X5 RETAIL GROUP

Актуальные вопросы ИБ в ритейле.

Пятерочка Перекресток супермаркет Гипермаркет КАРУСЕЛЬ

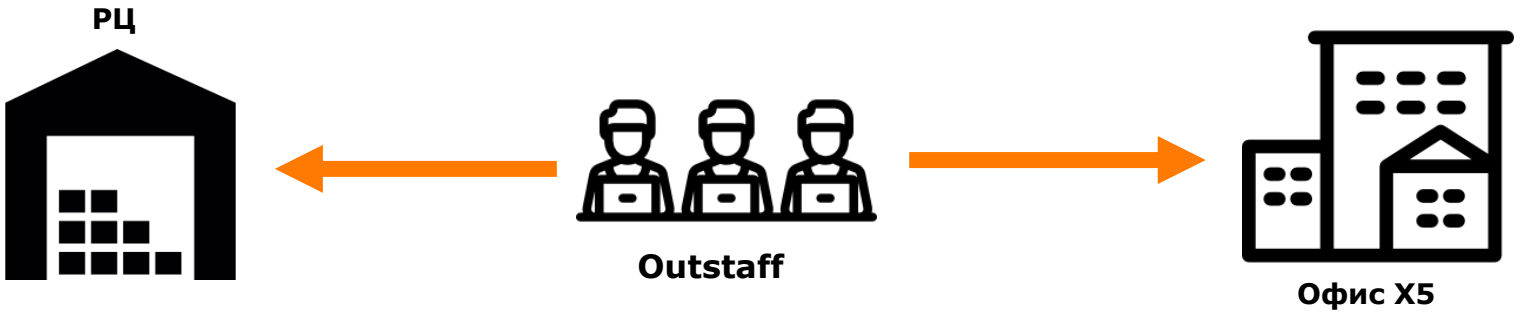
X5 RETAILGROUP : 10 ЛЕТ РАЗВИТИЯ

	2006	2016	
	1,6 магазинов в день	5 магазинов в день	в 3 раза больше открытий магазинов каждый день
	619 магазинов	7 397 магазинов*	в 12 раз увеличелось количество магазинов
	466 тыс. кв. м торговых площадей	3 514 тыс. кв. м* торговых площадей	в 8 раз возросло количество торговых площадей
	5 распределительных центров	35 распределительных центров	в 7 раз больше распределительных центров

	2006	2016	
	**18** субъектов РФ	**53** субъекта РФ	**+35** субъектов РФ за 10 лет
	**33 828** сотрудников	**149 736** сотрудников*	в **4** раза увеличелось количество сотрудников
	**445,8** млн покупателей	**2 468** млн покупателей**	в **6** раз увеличелось количество покупателей
	**76,2** млрд руб.	**808,8** млрд руб.**	в **11** раз увеличилась выручка
	**8,1** млрд руб.	**55,2** млрд руб.**	в **7** раз увеличелся показатель EBITDA

** на 31.12.2015 * на 31.03.2016

3PL операторы на РЦ



Риски

Несанкционированный доступ.

Мошенничество.

Митигация рисков

Двухфакторная аутентификация.

Система мониторинга активности пользователей.

Ведение товара в 2 системах и корреляция.

ЕГАИС РАР

ФЗ-54 О применении ККТ

Риски

КТ передается третьим лицам.

При высокой нагрузке микропроцессора ФН, процесс шифрования чеков не будет осуществляется.

Митигация рисков

Создания своего ОФД или использование аффилированного.

Защита канала связи.

