

**Выстраивание
системной работы
с персональными данными
подразделением
комплаенс-контроля
в АО КБ Хлынов**



Регуляторные требования в области ПД

- ❑ Федеральные законы: **152-ФЗ**; 149-ФЗ; 187-ФЗ; 115-ФЗ; 572-ФЗ; 218-ФЗ; 395-1-ФЗ (ст.26), 195-ФЗ (КоАП); ТК РФ
- ❑ Нормативные акты Банка России: Указание Банка России от 11.07.2024 № 6801-У; Положение Банка России от 30.01.2025 № 851-П; Стандарты Банка России, например, СТО БР ИББС-1.0-2014, СТО БР БФБО-1.5-2023
- ❑ Подзаконные акты и приказы регуляторов:
 - Приказ ФСТЭК России от 18.02.2013 N 21; Приказ ФСТЭК России от 11.04.2025 N 117
 - Приказ ФСБ России от 10.07.2014 N 378
 - Приказ Роскомнадзора от 27.10.2022 N 178
 - Постановление Правительства РФ от 01.11.2012 N 1119
 - ГОСТ Р 57580.1-2017

Ответственность

Административная (КоАП РФ)

Уголовная (УК РФ)

Гражданско-правовая (ГК РФ)



Регуляторные требования в области ПД

Направлены на

- обеспечение правомерности обработки персональных данных
- обеспечение реализации мер по защите персональных данных операторами
- обеспечение контроля соблюдения требований законодательства в рамках поручения на ОПД
- защиту субъектов ПД при трансграничной передаче
- уничтожение/своевременное уничтожение ПД
- формирование системы контроля и оценки рисков при обработке ПД



Размер ответственности

Нарушение требований

Нарушение	Размер штрафа
Нарушение требований по обработке ПД	до 700 тыс. руб
Нарушение требований к локализации баз данных	до 6 млн. руб
Нарушение требований по уведомлению РКН о неправомерной передаче ПД	до 3 млн. руб
Нарушение порядка обработки биометрических ПД и требований к обеспечению безопасности при их обработке	до 1 млн.руб.
Нарушение требований в области обеспечения безопасности КИИ	до 500 тыс. руб

Размер ответственности

Неправомерная передача без признаков уголовно наказуемого деяния

ЮЛ

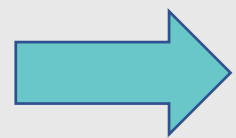
У сведений	Размер штрафа (млн.руб)
1000-10 000 СПД и (или) 10 000 – 100 000 И-Р	до 5
10 000 - 100 000 СПД и (или) 100 000 – 1 000 000 И-Р	до 10
более 100 000 СПД и (или) более 1 000 000 И-Р	до 15
Специальные категории СПБ	до 15
Биометрические ПД	до 20

ДЛ

У сведений	Размер штрафа (тыс.руб)
1000-10 000 СПД и (или) 10 000 – 100 000 И-Р	до 400
10 000 - 100 000 СПД и (или) 100 000 – 1 000 000 И-Р	до 500
более 100 000 СПД и (или) более 1 000 000 И-Р	до 600
Специальные категории СПБ	до 1300
Биометрические ПД	до 1500

Почему соблюдение норм критично для банков сегодня

- Защита клиентов — основной ресурс банка
- Снижение финансовых рисков
- Предотвращение репутационных потерь
- Обеспечение операционной устойчивости
- Соблюдение законодательства о противодействии отмыванию денег (ПОД/ФТ)
- Участие в системах межведомственного взаимодействия, платежных системах, цифровых платформах



