

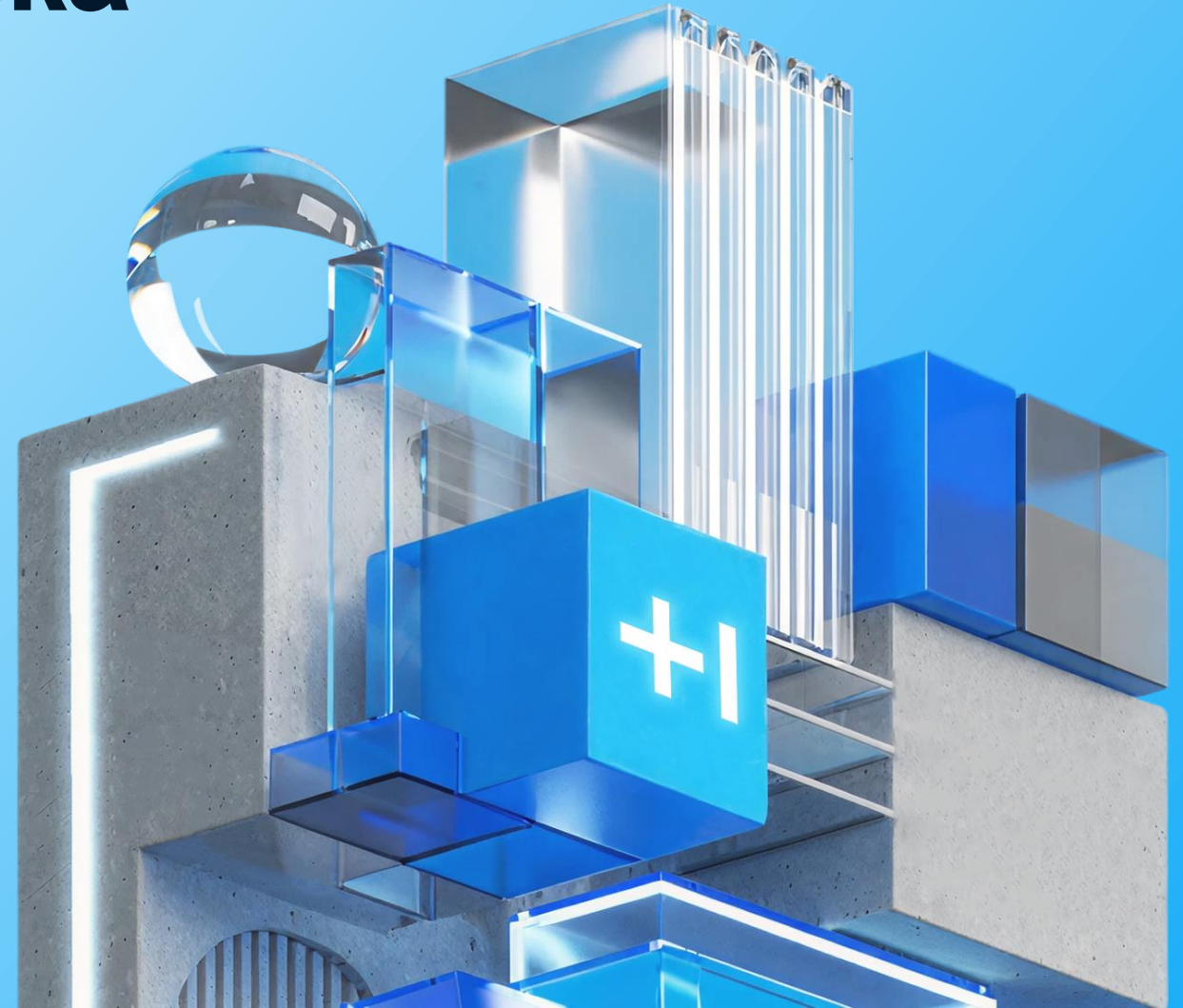
Библиотека сценариев реализации операционного риска и другие новинки инструментария Орикс

22/06/2026

- библиотека сценариев реализации операционного риска
- экстремальные значения и бенчмарки
- показатели концентрации потерь — как считать среднее
- бенчмарки Орикс за рамками ф.0409106



Библиотека сценариев реализации операционного риска



Сценарный анализ глазами регулятора

Сценарный анализ операционного риска осуществляется для целей:

- идентификации угроз и негативных последствий реализации операционного риска на уровне процессов банка, включая:
 - выявление недостатков и пробелов в процессах,
 - разработку мероприятий по устранению недостатков и предотвращению реализации угроз,
 - оценку эффективности (результативности) данных мероприятий,
 - качественную оценку уровня операционного риска до и после реализации этих мероприятий путем определения уровня остаточного риска.

