Минимизация операционных и репутационных рисков банка: сервис для мониторинга критичных событий и действий пользователей в системе

Юлия СОХОВА,
ведущий менеджер отдела
по развитию Банковских Продуктов, ГК ЦФТ

ЦФТ

FT meet up MOSCOW

Мониторинг критичных событий и действий пользователей в системе ЦФТ-Банк

1. Формирование базы данных о действиях пользователей в системе ЦФТ-Банк

2. Проведение внутренних расследований по инцидентам экономической и информационной безопасности

3. Непрерывный мониторинг событий в системе по заданным правилам

Формирование базы данных о действиях пользователей в системе ЦФТ-Банк

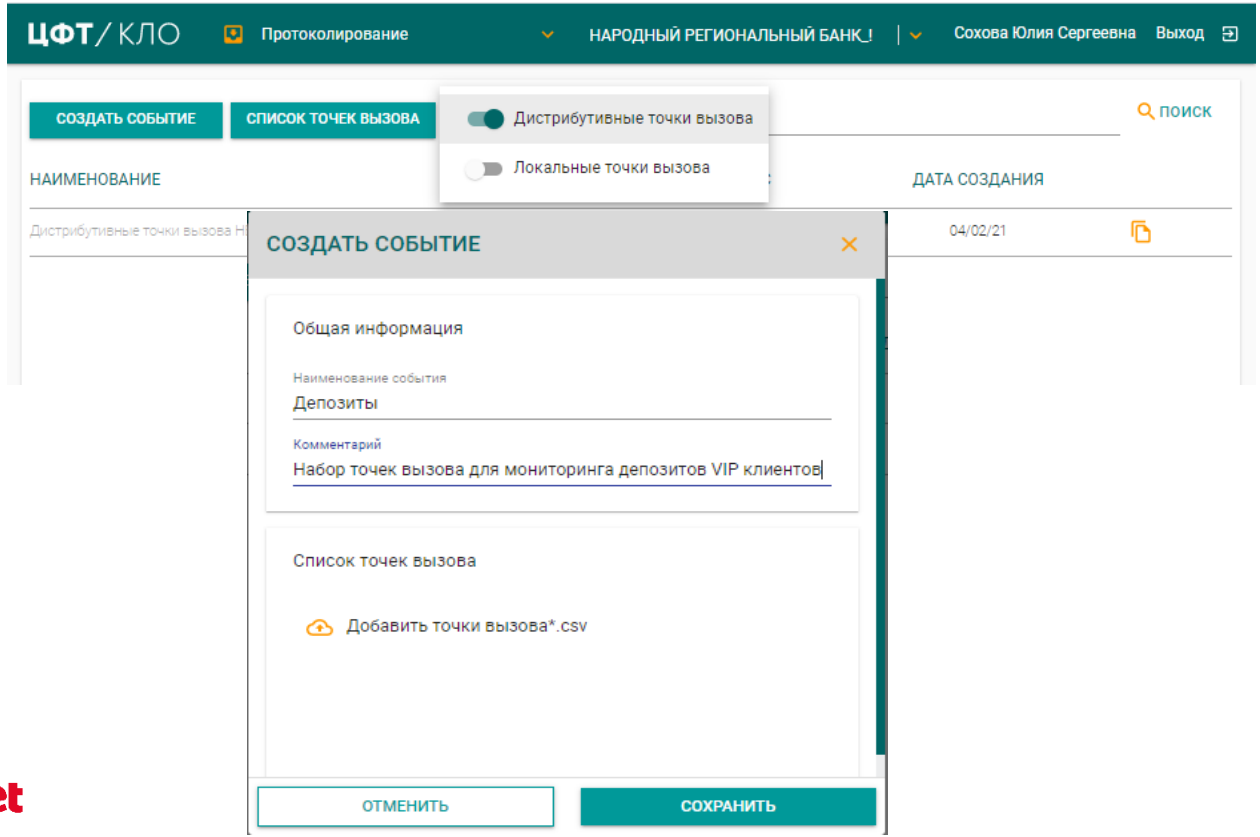
ДО

- Затраты на хранение данных
- Высокая нагрузка на продуктовую базу
- Потеря данных при точечном журналировании
- При расширении функций системы настройка требует обновления

