Некоммерческое партнерство «Национальный платежный совет» (НП «НПС»)

«Социальное мошенничество в платежной индустрии и способы противодействия ему: нужны ли изменения в законодательство?»

Деловой завтрак
«ИТ безопасность бизнеса»
7 июня 2018 года, Москва

Андрей Лисицын
Советник
Председателя Правления
НП "НПС"

Статистика по рискам несанкционированных операций

рост числа несанкционированных операций, осуществленных посредством сети "Интернет" и устройств мобильной связи

По сведениям Банка России по несанкционированным транзакциям

по платежным картам (2016): 300 тыс. транзакций на 1 млрд руб

по счетам юр лиц (2016): 717 транзакций на общую сумму 1,89 млрд. рублей (50% «успешных»)

Ист: http://sozd.parliament.gov.ru/download/B34306B2-26CE-46F9-AE56-298040AE9C3D

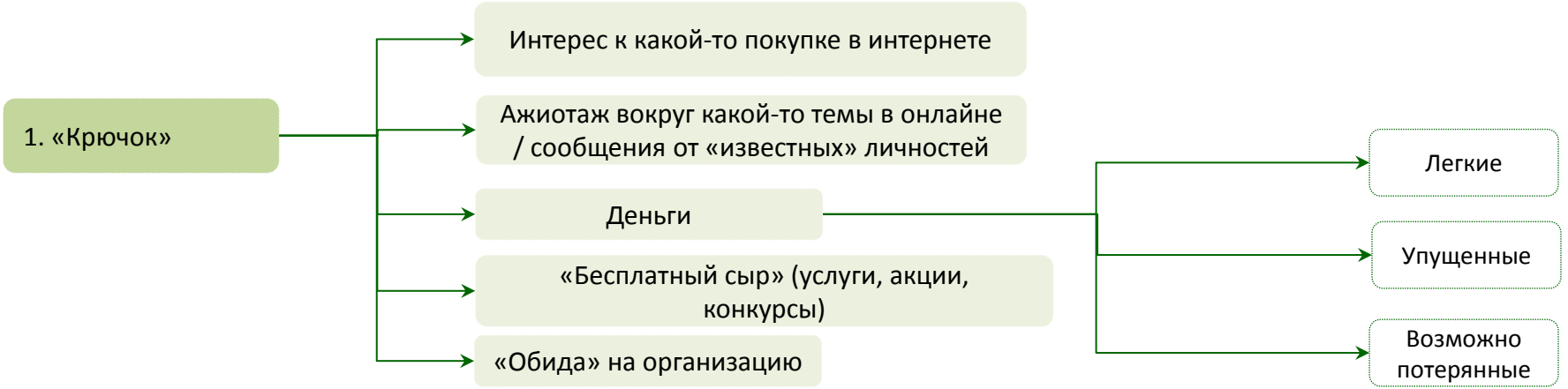
ИТ безопасность и социальная инженерия

Социальная инженерия → метод получения необходимого доступа к информации или денежным средсвам, основанный на особенностях психологии людей

Факторы применения
- дешевизна средств
- социальные проблемы (отсутствие работы, бедность и т.д.)
- трудности выявления и пресечения в связи с использованием удаленных каналов

Влияние на ИТ безопасность бизнеса
- снижение эффективности организационно-технически мер, а сл-но, затрат на них
  - человеческий фактор внутри бизнеса
  - человеческий фактор на стороне клиента / контрагента
- снижение лояльности клиентов / котрагентов
- риски внедрения / применения новых удаленных сервисов

Механика социального мошенничества в платежах



2. Общение с применением методов психологического воздействия

3. Использование полученной информации для доступа к системам удаленного обслуживания

4. Перевод денежных средств на подконтрольные счета / кошельки

5. Отмывка средств

Формы социального мошенничества в платежах

Склонение к добровольному перечислению средств → «Мама я попал в беду»

Склонение к предоставлению сведений для доступа к удаленному каналу обслуживания с целью недобросовестного получения денежных средств путем его использования от имени легального пользователя

- Открытое → «Вам сейчас придет код, сообщите мне его…»
- Закрытое
  - Рассылки материалов
  - Фишинг
  - Скимминг

Рекомендации специалистов (пример по кейсу с соц. сетями)