Критерии проведения сценарного анализа риска

одновременно выполняются минимум 2 из перечисленных ниже условий:

- по результатам самооценки риска его уровень оценен как **«Очень высокий»** как минимум в рамках одного критически важного процесса;
- операционный риск может реализоваться **более чем в двух критически** важных процессах банка;
- проведение сценарного анализа является целесообразным согласно суждению подразделения, ответственного за организацию управления операционным риском (ПУОР).

*Разъяснения Банка России по процедуре
качественной оценки операционного риска
от 30.09.2021 № 716-Р-2021/47*

Данные и результаты

Объект анализа



сценарий (пример) реализации риска – детальное описание реализации риска



возможные источники риска, которые могут повлечь реализацию сценария



недостатки процессов/систем, усиливающие воздействие сценария, сильные стороны процессов/систем, снижающие влияние недостатков

Результат анализа

наиболее негативный сценарий реализации операционного риска

потенциальные события операционного риска, их классификация

сильные и слабые стороны организации процессов, информационных систем, контрольной среды

меры для уменьшения негативного влияния операционного риска

ключевые индикаторы операционного риска, которые смогут отслеживать риск, по которому был проведен сценарный анализ

Доступно в библиотеке сценариев

По каждому сценарию

- Суть произошедшего сценария
- Детали сценария
 - Последовательность событий при реализации сценария
 - Обстоятельства выявления сценария
 - Реагирование банка на сценарии
 - Меры, предпринятые по результатам анализа произошедшего
- Уязвимости процессов, сбои / неэффективность контрольных процедур
- Алгоритм расчета величины потери по реализованному риску в разрезе типов потерь
- Формула расчета совокупных потерь:
- Мероприятия по управлению риском
- Виды потерь, которые банк несет в результате сценария: Прямые / Косвенные / Потенциальные потери / Потенциальные потери 3-их лиц
- Риск, под воздействием которого реализовался сценарий
- Направление деятельности (2 уровня)
- Тип рискового события (2 уровня)
- Источник риска (2 уровня)

Доступно в библиотеке сценариев



Состав сценариев

1. Внутреннее мошенничество: хищение средств со «спящих» депозитов Отказ инфраструктуры VPN удаленного доступа
2. Отказ инфраструктуры VPN удаленного доступа
3. Сбой в системе платежей: массовая задержка межбанковских переводов через СБП
4. Потери от конверсионных операций из-за некорректного курса конвертации
5. Выдача кредитов с повышенным риском из-за утраты клиентской истории
6. Выдача кредитов физическим лицам банкротам
7. Введение внешних санкций со стороны других государств
8. Недоступность использования зарубежных корневых DNS-серверов
9. Отключение внешнего Интернета по решению Роскомнадзора
10. Сбой в базе данных / программном обеспечении, обеспечивающем работу процессингового центра
11. Распространение опасного заболевания / эпидемия / пандемия и вызванные ими последствия
12. Нарушение штатного режима функционирования сетевого оборудования системы расчетов, повлекшее частичное или полное прекращение предоставления сервиса:
13. Недоступность / отказ от сотрудничества контрагента, оказывающего услуги инкассации
14. Осуществление сотрудниками точек продаж заведомо некорректных консультаций о продуктах и услугах Банка с целью выполнения плана продаж
15. Отсутствие полной и прозрачной информации о продукте и/или профиле целевого клиента в ПО/документах/памятках/скриптах для продающих сотрудников точек продаж
16. Заведомое содержание в продуктах кросс-продаж дополнительных услуг, завышенных комиссий и других недобросовестных практик, отсутствие проработки клиентской ценности разрабатываемых продуктов и т.д. (несоблюдение рекомендаций 19-МР)
17. Действующая настройка отражения информации о продукте и клиентский путь (возможность отказа от доп. услуг и т.д.) на сайте Банка и в приложении (несоблюдение рекомендаций 22-МР)
18. Выход из строя сетевой инфраструктуры Банка (в т.ч. в результате внешних санкций)
19. Кибер-атака на инфраструктуру ЦОД
20. Недоступность / Отказ от сотрудничества контрагентов, оказывающих услуги сопровождения и эксплуатации оборудования для ИТ-систем Банка
21. Выход из строя ключевого оборудования ЦОД с учетом дефицита оборудования/комплектующих на рынке
22. Внедрение вредоносного ПО, программ шпионов, троянов и вирусов с помощью флэш-накопителей/мобильных устройств работниками Банка, фишинговых сообщений/методов социальной инженерии работниками Банка / третьими лицами
23. Раскрытие/кража конфиденциальной информации

