



НАЦИОНАЛЬНЫЙ БАНК КАЗАХСТАНА

# Обеспечение информационной безопасности по электронным финансовым услугам

# Содержание

## 1 Инфраструктура электронных финансовых услуг

---

## 2 Основные риски

---

## 3 Тренды и меры по предупреждению мошенничества и обеспечению безопасности по электронным платежным инструментам

---

## 4 Единый Центр реагирования

---

## 5 Направления дальнейшей деятельности

---

## 6 Законодательные меры



# Инфраструктура электронных финансовых услуг



**Банкоматы**

**POS – терминалы**

**Интернет-банкинг**

- компьютеры;

- смартфоны;

- планшеты

**Банковские киоски**

**Мобильный банкинг**

**Платежные терминалы**



# Основные риски

## Естественные угрозы

вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека

## Искусственные угрозы

вызванные деятельностью человека. Среди них можно выделить:

- непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п.

- преднамеренные (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников)

## Система предоставления электронных финансовых услуг (ЭФУ)

Сеть обслуживания банка



Каналы передачи информации по операциям



# Основные риски

- ✓ низкое обеспечение конфиденциальности и целостности передаваемых данных;
- ✓ недостаточный уровень проверки участников соединения;
- ✓ недостаточная реализация или некорректная разработка политики безопасности;
- ✓ отсутствие или недостаточный уровень защиты от несанкционированного доступа (антивирусы, контроль доступа, системы обнаружения атак);
- ✓ существующие уязвимости используемых операционных систем (ОС), ПО, веб-систем и сетевых протоколов;
- ✓ непрофессиональное и слабое администрирование систем;
- ✓ проблемы при построении межсетевых фильтров;

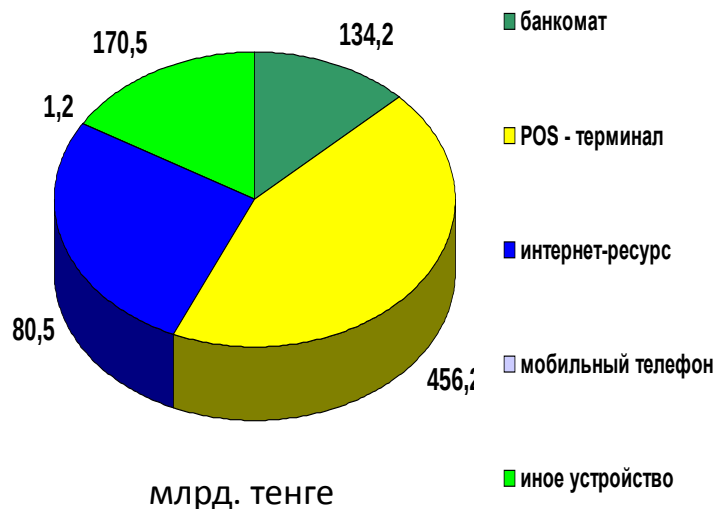
| Система ДБО банка                                                                                                                                                                            | Клиент банка                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>✓ Кража данных для входа в систему</li><li>✓ Кража информации о клиентах</li><li>✓ Обрушение сервисов (DDoS атаки)</li></ul> и тд...                   | <ul style="list-style-type: none"><li>✓ Кража данных для входа в систему</li><li>✓ Удаленное управление компьютером</li><li>✓ Автозалив</li></ul> и тд...                                                 |
| Защита от мошенничества                                                                                                                                                                      | Защита от мошенничества                                                                                                                                                                                   |
| <ul style="list-style-type: none"><li>✓ Системы фрод – мониторинга</li><li>✓ Многоуровневый firewall</li><li>✓ Защищенное соединение (SSL)</li><li>✓ Политики безопасности</li></ul> и тд... | <ul style="list-style-type: none"><li>✓ Аутентификация</li><li>✓ Электронная цифровая подпись</li><li>✓ SMS подтверждение</li><li>✓ Защищенное соединение (SSL)</li><li>✓ Антивирус (если есть)</li></ul> |
| Тех поддержка                                                                                                                                                                                | Тех поддержка                                                                                                                                                                                             |
| <ul style="list-style-type: none"><li>✓ Собственный штат сотрудников</li><li>✓ Кадровый аутсорсинг</li></ul>                                                                                 | <ul style="list-style-type: none"><li>✓ Сам клиент</li></ul>                                                                                                                                              |