**ПД — стратегический актив:
регуляторика, риски и доверие клиентов требует системности**

Банк Хлынов сегодня

37 ДОПОЛНИТЕЛЬНЫХ ОФИСОВ В
10 регионах

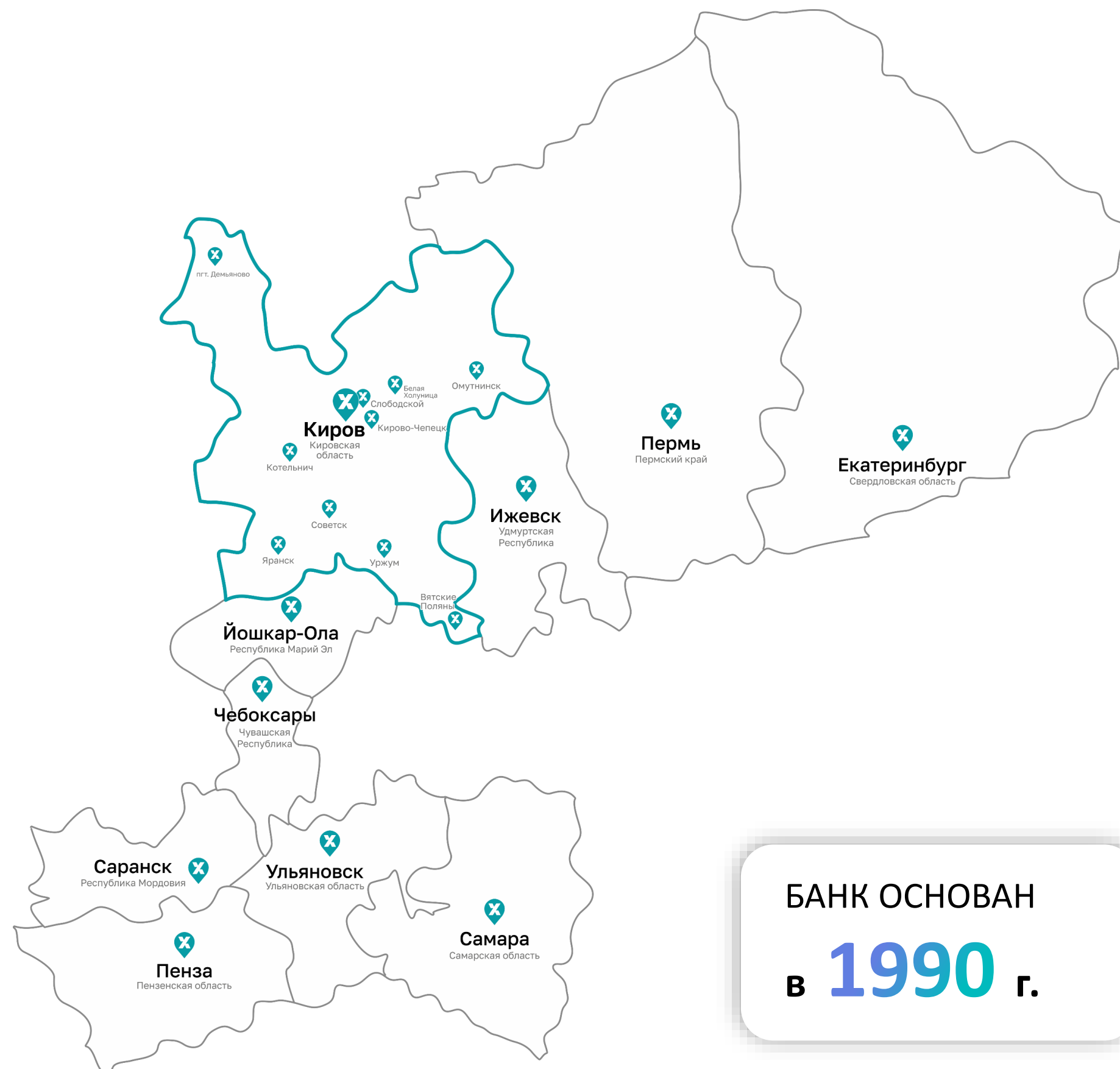
БОЛЕЕ **200 000** КЛИЕНТОВ



49 млрд ₽ АКТИВЫ



6 млрд ₽ КАПИТАЛ



БАНК ОСНОВАН
В **1990** г.