Будет доступен в Орикс до конца 2 кв. 2026

Сценарии в Орикс (1 из 2)



[Мои данные](#) [Сравнение с бенчмарками](#) [Аналитика](#) [Бизнес - кейсы](#) [Внешние события](#) **Сценарии** [Опросы](#) [Оценка методологии](#)

Сценарии операционного риска

Найдено сценариев: 7

Поиск

Сценарий № 1.2.1. Внутреннее мошенничество: хищение средств со «спящих» депозитов



В крупном универсальном банке сотрудник операционного офиса, имеющий расширенные права в АБС по вкладам физических лиц, в течение нескольких месяцев последовательно выводил средства со «спящих» депозитов клиентов, которые долго не совершали операций и не обращались в офис. Он подбирал счета по признакам: долгий срок без движений, пожилой возраст клиента, отсутствие активных дистанционных сервисов.

Механика заключалась в следующем: сотрудник инициировал операции закрытия вкладов на основании поддельных заявлений клиентов (сканы подписе...

Спящие депозиты, Мошенничество

Сценарий № 6.2.1. Отказ инфраструктуры VPN удаленного доступа



После введения очередного пакета международных санкций один из зарубежных поставщиков сетевых услуг Банка прекратил обслуживание части каналов связи и доступа к облачным сервисам, используемым Банком, что потребовало оперативной перестройки маршрутизации и переноса части сервисов аутентификации и управления доступом на локальные мощности. На фоне усиленной нагрузки и срочных изменений в конфигурации произошел сбой в Active Directory, в результате которого пользователи перестали корректно проходить аутентификацию при попытке подключения через VPN....

ОНИВД, Сбой ИТ

Сценарии в Орикс (2 из 2)

назад

Внутреннее мошенничество: хищение средств со «спящих» депозитов

Сценарий 1.2.1

Дата публикации
04.02.2026

Дата обновления
-

Хэштеги:

Спящие депозиты

Мошенничество

Вероятность понесения потерь (в год)



Суть произошедшего сценария

Хищение средств со «спящих» (неоднократно автоматически пролонгируемых) клиентских депозитов посредством расширенных прав доступа сотрудника к АБС и использования им подложных документов.

Детали сценария

В крупном универсальном банке сотрудник операционного офиса, имеющий расширенные права в АБС по вкладам физических лиц, в течение нескольких месяцев последовательно выводил средства со «спящих» депозитов клиентов, которые долго не совершали операций и не обращались в офис. Он подбирал счета по признакам: долгий срок без движений, пожилой возраст клиента, отсутствие активных дистанционных сервисов.

