Антифрод-система – пять шагов к успеху

от НИП «Информзащита»

Информзащита
Системный интегратор

Опыт «Информзащиты»

ВТБ24

ВОЗРОЖДЕНИЕ БАНК

Промсвязьбанк

Открытие Банк

ТРАСТ

МДМ Банк

МОСКОВСКИЙ ИНДУСТРИАЛЬНЫЙ БАНК

Nb НОМОС БАНК

Банк Москвы

Информзащита
Системный интегратор

Антифрод-система – пять шагов к успеху

Шаг 1. Как выбрать антифрод-систему (функциональные критерии, стоимостные критерии, тестовое задание).

Шаг 2. Как обеспечить внедрение антифрод в срок и в максимальной комплектации

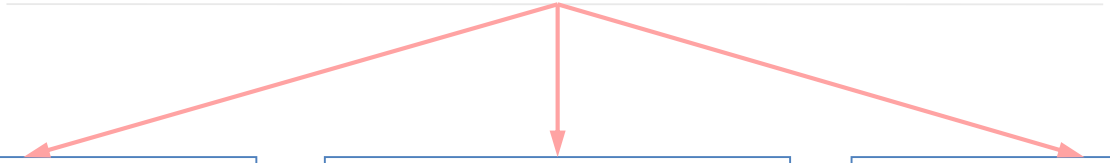
Шаг 3. Какие меры и инструменты из смежных областей могут снизить уровень мошенничества и злоупотреблений

Шаг 4. Основные участники внедрения антифрод-системы (компетентность команды внедрения)

Шаг 5. Структура эффективной антифрод-команды

Что такое антифрод и где он используется

Антифрод - это система для автоматического обнаружения подозрительного поведения и подачи уведомительных или блокирующих сигналов.



Банки

Банки используют антифрод для обнаружения и блокирования следующих операций:

1. Незаконных снятий с помощью:
   - карточных транзакций (банкоматы, POS-терминалы, карточные интернет покупки),
   - интернет-банк, мобильных приложений, киоски самообслуживания,
   - снятия по сговору в депозитных операциях, с неактивных счетов и пр.
2. Мошеннических кредитов:
   - в кредитных заявках (аппликационный),
   - накопительных (bust out fraud).
3. Злоумышленных фондовых операций, казначейских, рыночных.
4. Операций по отмыванию средств (AML)
5. См.ниже.

Телеком-операторы

Телеком-операторы используют антифрод для обнаружения и блокирования следующих операций:

1. Хищений у оператора посредством манипулирования трафиком, тарифами, бонусами, выплатами дилеров и агентов
2. Хищение у клиентов оператора посредством манипулирования трафиком
3. Хищение у клиентов оператора через:
   - интернет-банк,
   - мобильные приложения,
   - киоски самообслуживания,
   - через иные схемы мобильной коммерции
4. Создание ботсетей
5. См.ниже.

Нефтегазовые-компании

Нефтегазовые компании используют антифрод для обнаружения хищений и потерь в следующих областях:

1. Добыча
2. Переработка
3. Транспортировка
4. Хранение
5. Дистрибуция
6. Реализация

Любые крупные организации в т.ч. розничные сети

Используют антифрод для обнаружения и блокирования следующих операций:

1. Необычное поведение сотрудников, которое может быть подготовкой к совершению злоупотреблений (в т.ч. попытки ознакомления с информацией не входящей в компетенции сотрудников).
2. Хищение сотрудниками баз данных и внутренней информации
3. Манипуляции с услугами и работами, тарифами и бонусами, выплатами

Как работает антифрод

1. Настраиваются алгоритмы обнаружения подозрительности

Производится настройка фильтров, моделей аномального или злоумышленного поведения, моделей построения связей, баллов присваиваемых при срабатывании тех или иных алгоритмов, общего балла отсечения подозрительной активности.