Подходы к внедрению системной работы с ПДн в банке

Системная работа направлена на соблюдение требований к обработке и защите ПД с учетом ст. 18.1 и 19 152-ФЗ и основана на комплексе функций



↓

Организационная

↓

Техническая

↓

Процедурная

↓

Контрольная
и аудит

Организационная функция

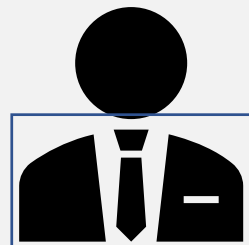
Управление риском ПД – распределенная функция по объектам риска

Организация управления риском ПД - функция СВК в рамках управления регуляторным риском

Организация управления риском ПД в части ИСПД - функция ИБ. СВК контроль в рамках управления регуляторным риском



Председатель правления



DSO

Ответственный за
организацию обработки ПД 152-ФЗ

Ответственный за обеспечение
информационной безопасности) – 149-ФЗ

*Обязанности и полномочия
в соответствии со ст. 22.1. 152-ФЗ*

отчеты



СВК

*Приказ DPO о назначении
модераторов, ответственных
за организацию системы
работы с ПД*

*Контроль
в рамках РР*



ИБ

*Указ Президента РФ от
01.05.2022 N 250*



Ответственные за обработку ПД

На основании ЛНА банка

- *Управление риском ПД в процессах*
- *Информирование СВК о намерении ТГПД*
- *Участие в уничтожении ПД*
- *Актуализация сведений в Реестре ПД*
- *Управление риском ИБ в процессах*
- *Согласование доступов в ИС и помещения банка*
- *Информирование СВК об инцидентах вне ИСПД*

*Мероприятия в рамках
мониторинга/контроля*

Организационная функция



- Методология, в т.ч. система ВК
- Постоянный аудит процессов банка
- Обеспечение автоматизированными инструментами для управления процессом обработки ПД
- Разработка ЛНА
- Правовое сопровождение
- Обучение
- Рассмотрение обращений субъектов ПД
- Оценка вреда
- Оценка риска ПД
- Формирование корпоративной культуры по управлению риском ПД
- Взаимодействие с Роскомнадзором
- Администрирование Реестра ПД (сервис для учета сведений, связанных с обработкой и защитой ПД, в разрезе бизнес- процессов)

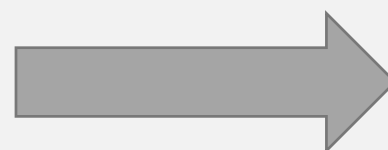


Техническая функция



ИБ

- Разработка ЛНА
- Обучение
- Реализация технических мер на основании оценки вреда
- Внедрение технических мер, направленных на защиту данных (криптографическая защита; DLP – система; контроль доступов; SIEM – система; СКУД и иные в соответствии с требованиями ФСТЭК, Банка России, ФСБ)
- Реагирование на инциденты, уведомление РКН и ФСТЭК
- Обеспечение проведения тестирования на проникновение, моделирование угроз
- Координация подразделений ИТ (в части ИБ)



ИТ

- Реализация мероприятий по обеспечению защиты информации



Процедурная функция



Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных

Процедурная функция

Фокус СВК

Для управления риском ПД на каждом этапе обработки ПД

- ✓ разработаны Политики, Положения. Изданы ЛНА
- ✓ Осуществляется систематический аудит процессов банка на предмет осуществления обработки ПД
- ✓ процессы банка описаны
- ✓ определены правовые основания обработки ПД во всех процессах банка
- ✓ форма согласия/договоров утверждены ВНД банка и проходят своевременную актуализацию для обеспечения выполнения требований НПА
- ✓ использование ИИ осуществляется в рамках законодательства в области ПД

Сбор

- ✓ перечень персональных данных, обрабатываемых в банке – не избыточный
- ✓ строгие формы для сбора – определены цели, объем и состав ПД соответствует цели
- ✓ способ сбора – канал включен в перечень ИС, канал защищен

Хранение

- ✓ определены места хранения вне ИС, материальных носителей для ИС, перечень ИСПД
- ✓ Определены ответственные за хранение
- ✓ система доступов к местам хранения
- ✓ определены сроки хранения с учетом номенклатуры дел – исключаются завышенные сроки хранения ПД

Распространение

- ✓ при наличии обязательного письменного согласия
- ✓ мониторинг официального сайта банка и доменов 3-го уровня
- ✓ работа с подразделениями по маркетингу и рекламе

Процедурная функция

Фокус СВК

Трансграничная передача ПД

- ✓ реестр иностранных государств для целей ТГППД
- ✓ направление в РКН Уведомления о намерении ТГППД (с учетом Приказа РКН от 05.08.2022 N 128)

