НАЦИОНАЛЬНЫЙ БАНК КАЗАХСТАНА

# Основные направления информационной безопасности в финансовом секторе Республики Казахстан

# РЕЙТИНГ ВИДОВ БЕЗОПАСНОСТИ В СТРАНЕ

По экспертной оценке, проведенной в августе-сентябре 2014 года, произошло изменение в рейтинге видов национальной безопасности. Очевидно, что на переоценку оказали существенное влияние военное противостояние на Украине, а также информационные «войны». В Законе о национальной безопасности 2012 года отсутствует, как вид, внешняя безопасность. В сравнительных целях экспертами она была объединена с военной безопасностью

2010 год

1. Экономическая безопасность
2. Общественная безопасность
3. Политическая безопасность
4. **Информационная безопасность**
5. Внешняя/военная безопасность
6. Экологическая безопасность

2014 год

1. Политическая безопасность
2. Внешняя/военная безопасность
3. **Информационная безопасность**
4. Общественная безопасность
5. Экономическая безопасность
6. Экологическая безопасность

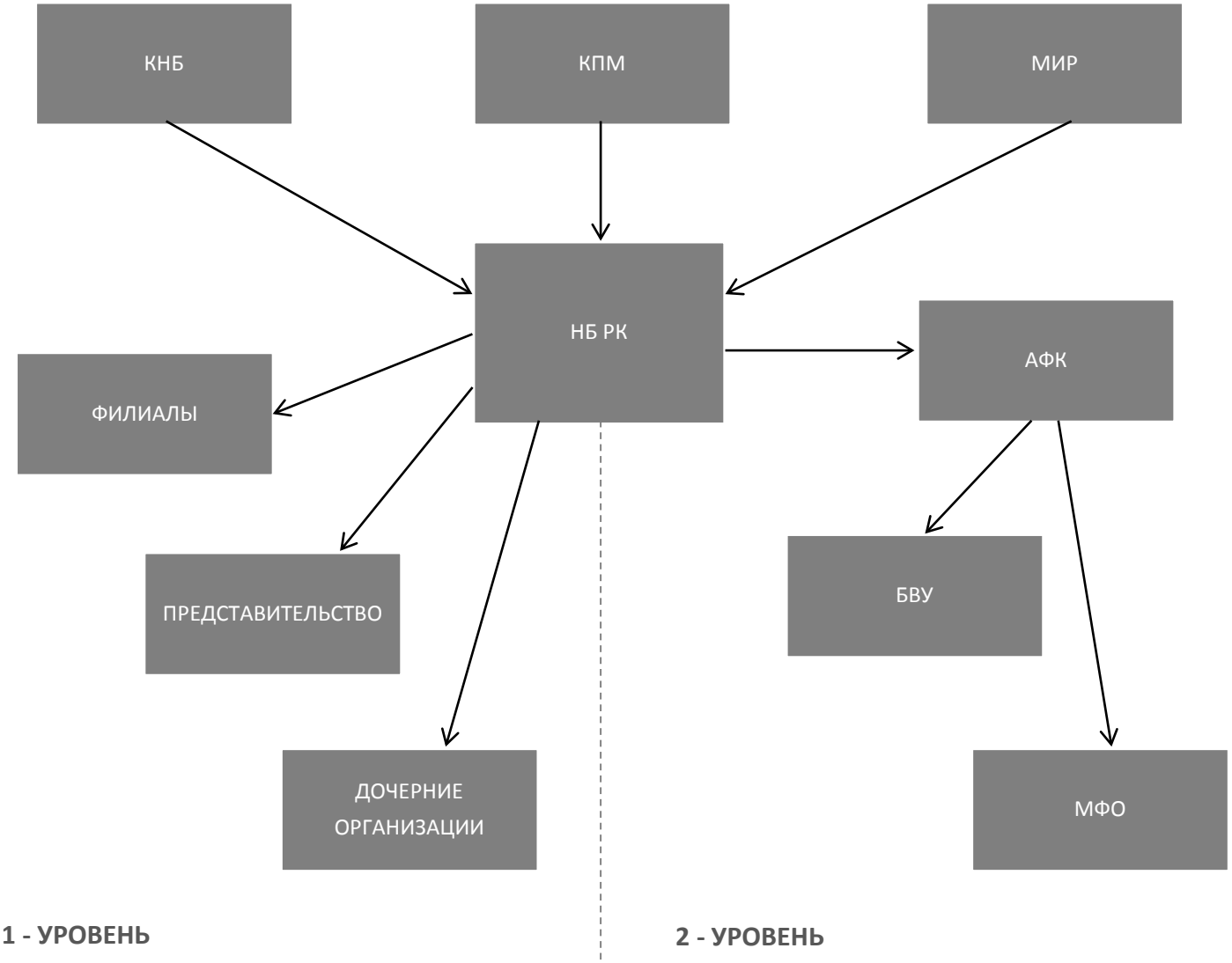
# НОРМАТИВНО-ПРАВОВАЯ БАЗА

- О Национальной Безопасности Республики Казахстан;
- О Национальном Банке Республики Казахстан;
- Об информатизации;
- Об электронном документе и электронной цифровой подписи;
- О персональных данных и их защите;
- О техническом регулировании;
- О связи;
- О Концепции информационной безопасности Республики Казахстан до 2016 года;
- О банках и банковской деятельности Республики Казахстан;
- Об утверждении Положения и структуры Национального Банка Республики Казахстан;
- О кредитных бюро и формировании кредитных историй в Республике Казахстан;
- О платежах и переводах денег.

# СТРАТЕГИЯ ИТ

- Постановление Правления Национального Банка Республики Казахстан №58 от 24 апреля 2015 года об утверждении Стратегии развития информационных технологий в Национальном Банке Республики Казахстан на период 2015-2020 годы;
- Постановление Правления Национального Банка Республики Казахстан №59 от 24 апреля 2015 года об утверждении Концепции «Создание центра обработки данных Национального Банка Республики Казахстан в городе Астана»;
- Постановление Совета Директоров №80 от 10 апреля 2015 года об одобрении Концепции развития и управления Единым центром обработки данных Национального Банка Республики Казахстан
- Стратегия ИТ Императивы развития:
- Переход на эталонный уровень информационной безопасности для финансового сектора;
- Сертификация ISO/IEC 27001 – 2017 год.