2. Организуется подключение к источникам данных

Производится подключение к источникам данных для сбора аналитической информации

3. Осуществляется подключение к системам ожидающим результатов проверки

Например, системы исполнения расчетов, выдачи кредитов, контроля операций и т.д. могут ожидать блокирующих, разрешающих или уведомительных сигналов. Например, расчетные транзакции могут останавливаться и «ждать» разрешительного или запретительного сигнала от Анти-фрод системы. Если результат проверки Анти-фрод будет в серой зоне (не ясно), то такие сигналы попадают предварительно в группу верификации, которая принимает окончательное решение.

4. Организуется последующее совершенствование алгоритмов обнаружения подозрительности, актуализация и расширение источников данных

Изменения способов злоумышленных действий требует изменения алгоритмов их детектирования и источников этой информации.

Информзащита
Системный интегратор

Какие алгоритмы анализа использует антифрод

1. Фильтры (правила «если, то»)

Настройка фильтров, правил и условий, при совпадении с которыми система присваивает бал подозрительности или отправляет сигнал о подозрительности.

2. Прогнозные модели (расчет вероятности фрода)

На основании исторических данных операций (нормальных и злоумышленных) строится модель, которая будет обнаруживать аналогичные злоумышленные действия.

3. Модели аномального поведения

На основании исторических данных выделяются группы схожих операций, обнаружение операций принадлежащих к той или иной группе, в которых одна или несколько характеристик выбивается из характеристик этой группы.

4. Обнаружение связей с дискредитированными субъектами

Построение сложных сетей взаимосвязей клиентов, контрагентов и иных объектов анализа.
Анализ операции на предмет прямой или опосредованной взаимосвязи с дискредитированными объектами.

5. Обнаружение признаков дискредитации во внешних ресурсах (в т.ч. в интернете)

Назначение для объектов анализа признаков дискредитации, при обнаружении которых объект будет обозначаться подозрительным. Автоматическая проверка объектов в интернете и внешних ресурсах в контексте обозначенных признаков дискредитации
Анализ прямой или опосредованной взаимосвязи с дискредитированными признаками.

Информзащита
Системный интегратор

Шаг 1. Как выбрать антифрод (функциональные критерии)

Список алгоритмов детектирования

	поставщик 1	поставщик 2	поставщик 3	поставщик 4
1. Фильтры (правила «если, то»)	есть	есть	есть	есть
2. Прогнозные модели (расчет вероятности фрода)	есть	отсутствует	отсутствует	есть
3. Модели аномального поведения	есть	ограничено	ограничено	ограничено
4. Построение сети взаимосвязей и обнаружение связей с дискредитированными субъектами	есть	есть	есть	ограничено*
5. Обнаружение признаков дискредитации во внешних ресурсах (в т.ч. в интернете)	есть	есть	есть	есть

Дополнительная функциональность

1. Анализ неструктурированной информации и информации содержащей ошибки	есть	отсутствует	отсутствует	отсутствует
2. Агрегирования всех правил и алгоритмов выявления к конечному скорбалу с возможностью просмотра	есть	отсутствует	отсутствует	есть
3. Инструмент проведения расследований (досье инцидента, визуальная настройка Workflow)	есть	ограничено	ограничено	ограничено
4. Инструменты построения отчетности «налету»	есть	есть	есть	ограничено*
5. Возможность настройки алгоритмов детектирования и доп. функциональности без привлечения программистов				

Шаг 1. Как выбрать антифрод (стоимостные критерии)