ПОСЛЕ

- Удобный инструмент настройки протоколирования
- Хранение обезличенных данных в облаке. Сокращение затрат на хранение
- Уменьшение нагрузки на продуктивную базу за счет автоматического удаления логов
- Возможность увеличения набора событий и их атрибутов для формирование базы данных
- Автоматический контроль полноты набора событий при тотальном протоколирование

Формирование базы данных о действиях пользователей в системе ЦФТ-Банк



Проведение расследований по инцидентам экономической и информационной безопасности

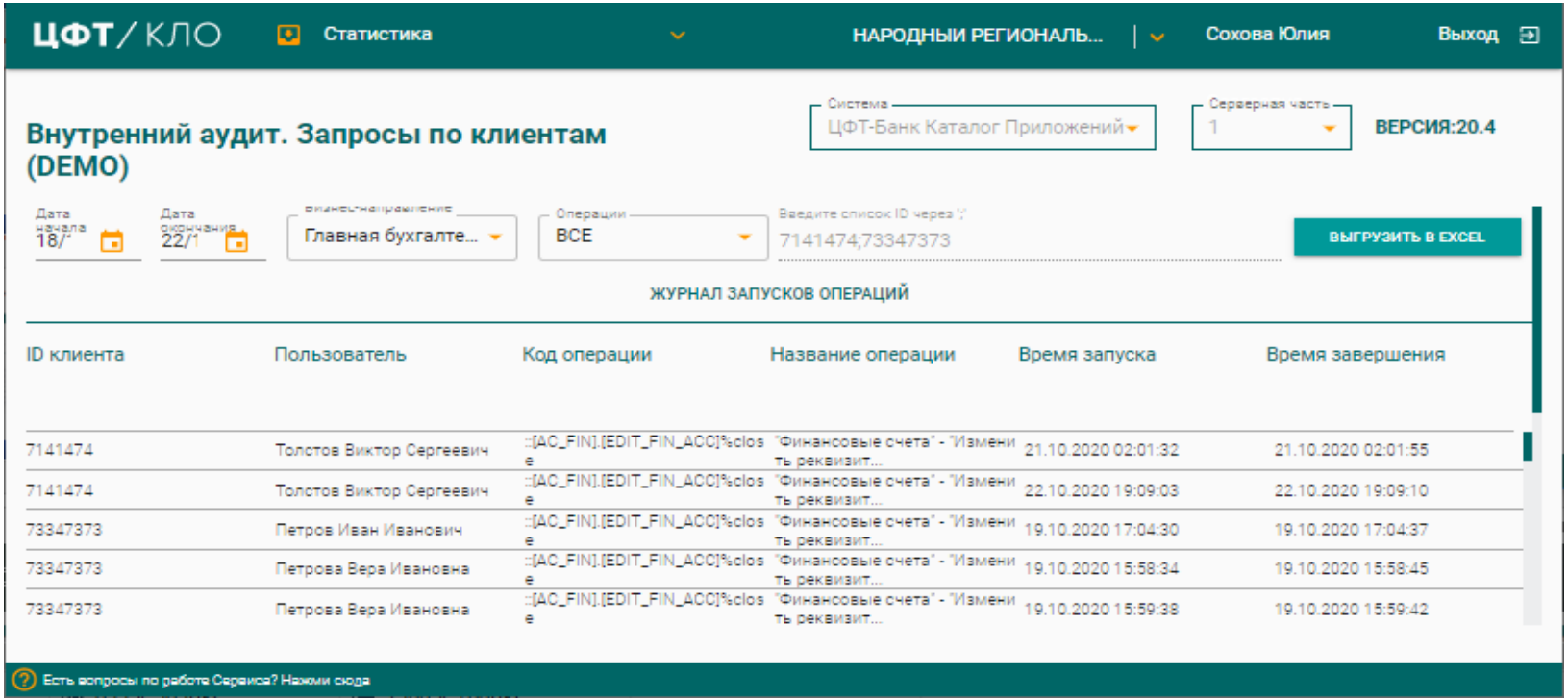
ДО

- Привлечение сотрудников IT-департамента
- Высокие ресурсные и временные затраты
- Большая вероятность искажение результатов расследования в связи с недостаточностью данных