# РЕГУЛЯТОРНАЯ ПОЛИТИКА (ПЕРСПЕКТИВА)



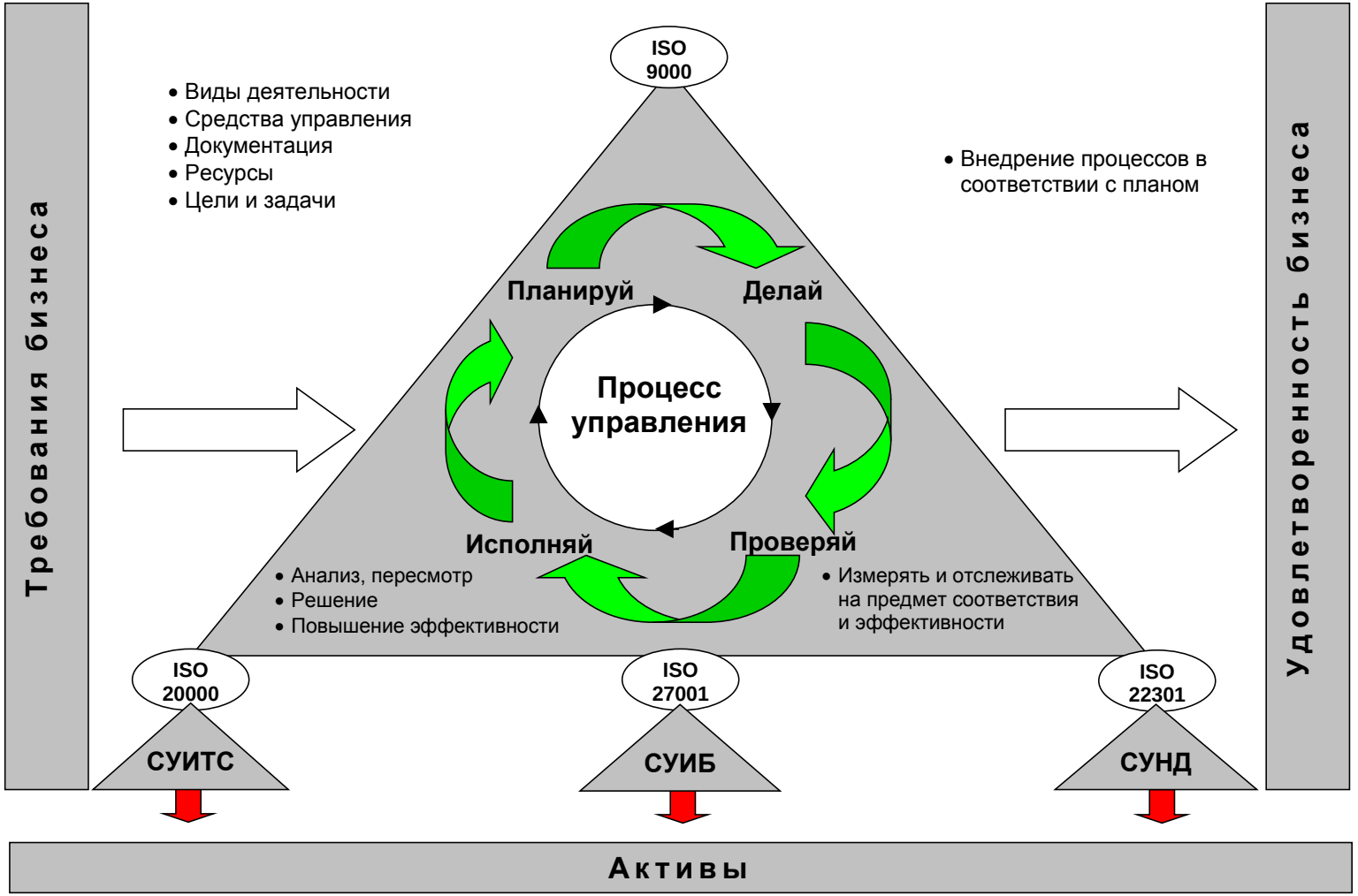
# Для устойчивого развития финансовой системы необходима реализация целей информационной безопасности на всех ее уровнях

**Цель: Обеспечение устойчивости финансовой системы и управление рисками информационной безопасности**

| **1-ый уровень: Национальный банк.**<br>**Создание в Национальном банке в эффективного механизма обеспечения информационной безопасности** | **2-ой уровень: Финансовая система.**<br>**Трансформация Национального банка в системообразующий институт в области информационной безопасности для финансовой системы** |
|---|---|

| Элементы модели | Текущая ситуация | Целевое состояние |
|---|---|---|
| **1. Политика ИБ и система управления рисками** | Политика ИБ и Система оценки и управления рисками ИБ носит формальный характер | Утверждение политики ИБ и создание эффективной системы управления рисками ИБ в соответствии с общей и ИТ стратегией НБРК |
| **2. Нормативная база** | Нормативная база ИБ устарела как на уровне НБ РК, так и финансовой системы в целом | Приведение Нормативной база в области ИБ в соответствие с общей ИТ стратегией НБРК |
| **3. Организация и роль** | Подразделение защиты информации должно реально решать возникающие проблемы | Создание организации с ресурсами и статусом достаточным для решения поставленных задач в области ИБ |
| **4. Инфраструктура** | Использование устаревших инструментов для защиты информации | Создание технологической инфраструктуры для решения поставленных задач в области информационной безопасности (построение CERT для финансовой системы) |
| **5. Культура** | Отсутствие устойчивой культура ИБ<br>Нехватка компетентных специалистов в области ИБ | Создание устойчивой культуры и достижение приемлемого уровня компетенции в области ИБ |
| **6. Контроль и отчетность** | Проверка информационной безопасности в финансовом секторе не проводится | Создание институциональной среды реализации и развития информационной безопасности |

# Интегрированная система менеджмента




**СУИТС** – система управления ИТ – сервисами
**СУИБ** – система управления информационной безопасности
**СУНД** – система управления непрерывности деятельности(бизнеса)