Стоимостные критерии

	поставщик 1	поставщик 2	поставщик 3	поставщик 4
стоимость бессрочной лицензии / начальный платеж	0.0	0.0	0.0	0.0
или возможность годовой лицензии и её стоимость	0.0	0.0	0.0	0.0
стоимость сопровождения первого года производителем ПО	0.0	0.0	0.0	0.0
иные обязательные платежи за пользование ПО в первый год (например, от увеличения размера операций, трафика, активов и т.д.)	0.0	0.0	0.0	0.0
Итого стоимость системы первый год				
стоимость серверного и аппаратного оборудования	0.0	0.0	0.0	0.0
стоимость лицензий для функционирования серверного и аппаратного оборудования	0.0	0.0	0.0	0.0
Итого стоимость серверного и аппаратного оборудования	0.0	0.0	0.0	0.0
стоимость внедрения и кастомизации системы	0.0	0.0	0.0	0.0
стоимость сопутствующего консалтинга	0.0	0.0	0.0	0.0
Итого стоимость внедрения, кастомизации и консалтинга	0.0	0.0	0.0	0.0
Итого стоимость системы первый год	0.0 **млн.руб**	0.0 **млн.руб**	0.0 **млн.руб**	0.0 **млн.руб**
- стоимость лицензии на второй год (или сумма лицензионных платежей, например с учётом плановых объемов операций и т.д.)	0.0	0.0	0.0	0.0
- стоимость ежегодного сопровождения и обслуживания	0.0	0.0	0.0	0.0
Итого ежегодная стоимость второго и последующих годов	0.0 **млн.руб**	0.0 **млн.руб**	0.0 **млн.руб**	0.0 **млн.руб**

Шаг 1. Как выбрать антифрод (тестовое задание)

Этап	Задачи
Этап 1. Подготовительные мероприятия	Заказчик получает у конкурсантов получает список полей на основании которых их Антифрод система производит присвоение детектирование признаков подозрительности. Заказчик сопоставляет эти списки полей со своим (с учетом перспектив появления у себя новых полей), определяет конечный список полей, который Заказчик сможет поддерживать по каждой транзакции. После этого Заказчик готовит три списка транзакции (со всеми заполненными полями): - «Тестовый список транзакций №1» (например, не менее 15 тыс. транзакций) - «Тестовый список транзакций №2» (например, не менее 15 тыс. транзакций) - «Обучающий список злоумышленных транзакций» (например, не менее 1 тыс. транзакций) «Обучающий список нормальных транзакций» (например, не менее 50 тыс. транзакций) для обучения скоринговой карты Антифрод системы (желательно чтобы он был реальным, но обезличенным)
Этап 2. Проверка эффективности Антифрод систем конкурсантов («вшитых» правил детектирования)	Всем участникам конкурса рассылается «Тестовый список транзакций №1» (например, не менее 15 тыс. транзакций) Конкурсанты должны прислать этот список с указанием для каждой транзакции дополнительно шести полей: 1) фродовый балл 2) фродовый балл - вероятность фрода в процентах (от 0 до 100%), 3) пояснения причин присвоения балла для администратора / аналитика АФ системы (текстовое описание) 4) источник присвоения признака (какое правило сработало / скоринговая карта) 5) отметка о том была бы эта транзакция заблокирована системой или нет (заблокирована / незаблокирована) 6) пояснение критичности причин для блокирования транзакции для администратора / аналитика АФ системы (текстовое описание) Конкурсанты должны предоставить результаты в два этапа: Первый этап - в списках заполняются только поля 1 и 5 (здесь дополнительно оценивается скорость фильтрации) Второй этап - с заполнением остальных полей (здесь оценивается качество и детализированность информации)

Шаг 1. Как выбрать антифрод (тестовое задание)