ПОСЛЕ

- Удобный интерфейс для проведения расследований (на входе достаточно ID клиента или экземпляра)
- Управление доступом к отчетам в Личном Кабинете
- Формирование отчета в течение нескольких минут
- Доступен единый отчет по всем договорам и счетам клиента
- На выходе журнал операций с полной информацией по расследуемым событиям
- Возможность обогащения журнала операций дополнительными атрибутами

Проведение расследований по инцидентам экономической и информационной безопасности

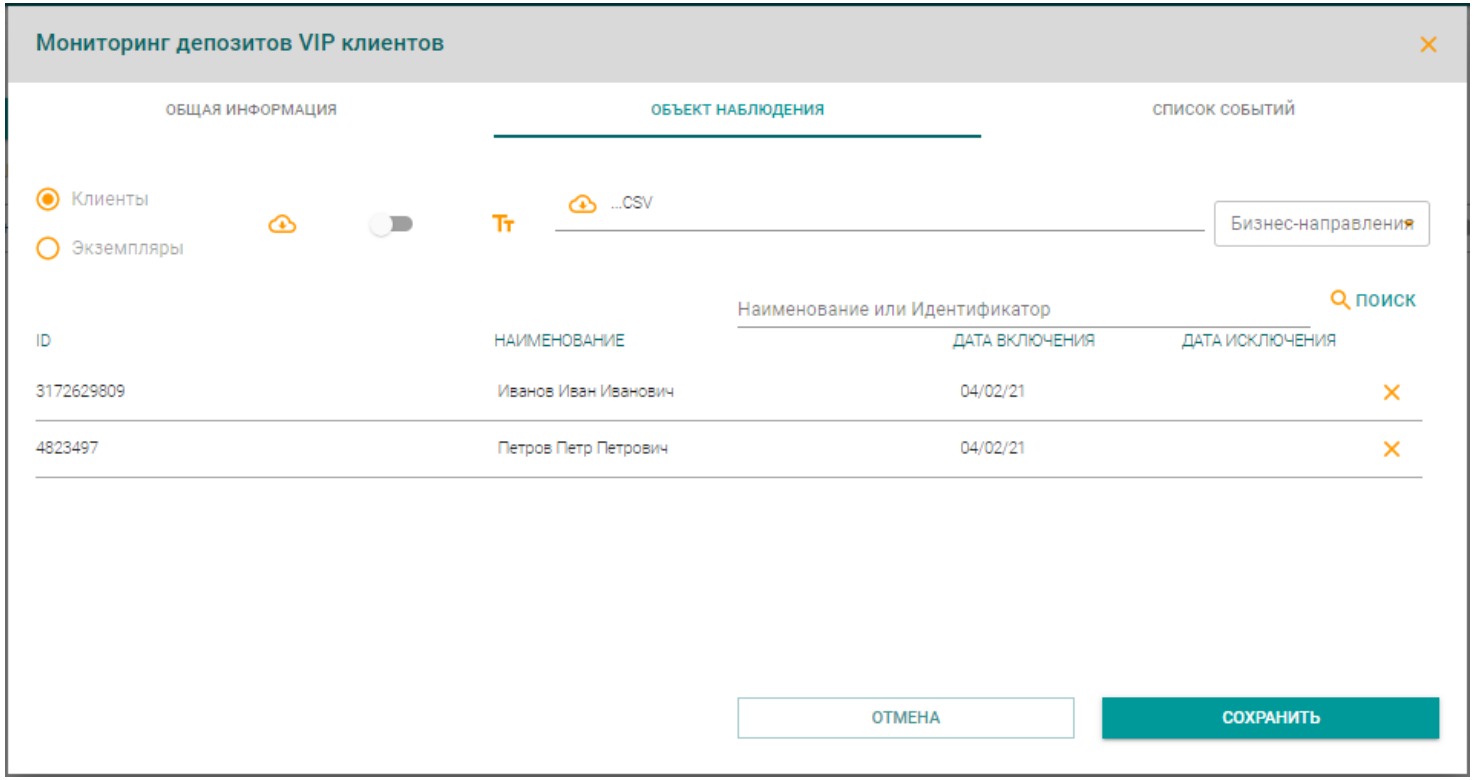