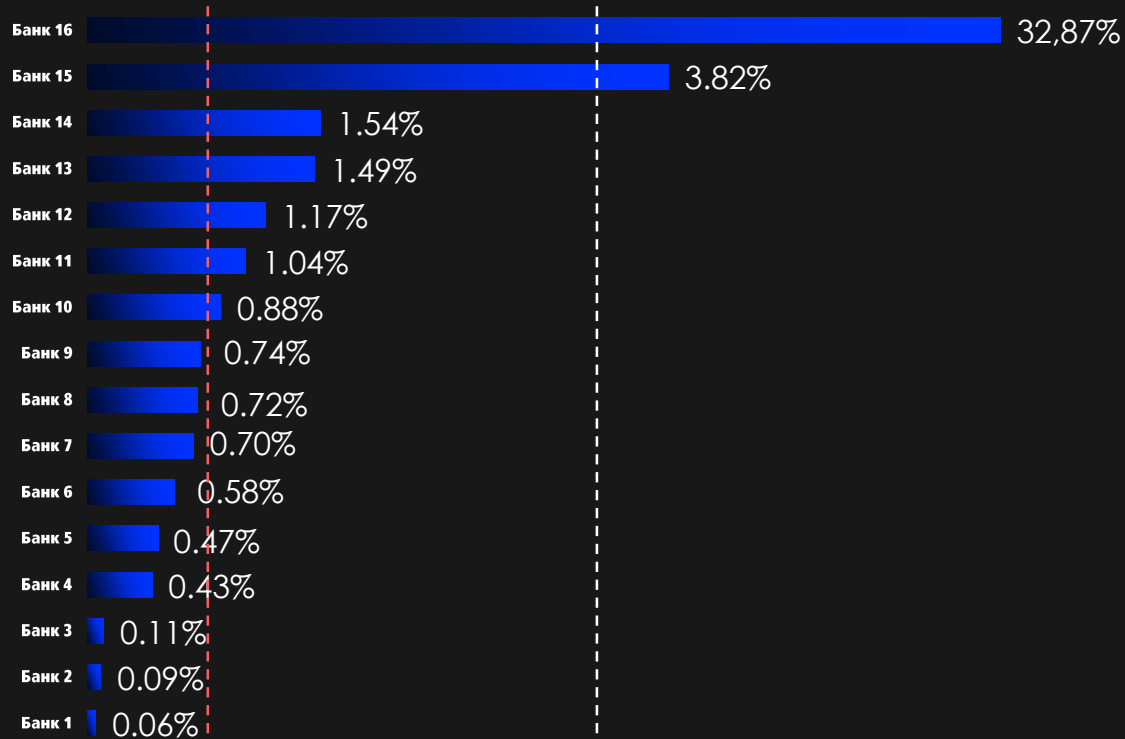
Экстремальные значения – как не испортить бенчмарки операционного риска



Основной показатель эффективности управления операционным риском – отношение чистых потерь к бизнес-индикатору

КПУР_3 за 2025 год

Зарабатывая каждые 100 руб. дохода, в 2025 году банки теряли на операционном риске в среднем 2,92 рубля



0,86%
Среднее без
экстремумов

2,92%
Среднее

если отбросить экстремальные значения - усреднённый показатель снижается с 2,92% до 0,86%

Экстремальное значение одного или всех показателей банка?

Экстремальное значение одного показателя банка в периоде

- + Показатель зависит не только от объема потерь по операционному риску
- + Показатель имеет аномальное значение в силу выбранной банком методологии учета потерь



Банк в целом за отчетный период – «экстремальное наблюдение»

- + Если совокупный уровень потерь существенно превышает отраслевые уровни из-за одной катастрофической операции (крупный судебный кейс, масштабный технологический сбой и т.п.) - вся агрегированная статистика банка за период становится нетипичной.



Отчет банка
считается
экстремальным в
отчетном периоде в
случае выполнения
условия (1) или (2)



Данные экстремального отчета не участвуют в расчете средних значений в случае выбора пользователем опции «Исключить экстремумы из расчета средних».

условие (1)



- количество событий банка за период, и среднее количество событий за последние 4 периода (включая текущий) > 500
- И
- доля ТОП-1 потери в общем объеме потерь банка в периоде $> 90\%$.

условие (2)



- величина ТОП -1 потери больше либо равна 1500 млн руб.
- И
- доля ТОП -1 потери в общем объеме потерь банка в периоде $> 50\%$

Условия на экстремальность значения показателя банка зависят от количества значений в выборке



Данные экстремального значения показателя не участвуют в расчете средних значений в случае выбора пользователем опции «Исключить экстремумы из расчета средних».



1. **в выборке 3 значения** – экстремум не исключается
2. **в выборке от 4 до 6 значений** – значение X_i считается экстремумом если:

$X_i/X_j \geq 10$ либо $X_i/X_j \leq 0,1$ для всех $j = 1..n$, кроме i , где n – число значений в ряду

3. **в выборке 7 и более значений:**

- рассчитывается центральное значение ряда – Медиана (M)
- рассчитывается MAD (Median Absolute Deviation) - Медиана ряда $\{|X_i - M|\}$, $i=1..n$, где n – число значений в ряду
- значение X_i считается экстремумом при условии, что $(X_i - M)/MAD \geq K$,
- K принимает значения в диапазоне $[2,5; 4]$, определяется индивидуально для каждого показателя

С учетом экстремумов или без?



