МОШЕННИЧЕСТВО В СФЕРЕ ЭЛЕКТРОННЫХ БАНКОВСКИХ СИСТЕМ

Подготовили: студенты 21 группы
направления «Экономическая безопасность»
Мурзагалеева Айгерим
Маликова Екатерина

Платежная система-это совокупность правил, договорных отношений, технологий, методик расчета, внутренних и внешних нормативных актов, которые позволяют всем участникам производить финансовые операции и расчеты друг с другом.

Банки России предлагают следующий перечень электронных банковских услуг:

- HOME BANKING (домашний банк)
- Система "Клиент-банк"
- Интернет-банкинг
- WAP-банкинг

Причины резкого возрастания числа интернет-мошенничеств

Субъективные причины

Объективные причины

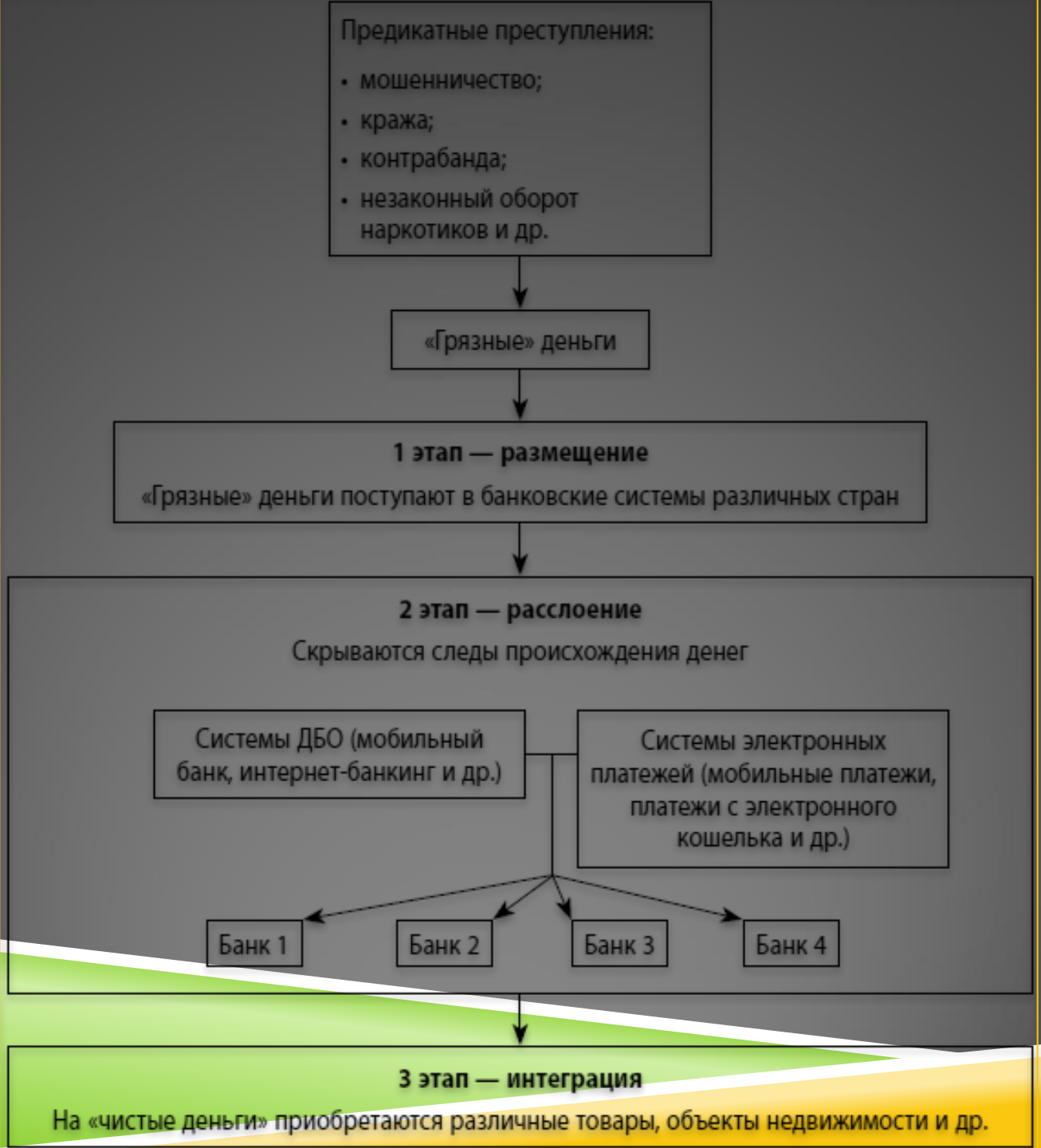
Банк обязан выполнять требования по обеспечению защиты информации следующих внешних по отношению к финансовой организации нормативно-правовых актов:

1. Федеральный закон РФ от 27 июля 2006 г. № 152-ФЗ "О персональных данных";

2. Федеральный закон РФ от 7 августа 2001 г. № 115-ФЗ "О противодействии легализации доходов, полученных преступным путем";

3. Стандарт международной платежной системы VISA PA DSS

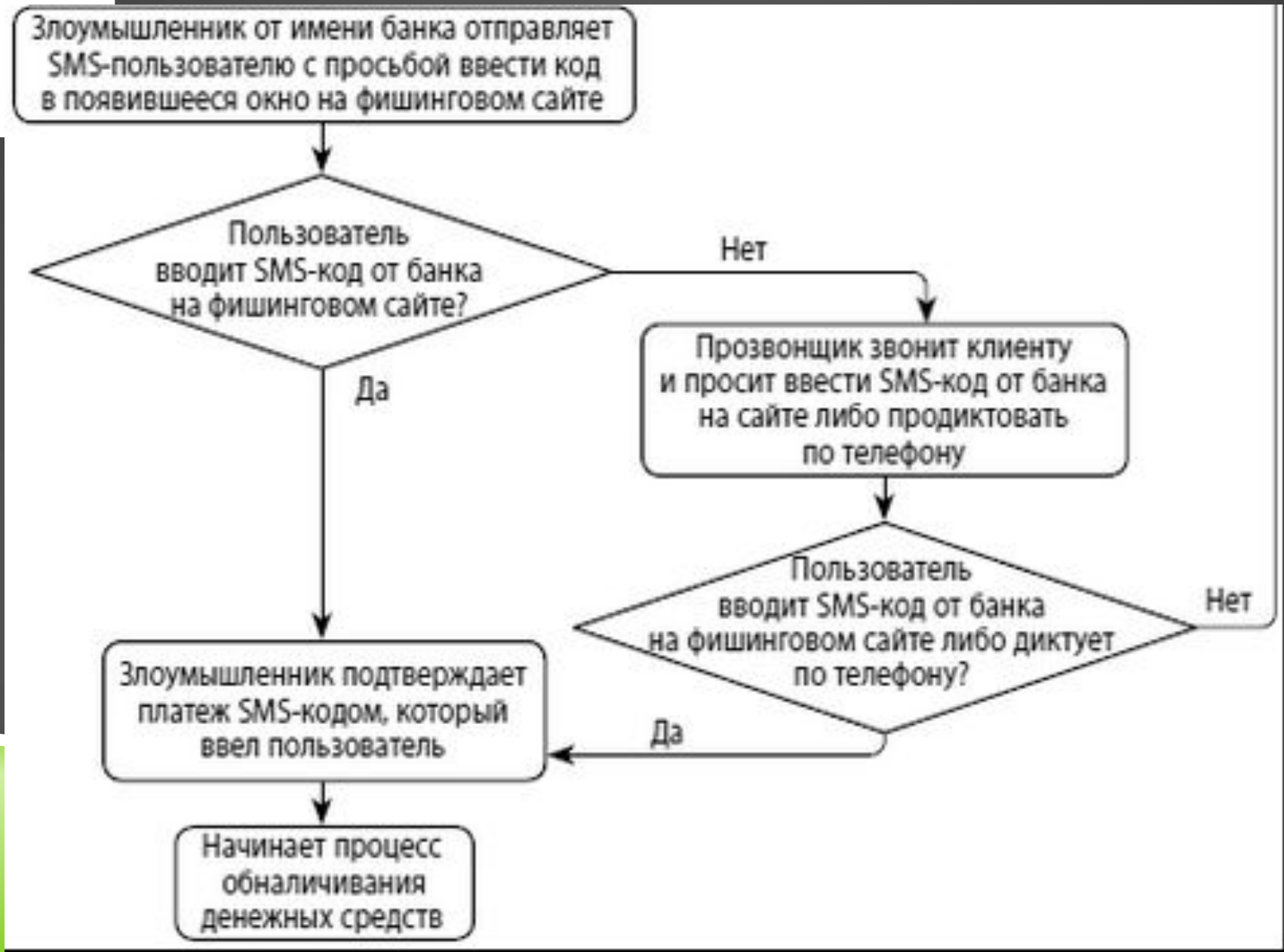
4. Рекомендации ЦБ РФ, направленные циркулярным письмом Московского ГТУ Банка России № 33-00-18/3183 от 25.01.2010 г. "О рекомендациях для кредитных организаций по дополнительным мерам информационной безопасности при использовании систем интернет-банкинга".