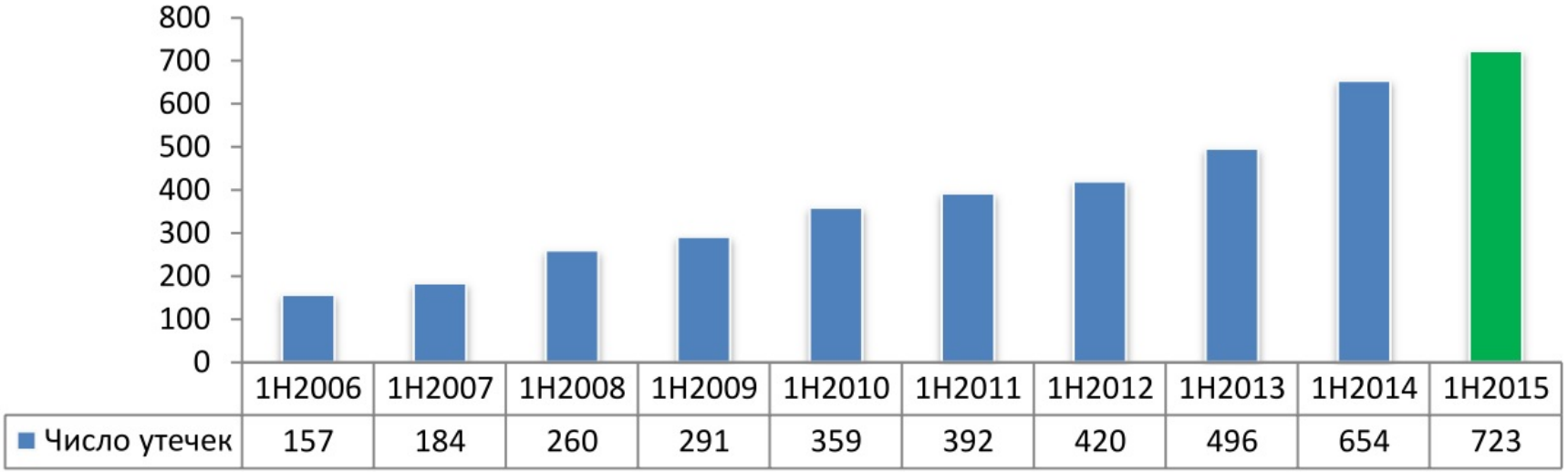
## Основные элементы системы управления информационной безопасностью которые должны соответствовать требованиям регулирующих органов и стандартов:

- использование лицензионного программного обеспечения;
- защита от несанкционированного доступа (НСД) к системам, в том числе и внутренняя защита от НСД сотрудников;
- защита персональных данных;
- защита каналов передачи данных, обеспечение целостности и актуальности данных при обмене информацией с клиентами;
- обеспечение юридической значимости электронных документов;
- управление инцидентами ИБ (SOC/CERT);
- управление непрерывностью деятельности (ведения бизнеса);
- внутренний и внешний аудит системы ИБ.

# Инициативы НБРК

- на постоянной основе организовано проведение обучающих семинаров по изучению международных стандартов на базе Академии РФЦА;
- совместно с  АФК организована площадка для связи с представителями БВУ по вопросам обеспечения ИБ и безопасности ИТ;
- разработан Проект положения О консультативно совещательном органе по вопросам ИБ;
- аккредитован УЦ КЦМР;
- переход к сервисной модели оказания ИТ услуг и защиты единой ИТ инфраструктуры НБРК на базе АО «Банковское сервисное бюро НБРК»;
- между НБРК и АО «Казахтелеком» заключен договор о долгосрочной аренде ЦОД в СЭЗ ПИТ «Алатау», который может быть использован БВУ в качестве резервного центра.