Этап	Задачи
Этап 3. Проверка эффективности их Антифрод («самообучающейся» скоринговой карты)	Всем участникам конкурса рассылаются «Тестовый список транзакций №2» (не менее 15 тыс.) и «Обучающий список злоумышленных транзакций» (например, не менее 1 тыс. транзакций) «Обучающий список нормальных транзакций» (например, не менее 50 тыс. транзакций) для обучения скоринговой карты Антифрод системы Конкурсанты должны прислать Тестовые списки транзакций №1 и №2 с указанием для каждой транзакции дополнительно шести полей: 1) фродовый балл 2) фродовый балл - вероятность фрода в процентах (от 0 до 100%), 3) пояснения причин присвоения балла для администратора / аналитика АФ системы (текстовое описание) 4) источник присвоения признака (правила / скоринговая карта) 5) отметка о том была бы эта транзакция заблокирована системой или нет (заблокирована / незаблокирована) 6) пояснение критичности причин для блокирования транзакции для администратора / аналитика АФ системы (текстовое описание) Конкурсанты должны предоставить результаты в два этапа: Первый этап - в списках заполняются только пол 1 и 5 (здесь дополнительно оценивается скорость самообучения карты, скорость фильтрации) Второй этап - с заполнением остальных полей (здесь оценивается качество и детализированность информации) Конкурсантам объявляется, что оценка будет производится по качеству блокирования, отсутствию ложных срабатываний, детализированности и понятности для администратора / аналитика АФ системы описаний причин присвоения бала и причин блокирования транзакции, скорости анализа; скорости самообучения скоркарты, качеству самообучения скоркарты. Конкурсантам может быть объявляно, что в случае выигрыша внедряемые у Заказчика правила АФ системы и настройки скоринговой карты АФ системы должны быть в том же состоянии, что и на момент тестирования и давать сходные результаты (в т.ч. результатов скоринговой карты).

Необходимо с осторожность относится к таким критериям сравнения как эффективность срабатываний и доля ложных срабатываний (т.к. очень много зависит от алгоритмов детектирования, а также уязвимостей процессов (например, СМС-пароль отправляется без IMSI кода). Эти критерии больше подходят к Антифрод команде, которая будет использовать саму систему.

Шаг 2. Как обеспечить внедрение антифрод в срок и в максимальной комплектации

Структурирование сделки. Условия, гарантирующие внедрение системы в установленные сроки и в максимальной комплектации

1. Включение в договор внедрения **подробнейших бизнес-требований** с указанием штрафных санкций при отсутствии соответствующей функциональности к определенной дате. Включение в договор лицензии условий обслуживания, технической поддержки и доработок системы

2. Истребование **наилучших условий оплаты**:
   - оплата лицензии после внедрения (trial версия на период внедрения)
   - оплата внедрения частями
   - штрафные санкции за просрочку внедрения
   - фиксация размера ежегодных платежей на конкретный период
   - включение работ по обслуживанию и технической поддержке в сумму лицензионных платежей

3. **Особенности условия договоров**:
   - условия расторжения договора
   - приоритетный язык договора
   - место разрешения споров

4. Квалифицированное **оформление и подписание документов:**
   - подписание договоров сначала контрагентами, одномоментное подписание договоров внедрения и лицензии- сшив договоров

Информзащита
Системный интегратор

Шаг 3. Какие меры и инструменты из смежных областей могут снизить уровень мошенничества и злоупотреблений

1. Эффективность процедур верификации

Защищенность процедур верификации – например, рассылка СМС паролей с проверкой IMSI кода.

Включение дополнительных линий верификации в т.ч. в фоновом режиме или режиме облегченного использованиям – например, видео и аудио верификация.

Защита данных, используемых в верификации и уведомлениях – например, при изменении полей досье клиента в т.ч. номера телефона используемых для верификации (досье клиента – телефон для уведомлений.

2. Распространение верификации на все инструменты управления счетом

Например, операций по изменению верификация изменения данных, используем.

3. Расширенное использование уведомлений по значимым операциям

Например, при изменении номера телефона (отправкой СМС на старый номер), при заказе крупной суммы, при снятии крупной суммы, при подключении нового инструмента управления счетами и т.д.

4. Установление ограничений инструментов платежей в состоянии «по умолчанию»

Например, установление лимитов операций (в день в разрезе инструментов и счетов). Или, например, ограничение (отключенность) по умолчанию интернет банка, запрет интернет покупок («включение» которых производится по специальному требованию клиента).

5. Защита средств платежа

Например, использование чипованных карт, использование технологий верификации интернет покупок (таких как 3D secure и пр.).

6. Использование дополнительных инструментов

Программно-аппаратные средства защиты (в т.ч. антивирусы) для всех компонентов системы (в т.ч. для мобильных средств управления счетами).

