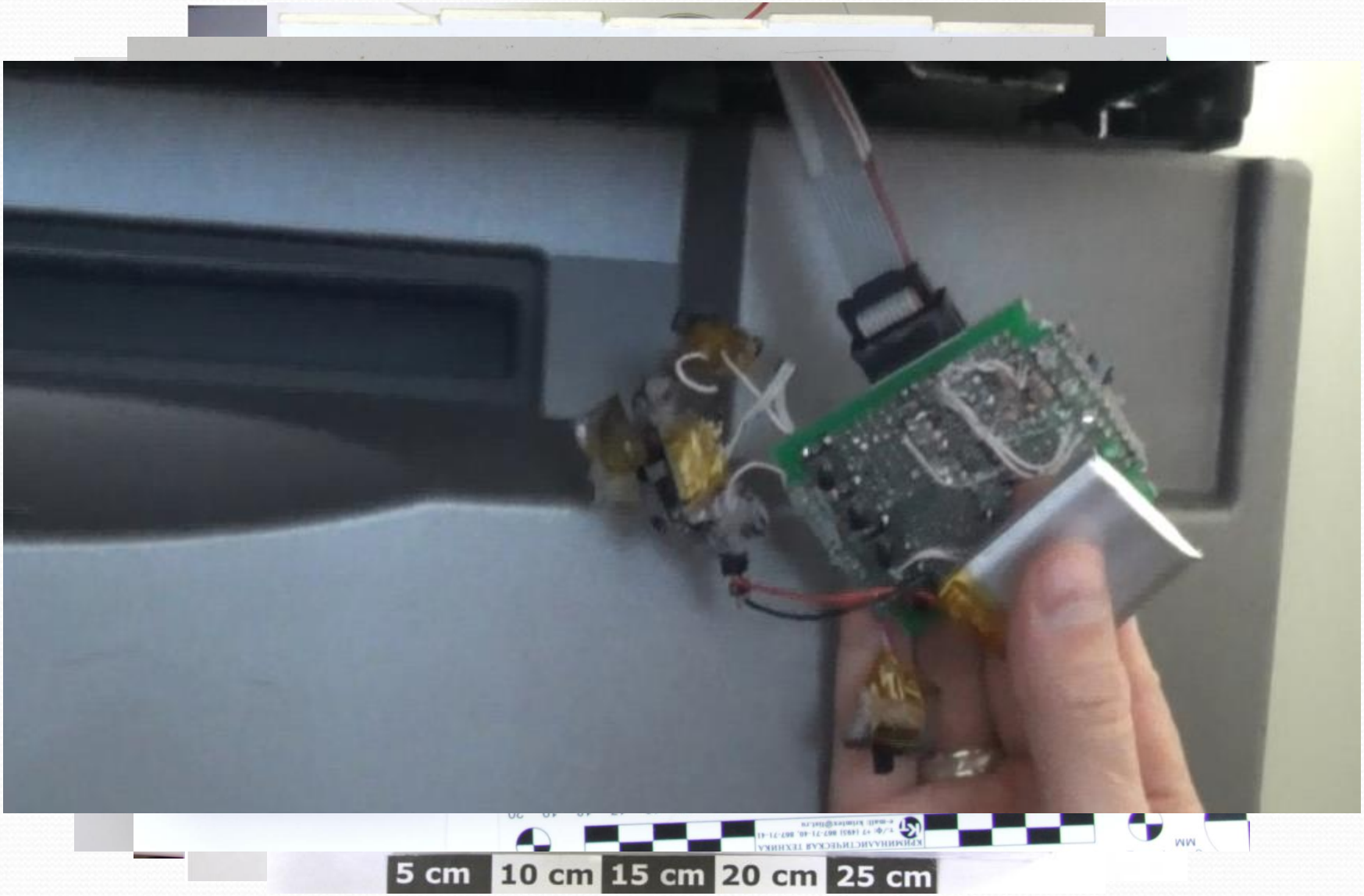
# Практические аспекты экспертного сопровождения раскрытия и расследования преступлений в сфере дистанционного банковского обслуживания

# Тенденции

- Резкое снижение числа скимминговых устройств (повышение защищенности или боязнь санкций ЦБ и имиджевых потерь?);
- Увеличение числа BlackBox;
- Снижение числа мобильных телефонов (повышение качества программ мобильного банкинга, работа с клиентами) (возможно временное);
- Увеличение числа системных блоков, НЖМД (низкий уровень безопасности в организациях и кредитных организациях, повышение квалификации сотрудников правоохранительных органов);
- Вещевой кардинг (реальный и Интернет).