Участие в проектной деятельности

- Анализ архитектуры
- Определение рисков
- Составление требований
- Определение путей митигации рисков
- Контроль реализации

3 торговых сети

84 проекта

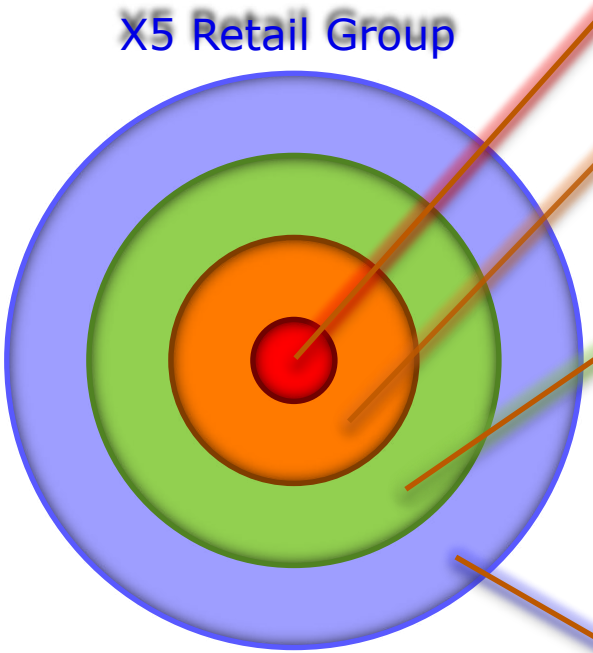
20 уровней детализации

Checklist

Осуществляется ли обработка персональных данных?	Осуществляется ли обработка коммерческой тайны?	Осуществляется ли взаимодействие сервисов по защищённым протоколам?	Используется ли сервисная учётная запись для взаимодействия с внутренними сервисами Компании?	Реализовано ли управление учётными записями и их правами в Системе?
Проводится ли разработка ПО в рамках внедрения Системы?	Описана ли процедура обновления программного и системного обеспечения?	Размещается ли Веб-сервер приложений в DMZ-сети, при необходимости доступа к нему из сети Интернет?	Сервер Системы на котором установлен web-сервер выполняет только основную функцию? (Не совмещает с функциями DNS, Firewall, SMTP….)	Сервер СУБД Системы располагается во внутреннем сегменте сети компании?
Осуществляется ли регистрация событий Системы и присутствует ли возможность передачи событий во внешнюю систему мониторинга и корреляции событий?	Доступ пользователей в Систему из сети Интернет осуществляется по защищённым протоколам?	Осуществляется ли подключение к Системе через мобильные устройства (IOS, Android, Windows) средствами корпоративной MDM-системы?	Присутствует ли полное описание всех компонентов Системы и подсистем?	Присутствует ли общая схема/архитектура Системы с привязкой к архитектуре корпоративной информационной сети Компании с отображением связей (односторонних/двухсторонних /множественных),
Под рисунком схемы/архитектуры присутствует таблица «Параметры портов и протоколов взаимодействия»?	Используются ли средства автоматического резервного копирования и восстановления Системы?	Резервное копирование производится на специально выделенные сервера?	Резервные копии Системы зашифрованы или восстановление копии осуществляется по паролю?	Имеет ли внешний подрядчик (внешние пользователи) или его Системы удалённый доступ в сеть Компании?

Построение эшелонированной защиты Компании

Построение системы информационной безопасности на разных уровнях



Уровень приложения

- контроль внешних бизнес-приложений

Уровень сотрудника

- контроль контента информационных потоков

Уровень внутреннего периметра

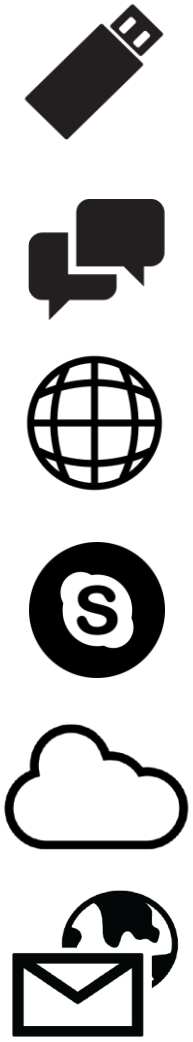
- контроль периметра
- обнаружение вторжений
- внутренняя сегментация сети
- контроль подозрительных (опасных) подключений NetFlow
- мониторинг событий и инцидентов
- Контроль подключений устройств к сети (NAC)

Уровень внешнего периметра

- мониторинг событий и инцидентов
- Контроль периметра
- Обнаружение вторжений
- Контроль подключений устройств к сети (NAC)
- Контроль контента информационных потоков

Среда эксплуатации DLP системы.