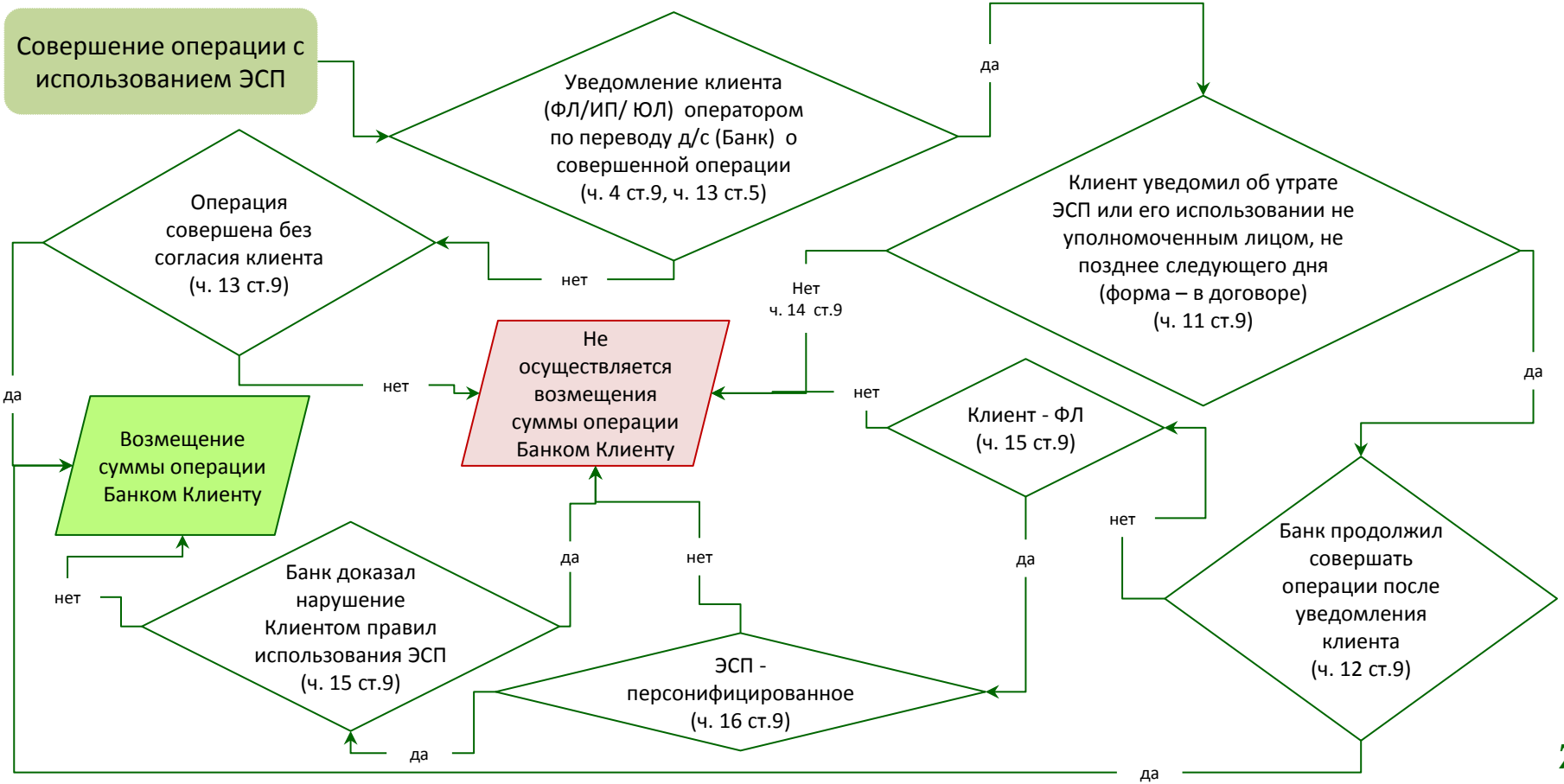
Рекомендует*:

1. Никому и ни при каких обстоятельствах не называйте реквизиты банковской карты. Сотрудники банка никогда не запрашивают эти данные.
2. Ни под каким предлогом никому не сообщайте SMS-коды, направленные от банка.
3. Никому не сообщайте конфиденциальные данные, использующиеся для доступа к личному кабинету онлайн-банкинга.
4. Если ссылок на официальные сообщества банка в социальных сетях нет на официальном сайте, не используйте эти сообщества.
5. При возникновении проблем с оказываемыми банковскими услугами лучше позвонить напрямую в банк по указанному номеру на официальном сайте банка или на вашей банковской карте.
6. Общаясь с клиентами в социальных сетях, сотрудники банка никогда не переводят общение «в личку» и не пишут персональных сообщений. Они консультируют только в официальном сообществе, в открытых обсуждениях.
7. Имейте ввиду, что сотрудники банка оказывают консультацию только по общим вопросам, что снимает необходимость персонализации клиента.
8. Стоит учесть, что сотрудники банка никогда не торопят клиента с решением, задача же мошенников – не дать времени проанализировать ситуацию.
9. Самое главное: в случае возникновения малейших сомнений при консультировании в сообществе банка необходимо прекратить общение и позвонить в банк.