Мошенники атакуют самое слабое звено

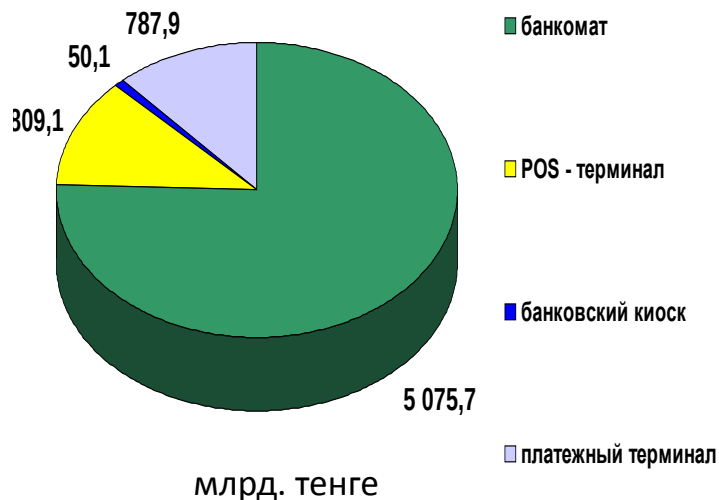


# Основные риски

## Безналичные операции



## С использованием наличных денег



Объем операций с использованием платежных карточек составляет свыше 83% от объема всех операций на территории Казахстана посредством электронных терминалов банков и Интернет

На долю мошеннических операций приходится 0,002% от объема всех операций с использованием платежных карточек казахстанских эмитентов. При этом, свыше 75% объема мошеннических операций совершены за пределами Казахстана.

Низкая доля мошеннических операций на территории Казахстана связана с тем, что основная часть карточек оснащена чипами и операции по ним в Казахстане, соответственно осуществляются путем считывания данных с чипа.



# Основные риски

## Мошенничество с использованием платежных карточек

На данный момент наиболее распространенный в мире вид мошенничества- это подделка платежных карт путем предварительной кражи информации.

Способы завладения информацией:

- кража данных карты работниками торговых и обслуживающих предприятий, путем считывания магнитной полосы карты и PIN-кода скимминговым устройством под видом обычного POS-терминала;
- организация мошенниками интернет-магазинов;
- фишинг (на сегодняшний день наиболее популярный вид мошенничества в странах СНГ);
- вишинг - сбор информации с использованием телефона (подвид фишинга);



Если еще несколько лет назад мошенничество с использованием платежных карт было в основном распространено в странах азиатско-тихоокеанского региона, то в настоящее время в зону риска попали страны со всех континентов, включая Австралию и США.



# Основные риски

## Мошенничество с использованием платежных карточек

- установка в картридер банкомата скиммингового устройства и накладки на клавиатуру или мини видеокамеры;
- кардинг – взлом (несанкционированный доступ) платежных систем или сервера интернет-магазинов;

## Иные способы мошенничества:

- «ливанская петля» - мошенничество с изъятием карты.
- скотч-метод – разъем для выдачи денег банкомата заклеивается скотчем или иным материалом.

## Мошенничество в системе интернет-банкинга юридических лиц

- кража данных осуществляется путем удаленного подключения к компьютеру или установки специальной программы



В мире наблюдается тенденция роста мошенничества в системе ДБО. Так, объем транзакций по картам, выпущенных мировыми брендами Visa, MasterCard, UnionPay, JCB, Discover/Diners и American Express, составил в 2014 году 23,8 трлн долл. США (рост 14,8%). В то же время убытки от мошеннических операций достигли 15,4 млрд долл. (рост 18,5%) или 0,06% от общего объема .