Оставить все значения

- + Проверка достаточности капитала под редкие, но тяжелые потери
- + Оценка потерь в рамках стресс-тестирования, анализа сценариев реализации крупных событий
- + Калибровка внутренних моделей



Исключить экстремумы

- + Расчет бенчмарков «нормального» уровня потерь
- + Калибровка пороговых уровней КИР
- + Сравнение по эффективности СУОР банков

Альтернативные механизмы расчета бенчмарков (средних значений) по концентрации потерь от операционного риска



Как считать бенчмарк для концентрации потерь



Среднее по банкам

Сначала для каждого банка рассчитывается доля потерь по выбранному классификатору, затем доли усредняются.

Каждый банк имеет одинаковый вес вне зависимости от масштаба потерь.

Банк А

800

1 000

Потери в Розничном
обслуживании

Общие потери

Простая средняя концентрация - **70%**



Среднее по объему потерь

Сначала суммируются потери по выбранному признаку и общие потери по всей выборке, затем рассчитывается их отношение.

Банки с более крупным объемом потерь оказывают большее влияние на результат.

Банк Б

60 000

100 000

Потери в Розничном
обслуживании

Общие потери

Средняя концентрация по объему потерь
60,2%

Алгоритмы расчета средних

Для банка i концентрация потерь c_i по выбранному классу k равна:

$$c_i = \frac{L_{i,k}}{L_i}$$

$L_{i,k}$ — потери по данному направлению, типу события или источнику риска,

L_i — совокупные потери банка за период.

Тогда простой средний бенчмарк $\bar{c}_{simple}$ по выборке из N банков равен:

$$\bar{c}_{simple} = \frac{1}{N} \sum_{i=1}^N c_i.$$

Простой средний бенчмарк

какова средняя концентрация у одного банка из выборки

При тех же обозначениях

Взвешенный (агрегированный) бенчмарк $\bar{c}_{weighted}$ по выборке из N банков равен:

$$\bar{c}_{weighted} = \frac{\sum_{i=1}^N L_{i,k}}{\sum_{i=1}^N L_i}.$$

Взвешенный(агрегированный) бенчмарк

какова доля потерь класса относительно совокупного объема потерь всей выборки

Для банка i концентрация потерь c_i по выбранному классу k равна:

$$c_i = \frac{L_{i,k}}{L_i}$$

$L_{i,k}$ — потери по данному направлению, типу события или источнику риска,

L_i — совокупные потери банка за период.

Тогда простой средний бенчмарк $\bar{c}_{simple}$ по выборке из N банков равен:

$$\bar{c}_{simple} = \frac{1}{N} \sum_{i=1}^N c_i.$$

Простой средний бенчмарк

какова средняя концентрация у одного банка из выборки

При тех же обозначениях

Взвешенный (агрегированный) бенчмарк $\bar{c}_{weighted}$ по выборке из N банков равен:

$$\bar{c}_{weighted} = \frac{\sum_{i=1}^N L_{i,k}}{\sum_{i=1}^N L_i}.$$

Взвешенный(агрегированный) бенчмарк

какова доля потерь класса относительно совокупного объема потерь всей выборки

Как использовать различные алгоритмы усреднения



Простое среднее подходит для сравнения банка с «типичным представителем» группы сравнения



полезно для определения внутреннего риск-аппетита, калибровки сигнальных и контрольных значений лимитов и индикаторов риска и выявления аномалий



Взвешенное среднее используется в качестве ориентира для структуры совокупных потерь



используется при оценке кластера/рынка в целом – где реально сосредоточены рубли потерь, при расчете отраслевых бенчмарков для сценарного анализа