Шаг 4. Основные участники внедрения антифрод системы (компетентность команды внедрения)

Участники внедрения антифрод:

1. **Представители Заказчика**
2. **Представители команды внедрения**
3. **Представители разработчика решения**

Команда	Задачи
Представители Заказчика	Бизнес-требования, тендер, выбор оптимального решения, привлечение специалистов ИТ внутри заказчика, контроль работ, контроль исполнение требований
Представители команды внедрения	Внедрение, кастомизация, обучение, документация
Представители команды внедрения	Поддержка при возникновении проблемных ситуаций при внедрении и кастомизации ПО

Компетентная команда внедрения помимо своих задач помогает заказчику выполнить и его задачи - прежде всего сформировать бизнес-требования и провести тендер, выбрать оптимальное решение.

Т.е. команда внедрения не привязана к одному конкретному решению.

Шаг 5. Структура эффективной антифрод команды

Четыре отдела:

1. **Отдел детектирования**
2. **Отдел верификации**
3. **Отдел расследований**
4. **Отдел контроля**

Название отдела	Задачи отдела	Ключевые показатели эффективности (KPI) отдела
Отдел детекти-рования	1. Настройка алгоритмов автоматического обнаружения подозрительного поведения: 1. Фильтры (правила «если, то»), 2. Прогнозные модели (расчет вероятности фрода), 3. Модели аномального поведения, 4. Обнаружение связей с дискредитированными субъектами, 5. Обнаружение признаков дискредитации во внешних ресурсах (в т.ч. в интернете) 1. Актуализация всех нормативных документов, схем процессов, методик и инструкций по своему отделу	1. Увеличение количества обнаруженных инцидентов 2. Увеличение сумм обнаруженных инцидентов 3. Увеличение доли обнаруженных инцидентов к общему количеству проверенных операций 4. Снижение доли ложных сигналов о подозрительности к общему количеству проверенных операций 5. Снижение доли сигналов, требующих верификации (сигналов серой зоны) к общему количеству проверенных операций 6. Увеличение количества источников аналитической информации
Отдел верифи-кации	1. Верификация всех заблокированных и подозрительных операций; 2. Подтверждение / неподтверждение инцидента; 3. Разблокирование / заблокирование верифицированных операций 4. Учет количества ошибочных срабатываний об инцидентах Отдела детектирования 5. Актуализация всех нормативных документов, схем процессов, методик и инструкций по своему отделу	1. Сокращение времени верификации подозрительных операций 2. Снижение количества верификаций с ошибками (операция была разблокирована, но в последствии оказалась мошеннической) 3. Увеличение количества верифицированных операций на одного верификатора 4. Обработка 99% сигналов в срок не более 20 минут на один сигнал (или иной норматив)