# Тренды по обеспечению безопасности в ДБО

## Внедрение новейших технологий

### Платежные карты с динамическим CVV кодом

Динамический верификационный код (DVC)

Код DCV формируется на дисплее EMV-чипа или на экране смартфона с номером, «привязанным» к карте держателя. Обновление динамического кода (DCV) осуществляется в режиме реального времени с периодичностью, задаваемой банком — эмитентом.



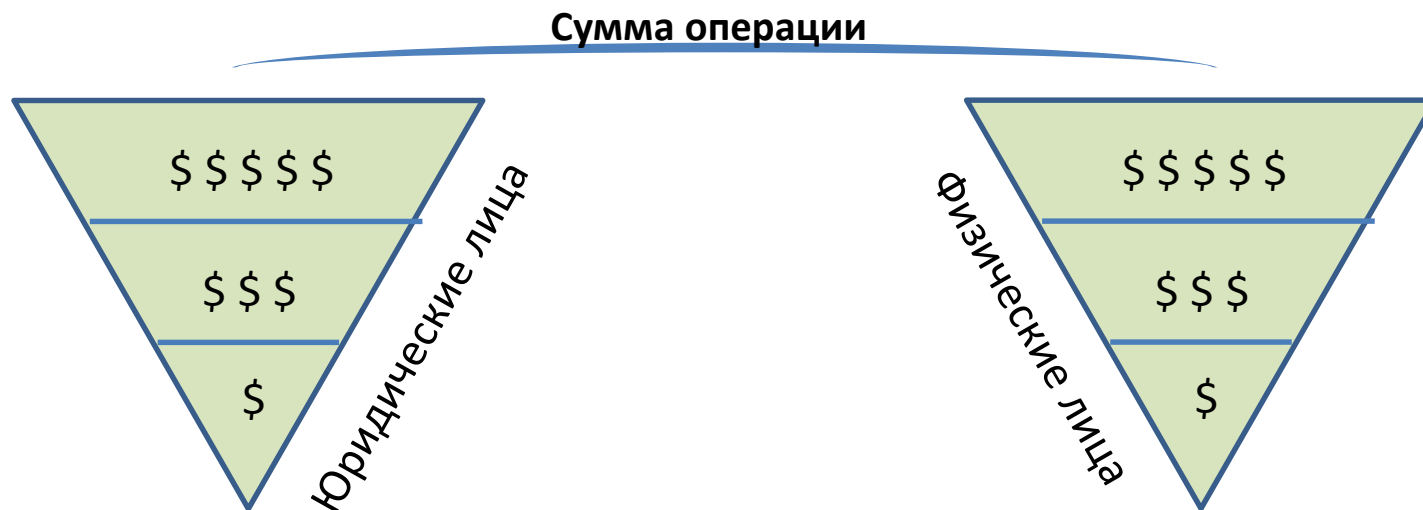
### Карты с биометрическим датчиком

Основное преимущество карт с биометрическим датчиком — возможность проведения транзакций по бесконтактному интерфейсу. Для совершения мгновенной покупки введение ПИН-кода не требуется. Весь процесс максимально упрощен: для выполнения операции держателю карты достаточно прижать большой палец к окошку датчика. Идентификация отпечатка проводится внутри самого чипа карты, где хранится эталон отпечатка держателя карты, загружаемый в банке при получении карты. Таким образом, эталон отпечатка не передается из чипа ни на каком из этапов транзакции.