Обращения СПД

- ✓ организован процесс работы с обращениями – своевременное поступление обращений в СВК (ПО Jira)
- ✓ Определены полномочия на принятия решения о прекращении обработки ПД – соблюдение сроков для прекращения (ст.21; 10.1 152-ФЗ)

Работа с контрагентами

- ✓ основание для передачи ПД в соответствии с целью
- ✓ поручение на ОПД
- ✓ SLA о реагировании на инциденты
- ✓ Логистическая схема ПД (внутренний – внешний контур)
- ✓ анализ мер контрагента по защите ПД

Инциденты

- ✓ Определен порядок реагирования на инциденты, порядок проведения служебного расследования
- ✓ Определены ответственные за уведомление об утечке ПД РКН, ФинЦЕРТ
- ✓ Соблюдение сроков уведомления (ст. 21 152-ФЗ; СТО БР БФБО-1.5-2023)

Процедурная функция

Фокус СВК

Защита ПД

- ✓ наличие и эффективное функционирование мониторинговых систем
- ✓ уведомление СВК о тревогах SIEM и DLP – систем
- ✓ система доступов к ПД
- ✓ реализация мер в соответствии с оценкой вреда
- ✓ соответствие уровня защищенности категории ПД
- ✓ определены технические меры и утверждены ответственные за их выполнение
- ✓ Проводится аудит ИБ, пентесты

Уничтожение

- ✓ Определен порядок блокирования /удаления/уничтожения
- ✓ Составление акта в соответствии с Приказ РКН от 28.10.2022 N 179
- ✓ Определены ответственные за уничтожение вне ИСПД и в ИСПД
- ✓ Отсутствие недостигнутых целей по другим продуктам
- ✓ Соблюдение сроков, установленных для уничтожения

Какие инструменты применяем для достижения положительного результата **Процедурной функции**

Работники банка допускаются к исполнению своих должностных обязанностей только при условии ознакомления с внутренними нормативными документами, регламентирующими порядок обработки персональных данных и порядок работы в информационных системах банка.



Какие инструменты применяем для достижения положительного результата **Процедурной функции**

- ❖ Реестр ПД – система для управления информацией в отношении персональных данных, обрабатываемых в банке (ПО Privacy Box)
- ❖ Кросс-функциональное согласование бизнес-процессов (обязательное согласование службы внутреннего контроля, подразделениями информационной безопасности, юридическим управлением)
- ❖ Канал для оперативного взаимодействия СВК с ответственными за обработку ПД (Jira, Битрикс24)
- ❖ Единый методологический центр – организатор процесса работы с ПД в банке - СВК
- ❖ Регулярные обучения сотрудников банка

Контрольная функция и аудит

DPO

- Утверждение дорожной карты управления риском ПД
- Рассмотрение отчетов СВК и ИБ
- Принятие решения по оценке вреда в соответствии с Приказом Роскомнадзора от 27.10.2022 N 178
- Инициирование внешнего аудита
- Инициирование пентестирования

СВК

- Дорожная карта управления риском ПД
- Матрица рисков
- Контроль процессов через Реестр ПД
- Контроль обязательного обучения
- Контроль ознакомления с ВНД
- Оценка вреда в соответствии с Приказом Роскомнадзора от 27.10.2022 N 178

Ответственные
за обработку
ПД

- Определение контрольных процедур в бизнес - процессах
- Контроль согласования бизнес-процессов с СВК и ИБ

СВА

Внешние аудиторы



Минимизация риска за счет

- ✓ Управления риском на каждом этапе обработки ПД
 - ✓ Распределения ролей и ответственности
 - ✓ Создания эффективной системы контроля
- ! Особое внимание к ДБО, официальному сайту банка, и иным официальным информационным каналам банка**

Основные драйверы комплаенс-контроля по выполнению регуляторных требований в области ПД

- ➔ Технологические угрозы и рост кибератак
- ➔ Ужесточение требований, направленных на предотвращение мошенничества
- ➔ Расширение географии присутствия банка
- ➔ Проверки регулятора
- ➔ Развитие ИИ
- ➔ Усиление ответственности за нарушений законодательства в области ПД
- ➔ Управление регуляторным риском

**Благодарю
за внимание!**