Шаг 5. Структура эффективной антифрод команды

Название отдела	Задачи отдела	Ключевые показатели эффективности (KPI) отдела
Отдел рассле-дований	1. Подробное разбирательство по всем подтвержденным инцидентам; 2. Ведение списка видов инцидентов и отнесение инцидентов к одному из видов 3. Улучшение алгоритмов детектирования инцидентов конкретного вида 4. Разработка и назначение мероприятий, процедур, механизмов недопущения повторения инцидентов конкретного вида и рекомендаций на изменение процессов, для недопущения повторений инцидентов этого вида; 5. Подготовка материалов к привлечению к ответственности виновных в инцидентах; 6. Учет количества ошибочных верификаций Отдела верификации 7. Актуализация всех нормативных документов, схем процессов, методик и инструкций по своему отделу	1. Снижение количества повторений инцидентов конкретного вида 2. Увеличение количества рекомендаций по недопущению инцидентов, актуальность которых подтверждена подразделением аудита 3. Увеличение количества привлеченных к дисциплинарной ответственности сотрудников ФК 4. Увеличение количества привлеченных к уголовной ответственности сотрудников ФК и третьих лиц 5. Увеличение сумм возмещения убытков, нанесенных фродовыми операциями
Отдел контроля	1. Актуализация плановых значений ключевых показателей эффективности (KPI) всех отделов Антифрод-подразделения и контроль их достоверности 2. Актуализация форм отчетности всех отделов Антифрод-подразделения и контроль их достоверности 3. Контроль актуализации регламентных документов, методик и инструкций всех отделов Антифрод-подразделения 4. Контроль правильности Кластеризация инцидентов по группам 5. Коррекция KPI других отделов 6. Актуализация всех нормативных документов, схем процессов, методик и инструкций по своему отделу 7. Контроль правильности отнесения Отделом расследований инцидентов к одному из видов инцидентов 8. Актуализация всех нормативных документов, схем процессов, методик и инструкций по своему отделу	1. Увеличение количества получателей отчетности Антифрод-подразделения 2. Увеличение количества положительных отзывов по отчетности (по , по эффективности Антифрод-подразделения, по качеству и удобности отчетности) 3. Обеспечение достоверности и актуальности документации и отчетности Антифрод-подразделения 4. Увеличение количества обнаруженных ошибок в работе отделов Антифрод-подразделения 5. Обеспечение ежегодного обновление всех нормативных документов Антифрод-подразделения

Смежные решения -
Комплексное управление рисками на базе eGRC

Информзащита
Системный интегратор

Решение для комплексного управления инцидентами, рисками и угрозами всех категорий

на платформе систем eGRC (Governance, Risk and Compliance)

*Решение не охватывает управление кредитными и рыночными рисками

Издержки на обработку инцидентов

Факт 1. Компания несёт существенные издержки на обработку инцидентов и угроз

- **масштаб расходов: от 7 до 25 процентов ФОТа и сопутствующих расходов***
  от 15 до 30 департаментов (см. таблицу ниже), включая всех функционально подчиненных им территориальных сотрудников, полностью или частично заняты работой с инцидентами и угрозами
- **эффективность расходов: полутора-трехкратное завышение трудозатрат на обработку инцидентов**
  работа этих служб с инцидентами и рисками зачастую не автоматизирована и не стандартизирована
- **эффективность работ: недостаточная**
  отсутствует контроль за работой с инцидентами со стороны надзорной службы (риск службы, или комплаенс службы, или службы внутреннего контроля) по причине отсутствия сводной детализированной он-лайн отчетности по всем инцидентам и рискам, с возможностью детализации

№	Вид инцидентов, рисков и угроз	Название ответственного подразделения
1	Нарушения обслуживания клиентов, жалобы клиентов	Подразделение клиентского сервиса
2	Брак, несоответствие качества продуктов и процедур (в т.ч. внутренних) установленным критериям	Подразделение качества
3	Претензии и иски к компании, претензии и иски от компании	Юридическое подразделение
4	Внутреннее и внешнее мошенничество в бизнес-процессах; заключение клиентами / контрагентами договоров без намерения их оплаты; завышение / занижение сумм,	Подразделение по противодействию мошенничеству и злоумышленным действиям
5	Злостные уклонения от погашения задолженности	Подразделение по взысканию задолженности
6	Нарушения использования основных и оборотных активов, закупок и продаж	Подразделение по управлению имуществом
7	Нарушения функционирования инфраструктуры	Административно-хозяйственное подразделение
8	Нарушения хода исполнения проектов	Проектное подразделение
9	Технологические и программные сбои	Подразделение технологий и поддержки
10	Неэффективность и нелогичность бизнес-процессов	Подразделения методологии
11	Инциденты и угрозы информационной безопасности	Подразделение информационной безопасности
12	Злоумышленные действия по экономической и внутренней безопасности	Подразделение общей безопасности
13	Трудовые споры, нарушения охраны труда, промышленной и пожарной безопасности	Подразделение по работе с персоналом
14	Нарушения финансовой прозрачности, экономической стабильности, иные нарушения	Подразделения внутреннего аудита и контроля
15	и т.д.	