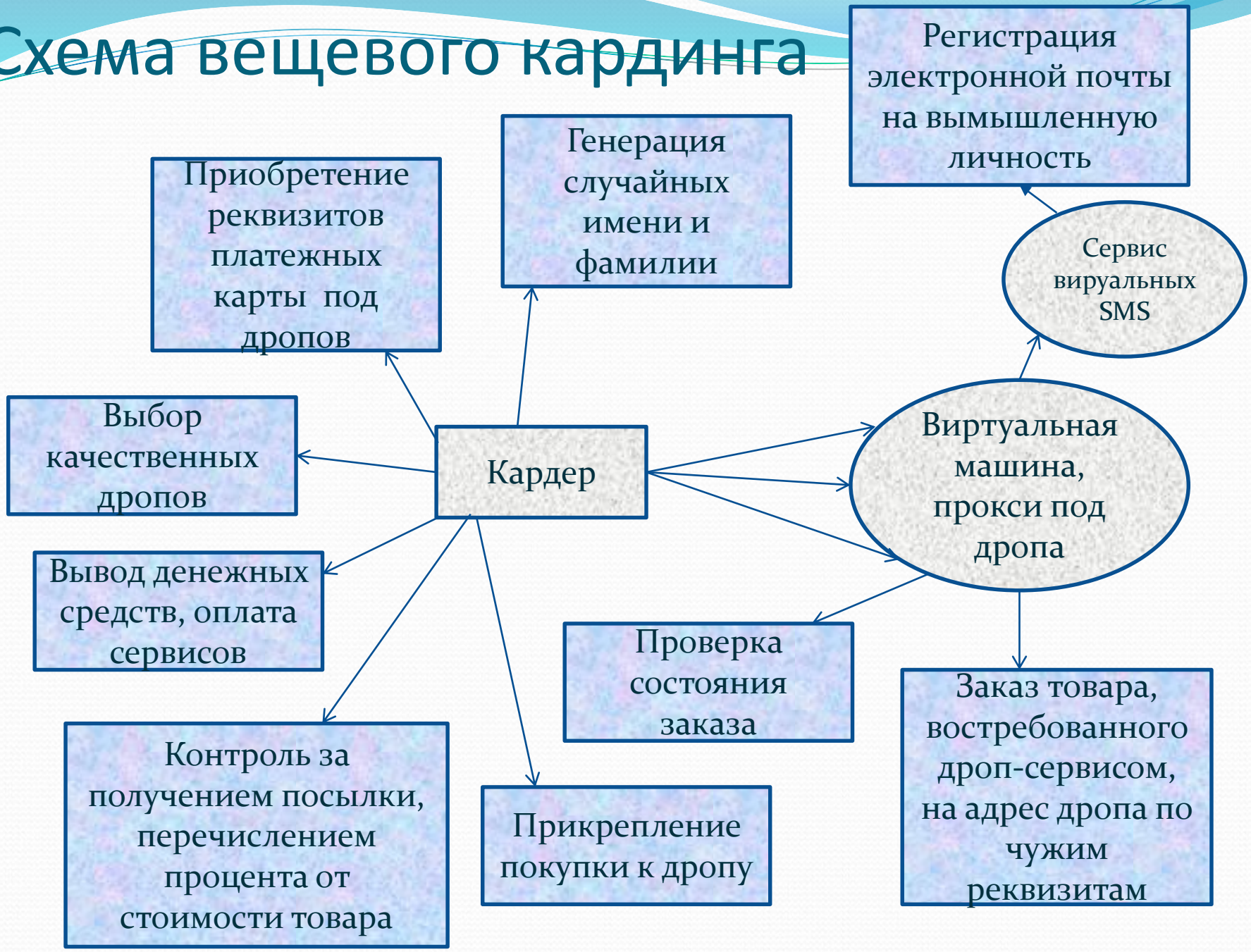
# BlackBox



# Вещевой Интернет-кардинг

- Дроп-сервисы
  - Предоставление дропов
  - Скупка товаров
- Ресурсы, торгующие реквизитами платежных карт
- Интернет –магазины
- Бесплатные почтовые сервисы
- Средства защиты информации, подмены IP-адресов
- Ресурсы по обмену электронных денег
- Сервисы по созданию виртуальных личностей
- Сервисы виртуальных SMS

# Схема вещевого кардинга



# Проблемы доказывания

- Держатели карт, магазины, дропы  находятся на территории иностранного государства
- Страхование вкладов

- Отсутствие потерпевших
- Квалификация по формальному составу (ст. 187 УК РФ)

# Объекты, которые могут быть исследованы в рамках компьютерной и радиотехнической экспертиз (ДБО)

«**Банкоматные» мошенничества:**

- скимминговые устройства;
- средства вычислительной техники, мобильные устройства;
- пластиковые карты;
- оборудование для изготовления скимминговых устройств, пластиковых карт и др.