# Меры по предупреждению мошеннических операций

Дифференцированный подход к требованиям обеспечения безопасности



| Использование ЭЦП          |                   |
|----------------------------|-------------------|
| Необходимо                 | Желательно        |
| Необходимо                 | Не желательно     |
| Необходимо                 | Нет необходимости |
| Логин и пароль             |                   |
| Необходимо                 | Желательно        |
| Необходимо                 | Желательно        |
| Желательно                 | Не желательно     |
| Динамическая идентификация |                   |
| Желательно                 | Необходимо        |
| Не желательно              | Желательно        |
| Не желательно              | Не желательно     |



# НБ РК на постоянной основе актуализирует требования по организационному обеспечению следования политике безопасности

Национальным Банком установлены требования по управлению рисками, в частности:

Правление банка разрабатывает политику управления операционным риском и осуществляет мониторинг соблюдения банком и его работниками политики управления операционным риском

Совет директоров банка утверждает политику управления операционным риском

Уполномоченный компетентный орган банка обеспечивает разработку политики управления операционным риском и осуществляет мониторинг и контроль за соблюдением банком и его работниками политики управления операционным риском

Внутренние правила банка должны содержать описание процедур безопасности, включающих организационные меры и программно - технические средства защиты обеспечения информационной безопасности при предоставлении электронных банковских услуг