Непрерывный мониторинг событий в системе по заданным правилам

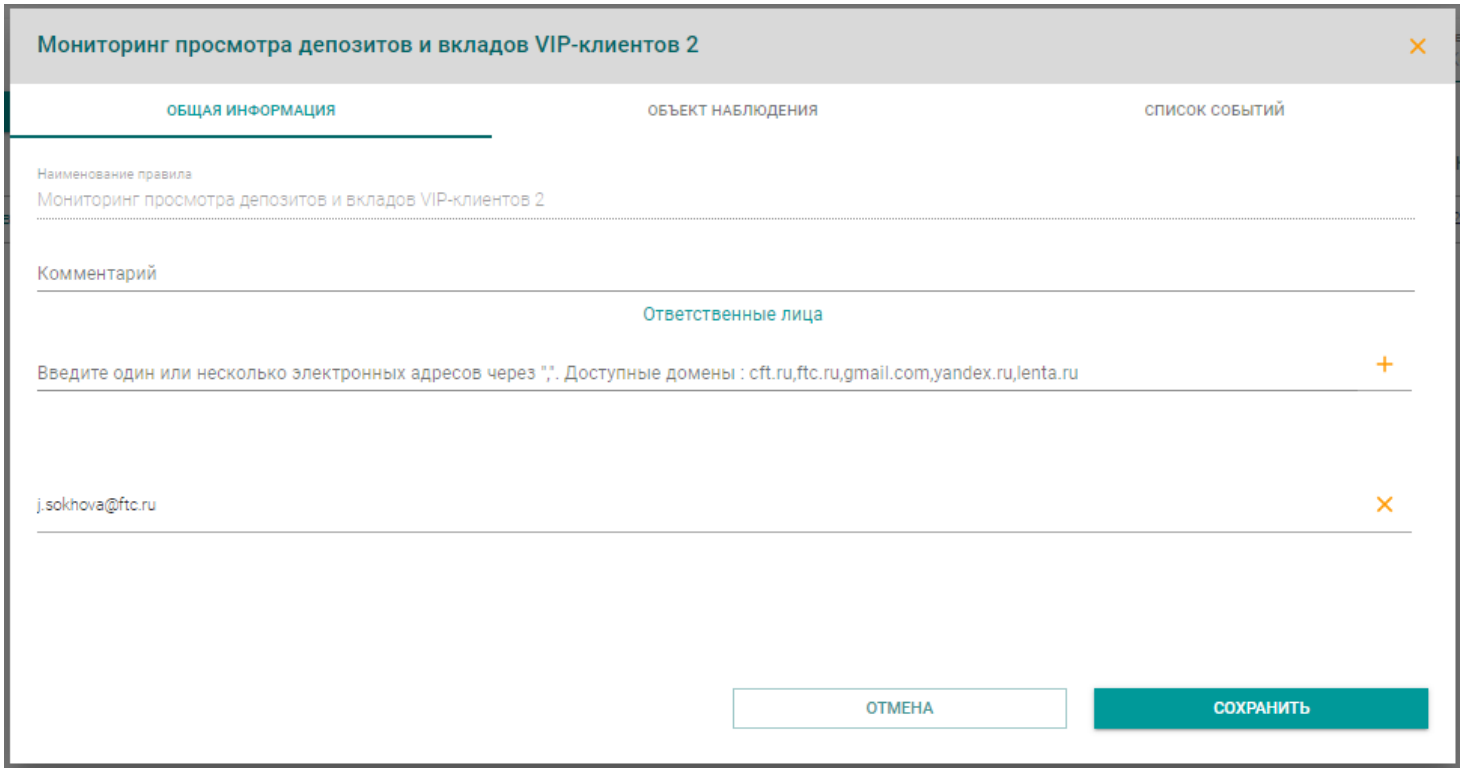
ПОСЛЕ

- Удобный инструмент настройки правил наблюдения по клиентам и их договорам/конкретным экземплярам в системе
- Система уведомлений о возникновении событий, требующих дополнительного контроля
- Уведомление ответственного лица в течение 1 часа после возникновения события
- Возможность интеграции с SIEM-системой Банка
- Формирование профиля пользователя, анализ поведенческих моделей, выявление характерных и нехарактерных профилю пользователя операций