**Мошенничества, совершенных с использованием «социальной инженерии»:**

- устройства, на которых могут остаться следы общения потерпевшей стороны с преступником (мобильные устройства, СВТ и др.)

**Преступления с участием сотрудников организации:**

- Личные и рабочие компьютеры, мобильные устройства, на которых могут содержаться сведения о преступлении;
- Средства вычислительной техники, на которых могут содержаться следы преступления.

# Объекты, которые могут быть исследованы в рамках компьютерной и радиотехнической экспертиз (ДБО)

**Заражение компьютера на стороне клиента:**

- компьютеры, мобильные устройства клиента, на которых могут содержаться следы преступления, программное обеспечение, использованное преступниками;
- средства вычислительной техники, используемые преступником (-ами) для подготовки и совершения преступлений.

**Заражение мобильного устройства:**

- мобильные устройства клиента, на которых могут содержаться следы преступления, программное обеспечение, использованное преступниками;
- средства вычислительной техники, используемые преступником (-ами) для подготовки и совершения преступлений.

**Компрометация (заражение) кредитной организации:**

- образы компьютеров кредитной организации, на которых могут содержаться следы преступления, программное обеспечение, использованное преступниками;
- образы оперативной памяти компьютеров кредитной организации, на которых могут содержаться следы преступления;
- средства вычислительной техники, используемые преступником (-ами) для подготовки и совершения преступлений.

# Следы преступления (ДБО)

- сведения о платежных картах, данных клиента, pin-кодах, кодах подтверждения, именах и паролях доступа, платежных поручениях;
- сведения из протоколов работы программ, фиксирующих различные аспекты работы пользователей (создания, передачи, удаления, изменения информации);
- сведения из  баз данных, фиксирующих распоряжения, передаваемые клиентами удаленным образом;
- сведения о программном обеспечении, использованном преступником (-ами) для подготовки и совершения преступлений, его появлении на средстве вычислительной техники и работе.

**Отражаются в:**

- электронной почте, SMS-сообщениях, переписке в мессенджерах и т.п.;
- содержании системных, временных, специализированных файлов, свойствах и метаданных файлов данных и т.п.;
- файлах данных;
- и т.д.

# Информация, необходимая эксперту для производства экспертизы

**из кредитной организации / банка:**

- как и когда установлен факт кражи / мошенничества (заявление клиента, фиксация инцидента службой безопасности организации, сообщение от правоохранительных органов и т.д.);
- об операциях, произведенных потерпевшим (сумма, точное время, способ оплаты, номера реквизитов отправителя и получателя, номера платежных карт, номера телефонов, IP-адреса, IMEI-номера и т.д.);
- особенности организации ДБО с потерпевшим (привязка к абонентскому номеру, номеру аппарата, IP или MAC адресу, наличие ограничений на совершаемые действия и т.д.);
- об организации ДБО в кредитной организации; (при компрометации сети)

**от оператора сотовой связи или провайдера:**

- о принятых и переданных SMS-сообщениях (биллинговая информация, в том числе номер телефона + IMEI);
- о телефонных соединениях (биллинговая информация, в том числе номер телефона + IMEI);
- о сетевом трафике.

**от обвиняемого:**

- вся информация, которую он сообщит о преступлении.

# Некоторые замечания

- Объективно  не существует специалистов в сфере обработки компьютерной информации, которые во всех случаях без дополнительных сведений могли бы ориентироваться на месте проведения следственного действия, давать грамотные советы и помогать в изъятии компьютерной информации;
- Зафиксировать информацию, в которой могут содержаться сведения о преступлении, его следовая картина (снять образы НЖМД, образы оперативной памяти) и только потом заниматься восстановлением системы (проверять антивирусом, форматировать носители, переустанавливать операционные системы и др.)
- Для сотрудников правоохранительных органов максимально подробно описать правила обработки и хранения информации в системе ДБО, особенности систем безопасности и др.

?