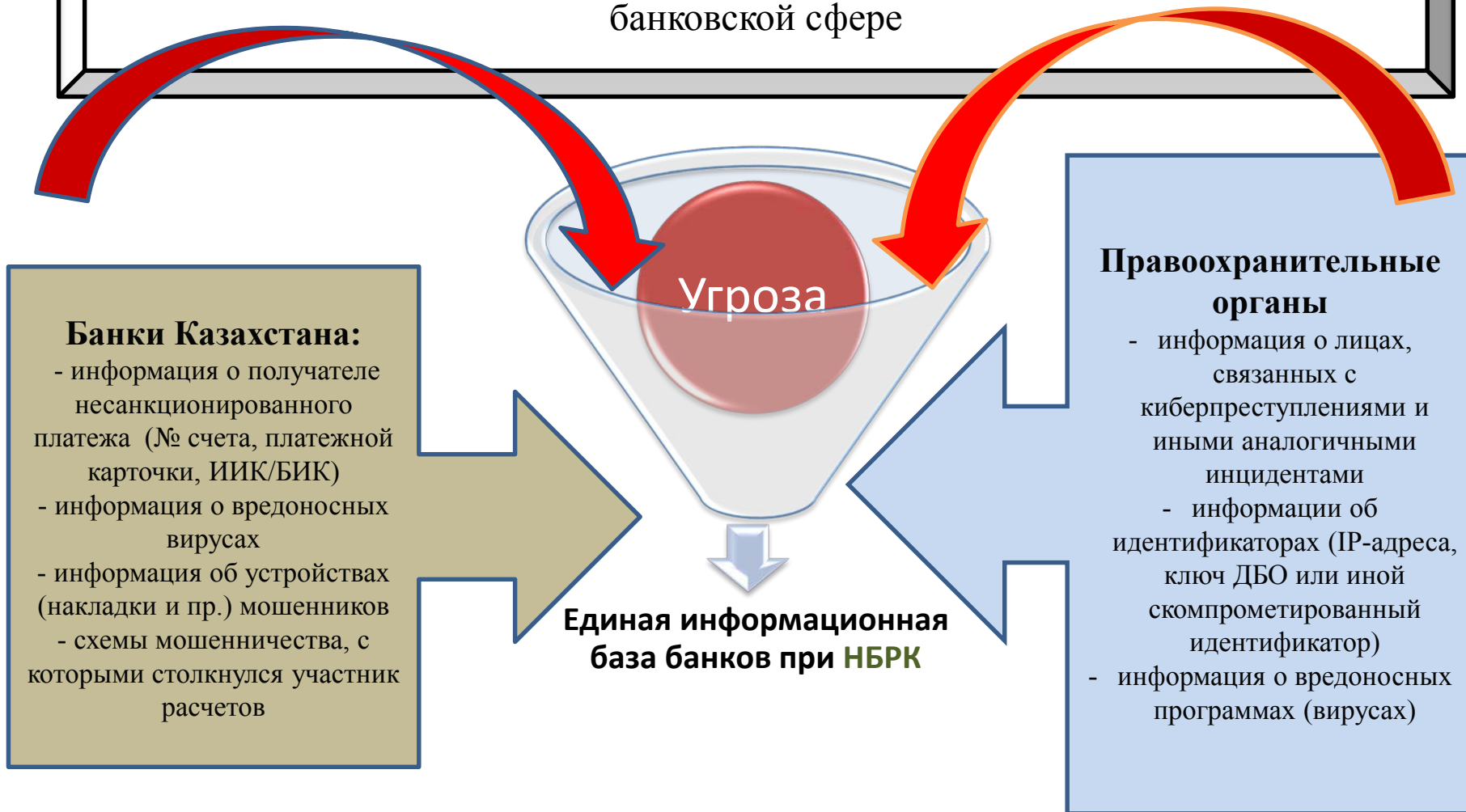


# Возрастающие вызовы требуют скоординированной работы



# Создание Единого центра реагирования позволит внедрять эффективные механизмы

Предоставление информации для предупреждения киберпреступлений в банковской сфере



# Направления дальнейшей деятельности

Как показывает практика подавляющая часть случаев мошенничества связана с пренебрежением клиентами банков правил безопасности

Открытое хранение средств идентификации:

- PIN-код вместе с картой;
- ЭЦП на компьютере или на внешнем носителе, который постоянно подключен к компьютеру

Передача карты третьим лицам

Совершение операций с картой в интернете на различных не проверенных торговых площадках

Невнимательность при совершении операций с картой на эл. терминалах

Дальнейшие усилия банков второго уровня и Национального Банка на пропаганде среди населения мер безопасного использования платежных карт и в целом систем ДБО

Мониторинг мировых тенденций в сфере киберпреступлений и своевременное принятие примитивных мер



# Законодательные меры

**Вносимые изменения в законодательство** (Проект Закона РК «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам неработающих кредитов и активов банков второго уровня, оказания финансовых услуг и деятельности финансовых организаций и Национального Банка Республики Казахстан»), **предусматривающие:**

**Законом «О Национальном Банке Республики Казахстан»** устанавливаются полномочия НБРК по утверждению требований к безопасности и непрерывности работы информационных систем банков и организаций, осуществляющих отдельные виды банковских операций

## **Закон «О банках и банковской деятельности в Республике Казахстан»**

Статья 61-5. Обеспечение непрерывности предоставления банковских услуг

1. Банк или организация, осуществляющая отдельные виды банковских операций, обеспечивают работу резервного центра информационной системы банка или организации, осуществляющей отдельные виды банковских операций, резервных каналов связи для восстановления деятельности информационной системы.
2. Банк или организация, осуществляющая отдельные виды банковских операций, уведомляют клиентов о планируемом введении в действие изменений (обновлений), вносимых в технические, программные и другие средства, обеспечивающие работу информационной системы, и влияющих на доступность клиенту банковских услуг в порядке и сроки, установленные внутренними правилами банка или организации, осуществляющей отдельные виды банковских операций, или договором.
3. Банк или организация, осуществляющая отдельные виды банковских операций, обеспечивают гарантированный уровень непрерывности предоставления услуг клиентам, который устанавливается внутренними правилами банка или организации, осуществляющей отдельные виды банковских операций, и подлежит обязательному размещению на интернет-ресурсе банка или организации, осуществляющей отдельные виды банковских операций.
4. Требования к безопасности и непрерывности работы информационных систем банков и организаций, осуществляющих отдельные виды банковских операций, устанавливаются уполномоченным органом.



## Законодательные меры

Проект постановления Правления НБРК «О внесении изменений и дополнений в постановление Правления Национального Банка Республики Казахстан от 29 марта 2010 года № 16 «Об утверждении Правил представления сведений по платежам и переводам денег, осуществленным через электронные терминалы и системы удаленного доступа, а также с использованием электронных денег») предусматривает:

- сбор информации о всех мошеннических операциях в системе ДБО

В настоящее время Национальный Банк осуществляет сбор информации о мошеннических операциях только с использованием платежных карточек