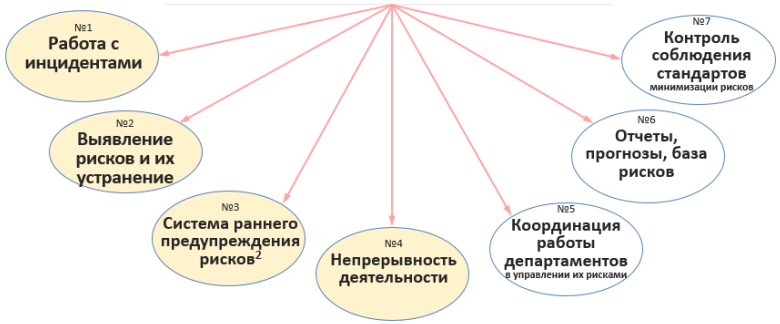
*ФОТ- фонд оплаты труда, сопутствующие расходы – аренда площадей, логистика и пр.

GRC инструменты для управления рисками. Что это.

Какие GRC инструменты мы поможем внедрить (визуальная схема).

Мы предлагаем внедрение всех инструментов управления рисками
как по отдельности, так и комплексно

Семь инструментов (компонентов)
для управления рисками



[1] Цветом выделены наиболее актуальные для заказчика решения (по нашим оценкам).
[2] **Система раннего предупреждения (№3 на схеме) включает 8 инструментов: (1). Самооценку рисков (в т.ч. инструмент анкетирования)** - Risk and control self-assessment – RCSA; (2). **Ключевые индикаторы рисков** - Key risk indicators – KRIs; (3) **Ключевые показатели эффективности управления риском** - Key performance indicators – KPIs; **(4) Ключевые контроли риска** - Key control indicators– KCIs; **(5) Сценарный анализ рисков и стресс-тестирование** - Scenario analysis, Stress tests; **(6) Анализ внешних потерь от операционных рисков** - External loss data; **(7) Ведение и оценка карт рисков (реестра рисков)** - Risk maps; **(8) Расчет размера риска** - VaR OpRisk.

Преимущества НИП Информзащита

наличие у наших сотрудников **успешного практического опыта** внедрения компонентов системы управления риском более чем в 10 компаниях и банках со следующими характеристиками:

1. **От 1000 до 7000 пользователей GRC системы.**
2. **От 120 до 800 экспертов по инцидентам.**
3. **От 14 до 45 владельцев профильного риска.**
4. **От 1000 до 40000 обрабатываемых инцидентов в месяц.**
5. **От 40 до 3000 обрабатываемых проблем в месяц.**
6. **От 70 до 300 ключевых индикаторов риска**
7. **и т.д.**

Наши сотрудники имеют следующие преимущества:
- первое в России внедрение GRC системы (в 2009 г. SAS GRC в одной из крупных организаций);
- четырехлетний опыт последующего ведения и оптимизации GRC системы;
- продвинутая методология процессов GRC (подтвержденная публикацией книги по GRC, статей, участием в рабочих группах (например, Ассоциации российских банков) и разработкой документов по GRC, участием в конференциях))

Также на текущий момент НИП «Информзащита» исполняет ряд проектов по внедрению систем управления риском в других организациях (в незавершенной стадии). В состоянии ожидании несколько тендеров, решение по которым заказчиками еще не принято.

Спасибо за внимание!

1. Мы поможем Вам сформировать бизнес-требования

2. Мы поможем сравнить различные антифрод-системы (у нас уже есть сравнительные таблицы)

3. Мы поможем внедрить и кастомизировать выбранное решение

4. Кроме этого мы поможем внедрить систему комплексного управления рисками eGRC

5. Мы проведем экспресс аудит действующих систем и процессов и поможем повысить их эффективность

Вам была представлена краткая презентация

За более подробной информацией - обращайтесь!

Информзащита
Системный интегратор