# Статистика утечки конфиденциальной информации за первое полугодие 2015 г.

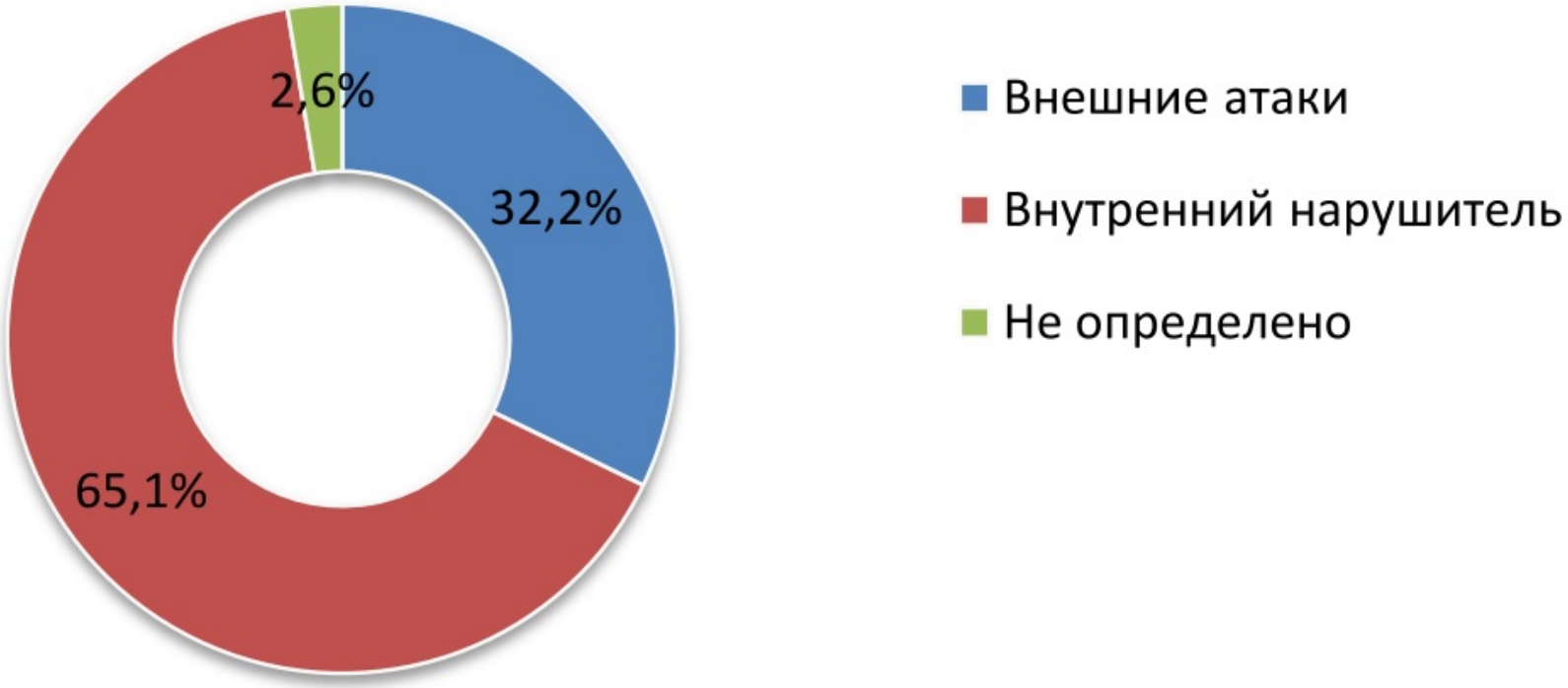



| | 1H2006 | 1H2007 | 1H2008 | 1H2009 | 1H2010 | 1H2011 | 1H2012 | 1H2013 | 1H2014 | 1H2015 |
|---|---|---|---|---|---|---|---|---|---|---|
| Число утечек | 157 | 184 | 260 | 291 | 359 | 392 | 420 | 496 | 654 | 723 |

За I полугодие 2015 года в мире зарегистрировано 723 случая утечки конфиденциальной информации. Это на 10% больше, чем за аналогичный период 2014 года (654 утечки). В пределах исследуемого периода рост утечек замедлился на 22 процентных пункта по сравнению с показателями I полугодия 2014 года (тогда рост к 2013 году составил 32%).

# Статистика по источнику утечки информации за первое полугодие 2015 г.

Зарегистрирована 471 (65%) утечка информации, причиной которой стал внутренний нарушитель. В 233 (32%) случаях утечка информации произошла из-за внешнего воздействия. Для некоторых случаев (2,6%) установить направление атаки оказалось невозможно.




Доля утечек под воздействием внешних атак оказалась на 9 процентных пункта выше аналогичного показателя за I полугодие 2014 года (тогда на долю утечек под воздействием внешних атак пришлось 22% утечек).