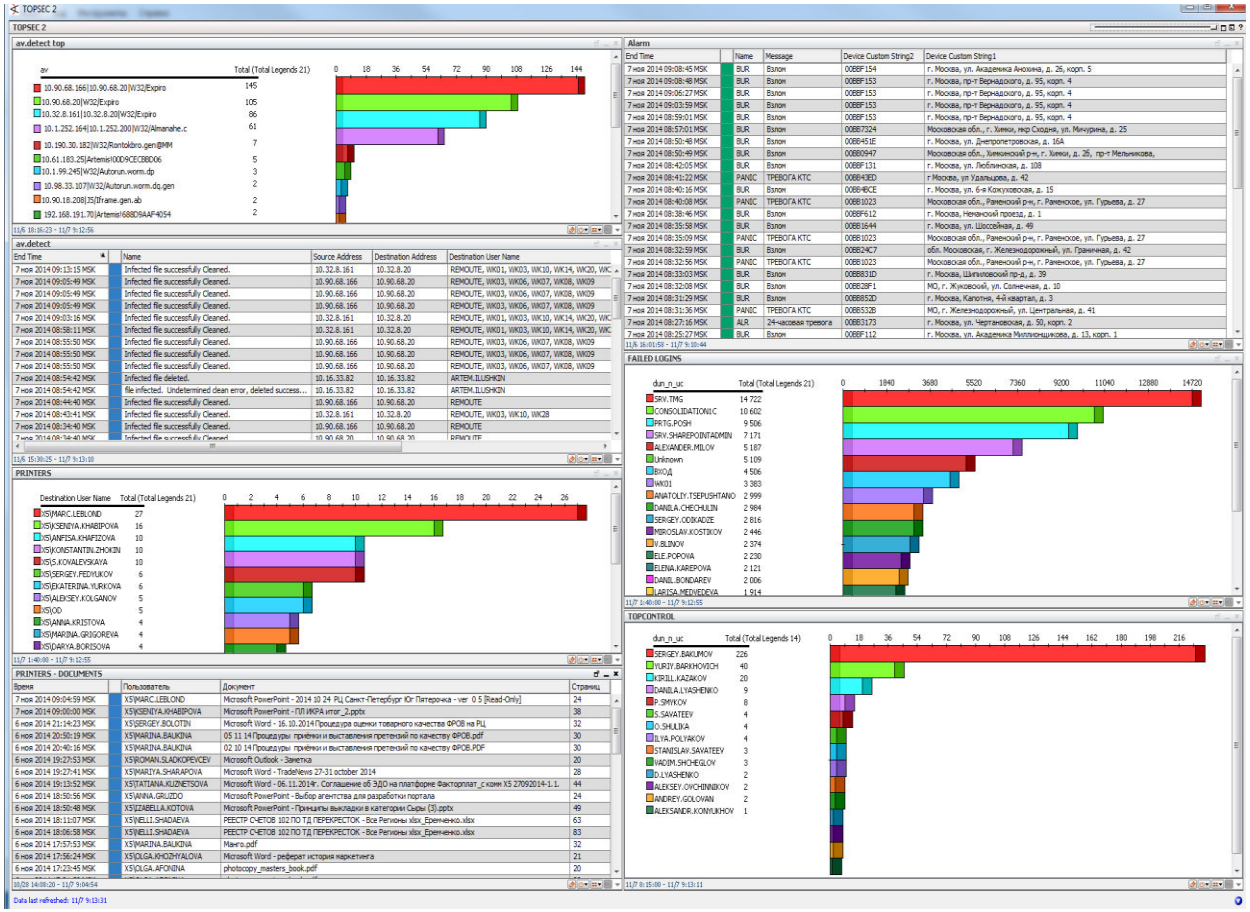
EndPoint agents



Network Sniffer mirroring

- **Каналы связи сильно нагружены бизнесом.**
- **Политика высокой открытости и доступности.**
- **Корпоративная почта шифруется.**
- **Большие объемы контролируемой и защищаемой информации.**
- **Сложная архитектура сети, территориальная распределенность.**