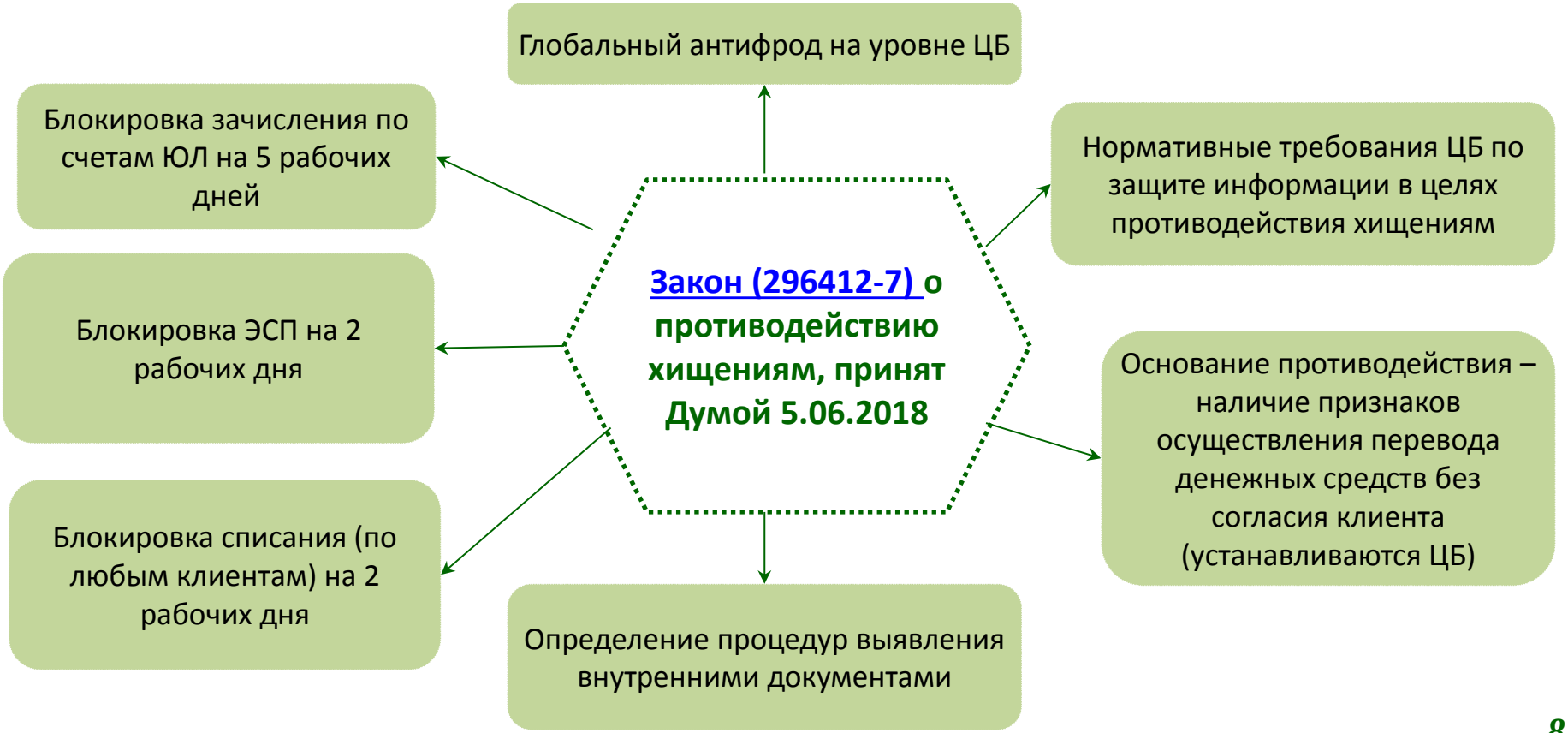
___

Ист.: https://www.group-ib.ru/blog/social

Текущий алгоритм защиты пользователей удаленных каналов платежного обслуживания (электронных средств платежа)



Законодательные изменения на выходе



Чего не хватает в регулировании системы противодействия социальному мошенничеству в платежах

Спасибо за внимание !

Андрей Лисицын
+7(929)944-1010
laj@npc.ru