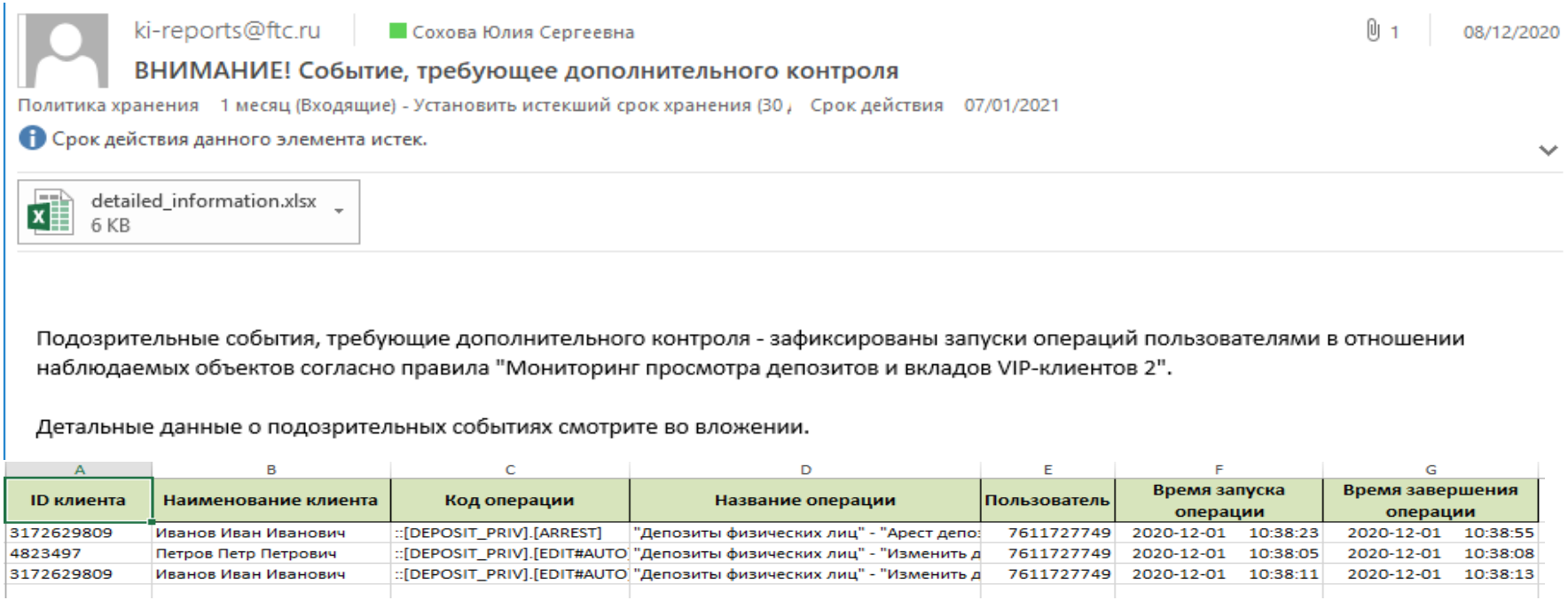
Непрерывный мониторинг событий в Системе по заданным правилам



Непрерывный мониторинг событий в Системе по заданным правилам



Непрерывный мониторинг событий в Системе по заданным правилам



ki-reports@ftc.ru | Сохова Юлия Сергеевна | 1 | 08/12/2020

ВНИМАНИЕ! Событие, требующее дополнительного контроля

Политика хранения 1 месяц (Входящие) - Установить истекший срок хранения (30 , Срок действия 07/01/2021

Срок действия данного элемента истек.

detailed_information.xlsx
6 KB

Подозрительные события, требующие дополнительного контроля - зафиксированы запуски операций пользователями в отношении наблюдаемых объектов согласно правила "Мониторинг просмотра депозитов и вкладов VIP-клиентов 2".

