждении уголовного дела за отсутствием в действиях неизвестного лица состава преступления, предусмотренный ст. 159 ч. 3 УК РФ.

2. Копии настоящего постановления направить Котельничскому межрайонному прокурору, а также председателю СКПК «Кхххххй Рхххс» Рххну С. Л., разъяснив последнему, что данное постановление может быть обжаловано Котельничскому межрайонному прокурору, или в суд, в порядке ст. 124, 125 УПК РФ.

О/У ОБЭП ОВД по Котельничскому району
ст. лейтенант милиции К. А. Мхххв

Копии настоящего постановления направлены Котельничскому межрайонному прокурору и председателю СКПК «Кхххххй Рхххс» Рххну С. Л.

«ХХ» хххххх 20хх г. «ХХ» часов «ХХ» минут

О/У ОБЭП ОВД по Котельничскому району
ст. лейтенант милиции К. А. Мхххв

Общие цели

- **Неотвратимость наказания**
- **Заинтересованность правоохранительных органов в результатах расследований**
- **Консолидация государственных органов, правоохранительных органов, операторов связи и банковского сообщества**
- **Повышение осведомленности в области информационной безопасности на государственном уровне**

Общие меры по минимизации рисков

- **Своевременное информирование клиентов о требованиях безопасности, выполнение которых обязательно для предотвращения хищений денежных средств злоумышленниками**
- **Разработка типовых рекомендаций по обеспечению информационной безопасности систем ДБО**
- **Разработка типового порядка разбора инцидентов, который позволяет оперативно получить всю необходимую информацию для передачи в территориальные подразделения «К» органов внутренних дел**
- **Разработка типового порядка взаимодействия с территориальными подразделениями «К» органов внутренних дел при разборе инцидентов**

Спасибо за внимание

А.Ф. Беликов

заместитель начальника управления информационной безопасности

ОАО «Россельхозбанк»

Belikov@rshb.ru

РоссельхозБанк

С опытом банковского сообщества, в том числе ОАО «Россельхозбанк», можно ознакомится в отраслевом журнале «BIS-Journal»

http://www.ib-bank.ru/bis/