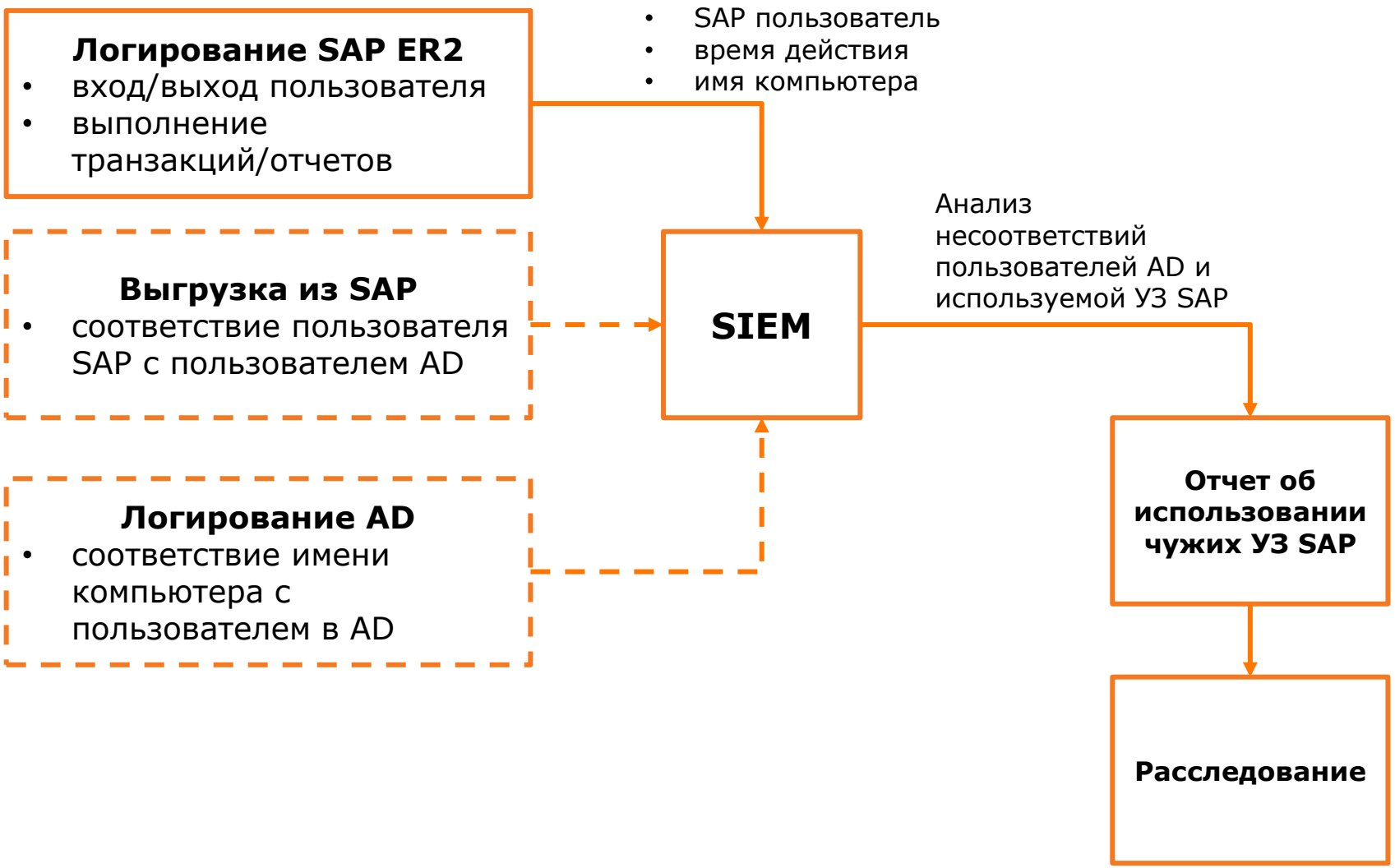
Security Operation Center



SOC X5 Retail Group в первую очередь используется для анализа систем фиксации событий ключевых информационных систем Компании. Система предназначена для корреляции различного вида событий из различных систем и акцентировать внимание сотрудников подразделений ИБ на наиболее важных или аномальных событиях. Система SOC получает события от почти пятисот устройств двадцати двух различных типов. В сутки система получает и обрабатывает порядка трёхсот миллионов базовых событий информационной безопасности. Для выявления инцидентов информационной безопасности и аномалий, разработано порядка трёхсот правил корреляции. Для работы аналитиков разработано более ста отчетов и семидесяти дашбордов.