Детальные данные о подозрительных событиях смотрите во вложении.

A	B	C	D	E	F	G
ID клиента	Наименование клиента	Код операции	Название операции	Пользователь	Время запуска операции	Время завершения операции
3172629809	Иванов Иван Иванович	::[DEPOSIT_PRIV].[ARREST]	"Депозиты физических лиц" - "Арест депо:	7611727749	2020-12-01 10:38:23	2020-12-01 10:38:55
4823497	Петров Петр Петрович	::[DEPOSIT_PRIV].[EDIT#AUTO	"Депозиты физических лиц" - "Изменить д	7611727749	2020-12-01 10:38:05	2020-12-01 10:38:08
3172629809	Иванов Иван Иванович	::[DEPOSIT_PRIV].[EDIT#AUTO	"Депозиты физических лиц" - "Изменить д	7611727749	2020-12-01 10:38:11	2020-12-01 10:38:13

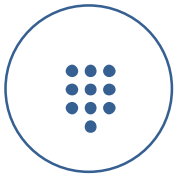
Системный подход
в работе с инцидентами

Минимизиция операционных
и репутационных рисков банка

MOSCOW ftmeetup

Порядок подключения к услуге

1. Оформление Дополнительного Соглашения
2. Получение доступа к Личному Кабинету Банка
3. Лицензирование Приложения ЦФТ-Статистика и подключение отчетов «Запросы по экземплярам», «Запросы по клиентам» для подключения пакета «Инструменты выявления событий в системе»
4. Лицензирование Приложения «Мониторинг пользователей» для подключения пакета «Инструменты мониторинга событий в системе»



Информация о тарифах,
технических требованиях по ссылке
https://www.cft.ru/pages/support_services

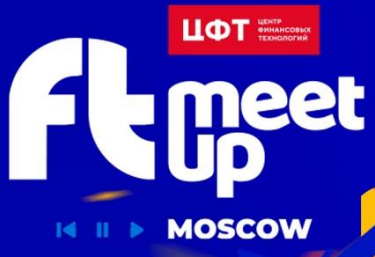
По вопросам подключения
и работы сервиса
обращайтесь по адресу
lk-support@cft.ru

Сравнительный анализ групп доступа и действий пользователей в системе

Группа доступа	Операции, не используемые в группе более 1 года
Депозиты (физические лица) Инспектор	Депозиты физических лиц - "Расчет %% по договору" (закрытие)
	Депозиты физических лиц - "Закрыть договор" (закрытие)
	Депозиты физических лиц - "Изменить депозитный договор" (закрытие)
	Платежные карты - "Выпустить карту" (закрытие)
	Денежные переводы физических лиц - "Редактировать исходящий перевод" (закрытие)
Кредиты. Кредитный инспектор (физические лица)	Кредиты частным лицам - "Выдача кредита" (закрытие)
	Кредиты частным лицам - "Регистрация условия реструктуризации" (закрытие)

Сравнительный анализ групп доступа и действий пользователей в системе

Группа доступа	Пользователи, которые не используют группу доступа более 1 года	ФИО
Зарплата и кадры	1458744	Иванов Иван Иванович
	6461431	Стрельцов Эдуард Петрович
	545137854	Васильев Олег Васильевич
	1875415	Иванова Ольга Петровна
	1457577	Лукина Татьяна Васильевна
Специалист валютного контроля	544577755	Петрова Елена Петровна
	544541465	Домаев Лев Васильевич
	544445555	Куравлев Василий Петрович



СПАСИБО ЗА ВНИМАНИЕ!

Юлия СОХОВА,
ведущий менеджер отдела по развитию
Банковских Продуктов, ГК ЦФТ
e-mail: j.sokhova@ftc.ru