Расхождение двух средних само по себе информативно

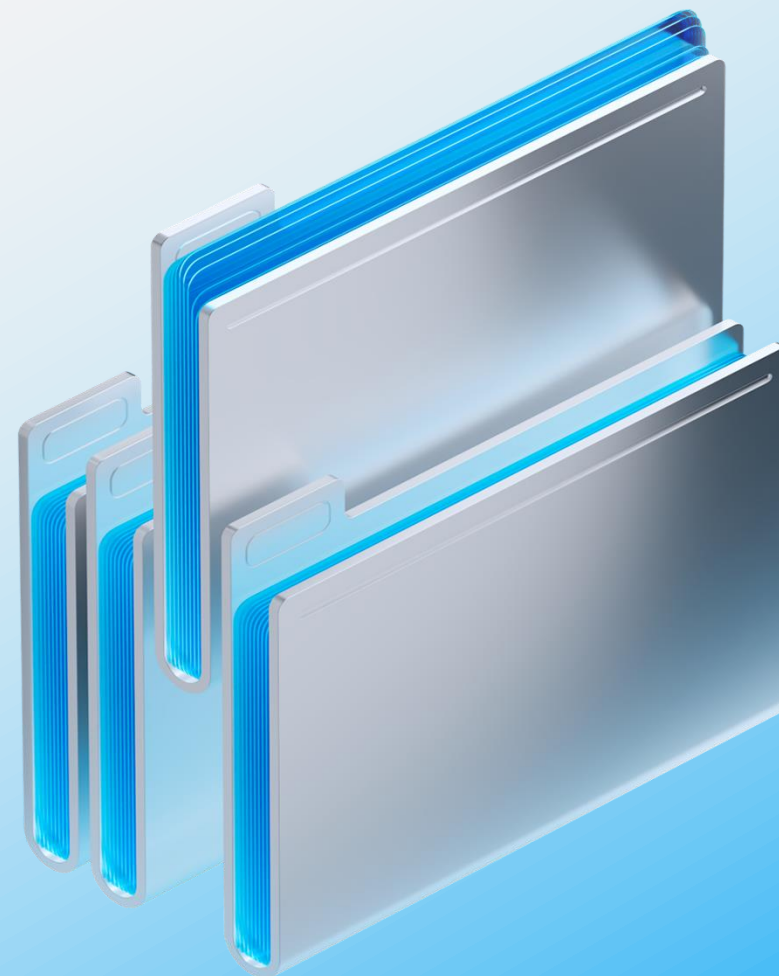
Большой разрыв между средними указывает на концентрацию потерь в отрасли (у малого числа крупных банков или крупных событий)

Орикс выходит за рамки ф.0409106



Бенчмарки за рамками ф.0409106

Численность и распределение
функционала в
Подразделении по управлению
операционным риском (ПУОР)



Бенчмарки по численности и функционалу ПУОР

Порядок формирования

- Цель – собрать бенчмарки, характеризующие численность и распределение функционала Подразделения УОР
- Вопросы были собраны в опросник
- Участвовать в опросе мог любой банк
- На основании обезличенных ответов будут рассчитаны бенчмарки и подготовлен отчет
- Отчет будет предоставлен всем участникам опроса
- Клиенты Орикс могут пройти опрос и увидеть результат в Орикс.

Бенчмарки по численности и функционалу ПУОР

Вопросы затрагивали количественный состав ПУОР и СУР, трудозатраты на исполнение типовых функций ПУОР, проникновение института риск-координаторов в банки

- **Количество работников** в ПУОР Банка
- Отношение **числа работников в ПУОР** к **общей** численности СУР Банка
- Отношение **числа работников в ПУОР** к **общей численности** персонала Банка
- **Общий объем трудозатрат** работников ПУОР (в ПШЕ) на:
 - развитие и поддержание системы ОНиВД
 - управление риском информационных систем и риском информационной безопасности
 - управление риском недобросовестного поведения
 - управление риском аутсорсинга
 - формирование отчетности по операционным рискам
 - разработку и поддержание методологии по операционному риску
 - разбор и классификацию событий операционного риска (в т.ч. анализ проводок, жалоб клиентов, выгрузок инцидентов ИБ/ИТ, и пр.)
- **Количество риск-координаторов** (т.е. работников вне ПУОР, ответственных за поддержку управления операционными рисками в своих подразделениях) в Банке
- Отношение количества риск-координаторов к количеству самостоятельных структурных подразделений Банка

Бенчмарки по численности и функционалу ПУОР

Общие выводы (отчет с фактурой будет предоставлен всем участникам опроса)

- Оставившие почту для участия в опросе получают опросник и инструкции для заполнения
- Отношение числа работников в ПУОР к общей численности персонала Банка тем ниже, чем выше размерный класс банка
- Лидер по трудозатратам в ПУОР – функционал по сбору данных о событиях,
- Второй по трудозатратам в ПУОР функционал – сбор отчетности
- Функция ОНиВД поддерживается в ПУОР в большинстве банков

Хотите получить отчет? Напишите на info@orixdata.ru для прохождения опроса

Спасибо
за внимание

Вопросы?

Если появятся
вопросы/предложения, пишите:
esyasakova@inno.tech

Елизавета Ясакова
Т1 Иннотех