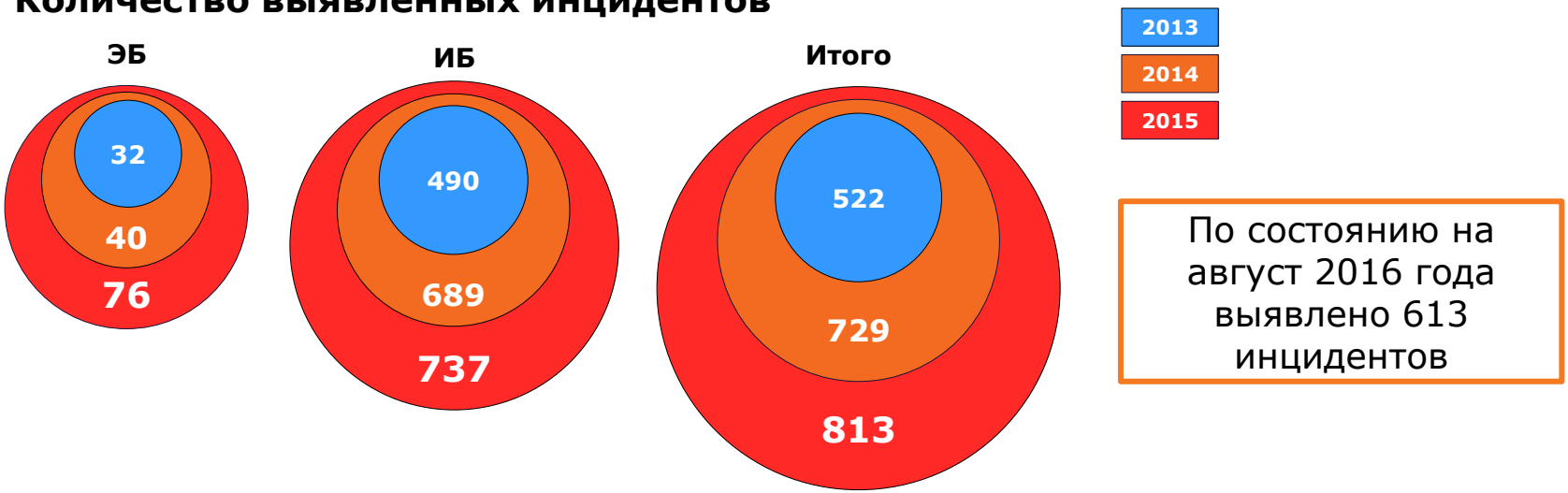
X5 RETAIL GROUP

Структура анализа SAP для целей сохранения коммерческой тайны

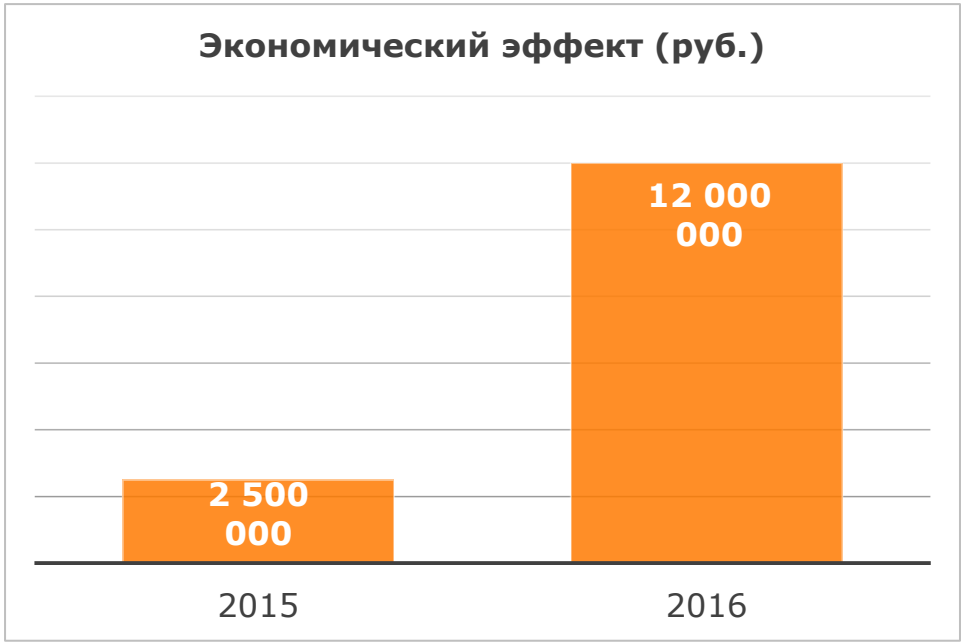


Результаты работы УИБ за 2013-2016 года

Количество выявленных инцидентов



По состоянию на август 2016 года выявлено 613 инцидентов



Заключенные с контрагентами договора по неразглашению коммерческой тайны и дополнительного соглашения по информационной безопасности позволили взыскать с контрагентов штрафы за нарушение требований X5 Retail Group.

Структура IdM и ее цели

Формализация процесса управления доступом и связанных с ним подпроцессов в АС

- Обследование существующей инфраструктуры АС, формализация функциональных требований;
- Проведение аудита процесса управления доступом в АС;
- Разработка организационных и технических рекомендаций по совершенствованию процесса управления доступом;
- Разработка организационно-распорядительной и внутренней нормативной документации, формализующей процесс управления доступом и связанных с ним подпроцессов в АС.

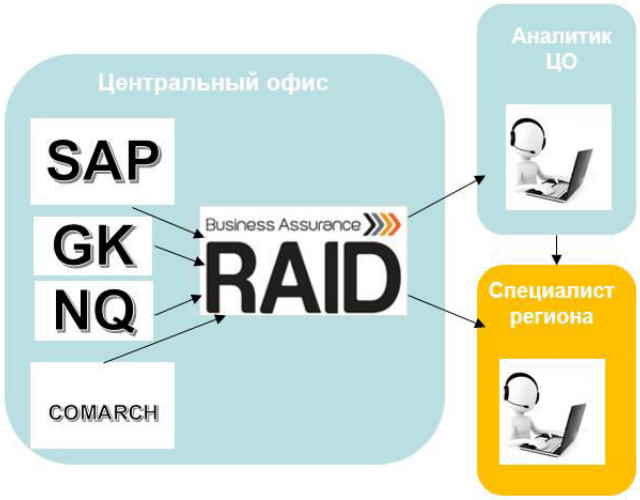
Автоматизация управления и аудита жизненного цикла УЗ, прав доступа пользователей к АС

- Разработка технического задания на создание системы, автоматизирующей управление и аудит жизненным циклом учетных записей пользователей и правами этих учетных записей в АС;
- Разработка инструкций и консультирование ИТ-специалистов по доработке и настройке АС в части реализации функционала, позволяющего автоматизировать управление и аудит жизненного цикла учетных записей пользователей и правами этих учетных записей в АС;
- Внедрение системы, автоматизирующей управление и аудит жизненным циклом учетных записей пользователей и правами этих учетных записей в АС;
- Разработка проектной и эксплуатационной документации.

Обеспечение однократной аутентификации пользователей в АС

- Разработка технического задания на создание системы, обеспечивающей однократную аутентификацию пользователей в АС;
- Разработка инструкций и консультирование ИТ-специалистов Заказчика по доработке и настройке АС в части реализации функционала однократной аутентификации;
- Установка и настройка модуля однократной аутентификации на автоматизированных рабочих местах пользователей и терминальных серверах;
- Разработка проектной и эксплуатационной документации.