Предикатные преступления:
• мошенничество;
• кража;
• контрабанда;
• незаконный оборот наркотиков и др.
«Грязные» деньги
1 этап — размещение
«Грязные» деньги поступают в банковские системы различных стран
2 этап — расслоение
Скрываются следы происхождения денег
Системы ДБО (мобильный банк, интернет-банкинг и др.)
Системы электронных платежей (мобильные платежи, платежи с электронного кошелька и др.)
Банк 1
Банк 2
Банк 3
Банк 4
3 этап — интеграция
На «чистые деньги» приобретаются различные товары, объекты недвижимости и др.

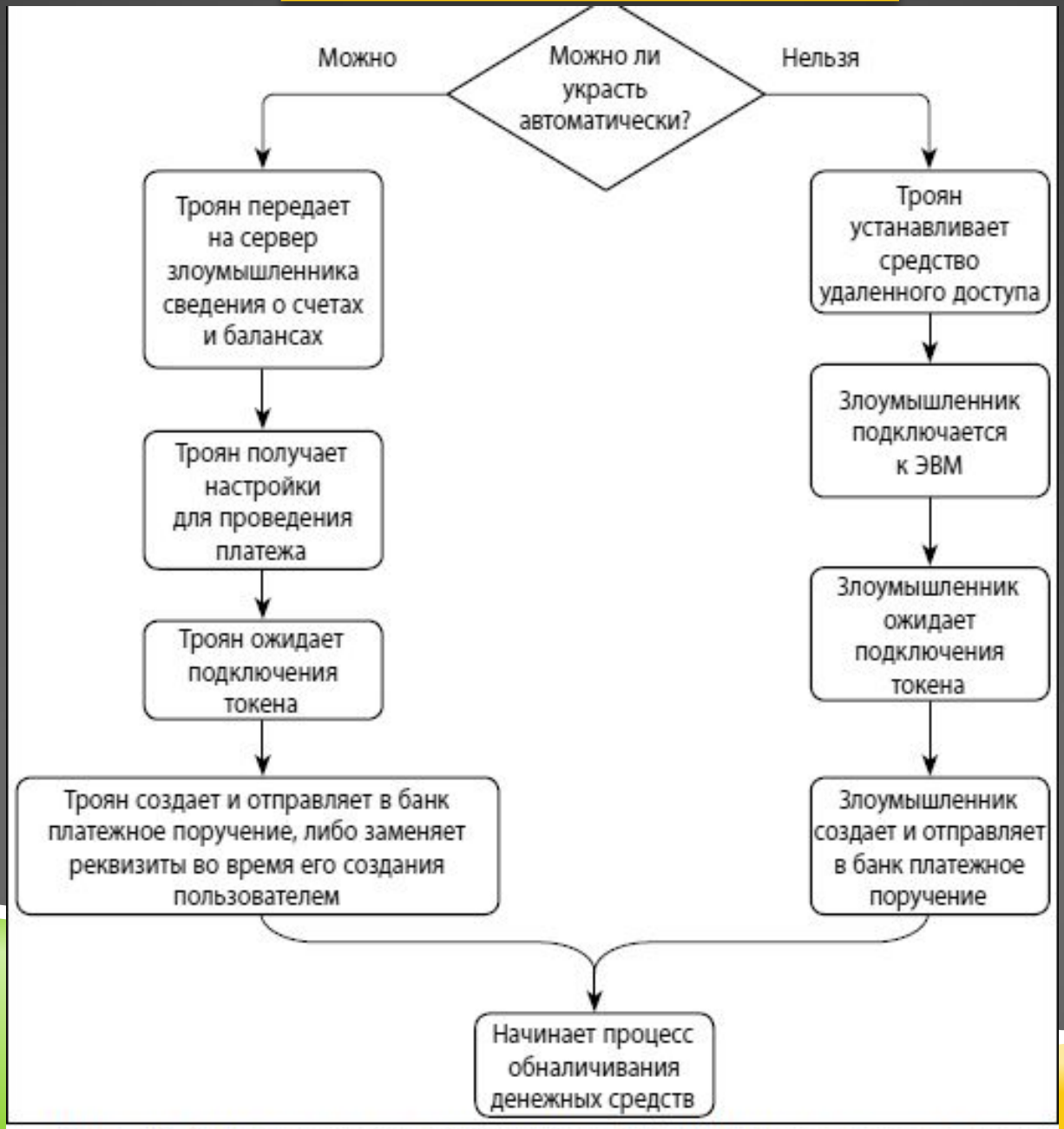
Основные виды правонарушений

- хищение денежных средств со счетов клиентов
- кража персональных данных
- высокотехнологичная операция

«Фишинг» схема



«Троянский конь» схема



Признаки, по которым косвенно можно определить, что происходит что-то неладное:

Нетипичное «поведение» клиента - операции производятся с другого IP-адреса, в странное время или списывается необычная сумма

Могут производиться нетипичные переводы со счетов как юр. лиц, так и физ. лиц на карточные счета физ. лиц.

Многократный отказ в проведении транзакции за короткий период и одновременное, либо за короткий промежуток времени, снятие наличных с одной карты в разных регионах,кроме того, это уже опоминавшееся переводы на счета электронных денег.

Введение условий использования карточных продуктов вне мест постоянного проживания клиентов дает хороший эффект.

Полный перечень мер безопасности для клиентов.

- Банк никогда не запрашивает пароли для отмены операций.
- При получении SMS с одноразовым паролем внимательно ознакомьтесь с его содержанием.
- Проверяйте, что установлено защищенное SSL-соединение с официальными сайтами услуги.
- Ни при каких обстоятельствах не разглашайте свой пароль никому, включая сотрудников банка
- Не используйте сомнительные места и компьютеры для работы с интернет-банком.
- Пользуйтесь дополнительными возможностями системы по повышению уровня безопасности

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ:

1. Консультант Плюс. Федеральный закон от 27.06.2011 N 161-ФЗ «О национальной платежной системе»
2. Реестр операторов платёжных систем на сайте России. Режим доступа http://www.cbr.ru
3. Федеральный закон Российской Федерации от 27 июня 2011 г. N 161-ФЗ г. «О национальной платёжной системе»
4. «Мошенничество в платежных системах». Режим доступа: http://protect.htmlweb.ru/pcard.htm
5. « Платежная система». Режим доступа: http://www.grandars.ru/student/bankovskoe-delo/platezhnaya-sistema.html

Спасибо за внимание!!!