Существующая архитектура системы противодействия мошенничеству



Источники данных:

- данные о кассовых операциях (закрытые чеки)
- мастер данные
- транзакции процессинга программы лояльности
- Интеграция с информационными системами HR

В настоящий момент происходит развитие системы в направлении

интеграции с информационными системами обеспечения логистических операций и товародвижения в магазинах

Система обеспечивает:

- Сбор и преобразование разнородных данных из различных систем компании;
- Аналитическую обработку собранных данных и выявление в них фактов мошенничества и его признаков;
- Управление процессом расследования инцидентов (workflow)

Реализованные контрольные процедуры.

Контроль кассовый операций:

- Мошенничество с картами лояльности
- Фиктивные возвраты
- Умышленное уменьшение суммы чека

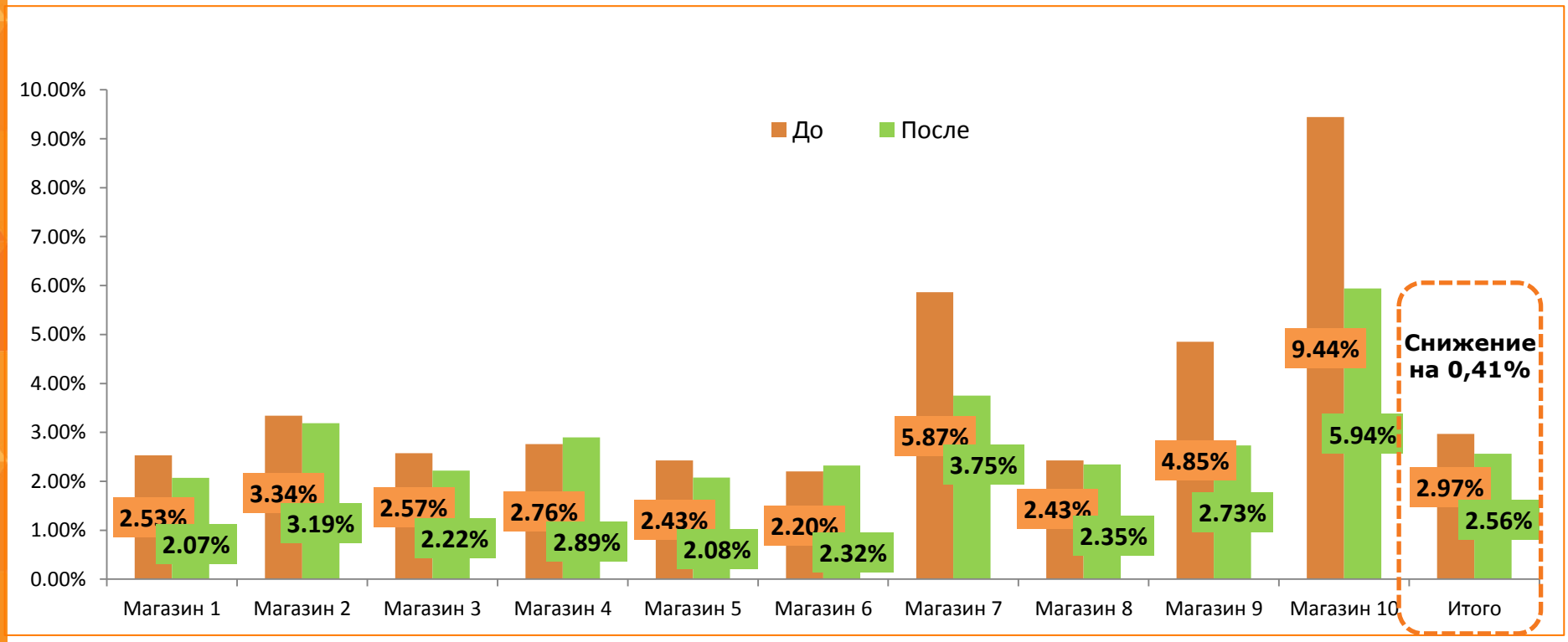
Контроль бизнес-процессов магазина

- Создание фиктивных излишков
- Сокрытие недостач
- Контроль списаний

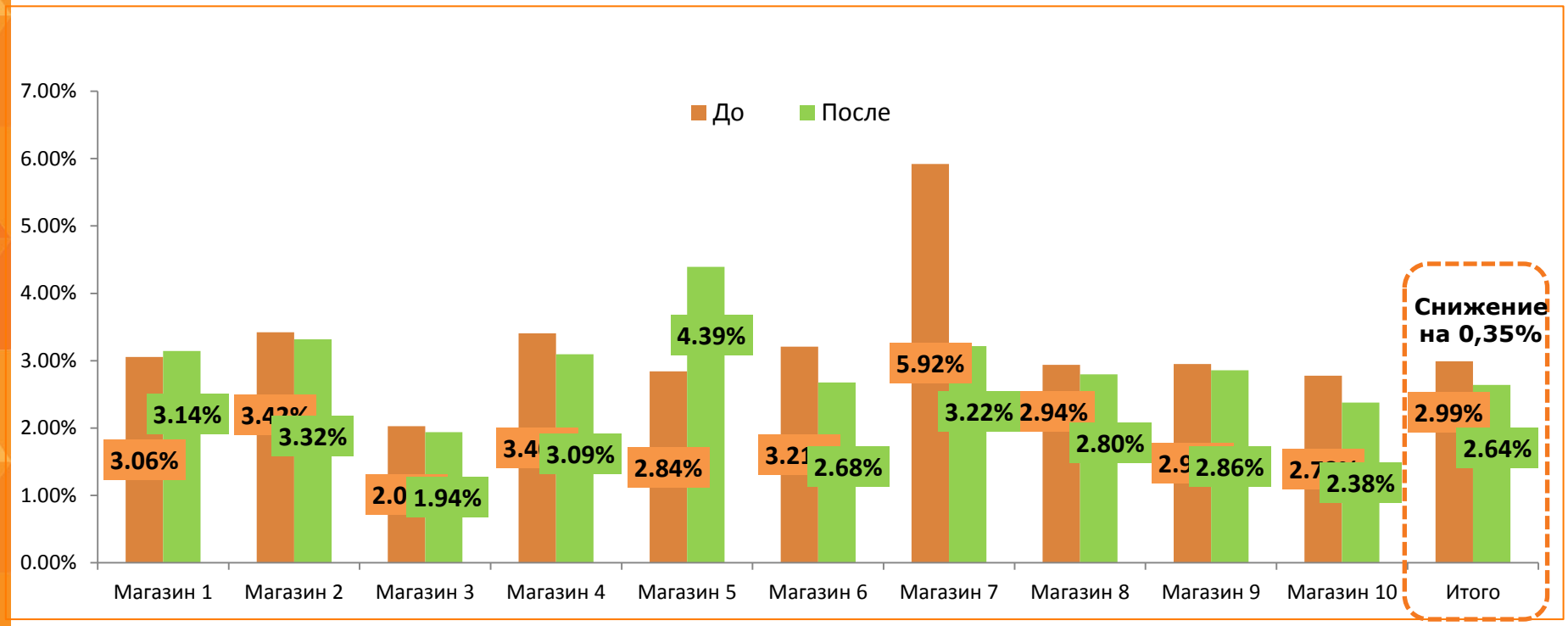
Контроль товародвижения

- Превышение объемов заказа
- Прогноз списаний
- Мониторинг всей цепочки движения товара от заказа до РКУ

Результаты фокусной группы №1



Результаты фокусной группы №2



Бизнес-выгоды:

Выявление мошеннических схем

Сокращение потерь компании

Возможность фиксировать попытки совершения мошенничества и оперативно реагировать на них;

Предотвращение хищений и мошенничества на этапах их подготовки (до того, как мошенничество станет свершившимся фактом);
предотвращение несанкционированных действий сотрудников;

Формирование статистических сведений по всему объему операций и составление моделей деятельности по различным уровням организации бизнес-процессов (территориальным, организационным и пр.) для дальнейшего их анализа и совершенствования.

X5 RETAIL GROUP

Алексей Овчинников

Начальник Управления информационной безопасности

Тел.: +7 (495) 662-88-88 доб.10-211
Моб.: +7 (963) 926-49-25
Эл.адрес: Aleksey.Ovchinnikov@x5.ru

Пятерочка Перекресток Карусель