ИНФОБЕЗ В НОВЫХ РЕАЛИЯХ:
ГЛАВНЫЕ УГРОЗЫ ДЛЯ БИЗНЕСА

Павел Карасев
Бизнес-партнер
ООО “Компьютерные технологии”

Давайте знакомиться

- Более 15 лет опыта работы в международных и российских компаниях на различных должностях в сфере информационных технологий.
- Спикер более 50-ти российских и международных конференций, посвящённых внедрению BI, ERP, CRM и других ИТ технологий.
- Обладатель звания QlikView Charter Luminary 2014.
- Лучший докладчик CFO Russia 2015, 2019 и 2023.
- Участник рейтинга ТОП-100 ИТ-лидеров РФ

ЦИФРОВИЗАЦИЯ

процесс, который одновременно оптимизирует работу компаний и является источником новых ИБ-угроз.

Цифровая трансформация сопровождается взрывным ростом объема данных, и данные сами по себе превращаются в ценный актив.

Оцифровывать бизнес-процессы,
устанавливать новое ПО,
но не ставить защитные решения, – это
как покупать красивый диван
вместо входной двери в квартиру.

Немного статистики

1

Более 90% утечек связано с внутренними нарушениями.

Исследование Varonis

2

Более 59 млрд.$ – ежегодные потери из-за утечек данных.

По данным мониторинга Министерства связи РФ

3

Количество инцидентов увеличивается на 21-52% ежегодно.

На режиме самоизоляции количество утечек возросло в 5 раз!

Отчет Cost of Data Breath Report

4

Более 34% утечек связано с преднамеренным и осознанным действием персонала компаний.

По данным РБК

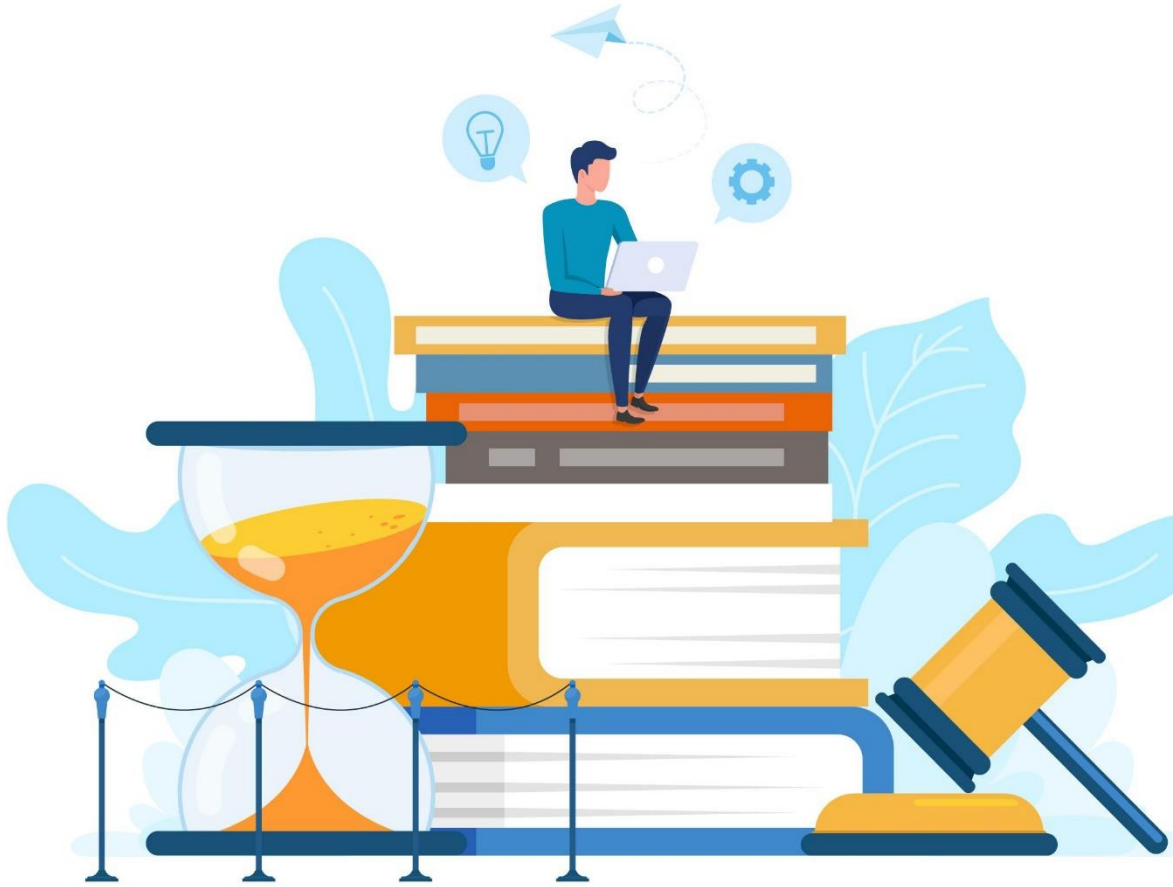
НОВОЕ В ЗАКОНОДАТЕЛЬСТВЕ:

Новый порядок отчетности о компьютерных инцидентах с ПДн:

- Персональная ответственность руководителя за состояние ИБ в организации (Указ №250).
- Сокращение списка операторов, которые могут НЕ регистрироваться в РКН.
- Необходимость предоставлять результаты расследования.
- Отмена моратория на проверки.

ОЖИДАЕМ В 2024

- Рост размера административной и введение уголовной ответственности за реализацию ПДн.
- Введение оборотных штрафов за утечки данных.



Ответственность за нарушения с ПДн: 2024

- **Законопроект № 502104-8 «О внесении изменений в КоАП РФ»:**

Нарушение	Объем штрафа для физических лиц	Объем штрафа для должностных лиц	Объем штрафа для организаций и ИП
Незаконная обработка ПДн (ч. 1 ст. 13.11 КоАП)	**10-15 тысяч** рублей, х2 при повторном нарушении	**50-100 тысяч** рублей, х2 при повторном нарушении	**150-300 тысяч** рублей, х2 при повторном нарушении
Неуведомление об утечке ПДн	**50-100 тысяч** рублей	**400-800 тысяч** рублей	**1-3 млн** рублей
Утечка ПДн (в зависимости от числа похищенных записей/пострадавших)	**100-400** тысяч рублей	**800 тысяч -2 млн** рублей	**3-15 млн** рублей
Повторная утечка ПДн	**400-600 тысяч** рублей	**2-4 млн** рублей	**0,1-3% выручки** за год (15-500 млн р.)
Утечка ПДн **специальных** категорий	**300-400 тысяч** рублей	**1,5-2 млн** рублей	**10-15 млн** рублей
Повторная утечка ПДн **специальных** категорий	**500-800 тысяч** рублей	**3-5 млн** рублей	**0,1-3% выручки** за год (20-500 млн р.)

- **Законопроект № 518022-8:**

Снимается мораторий на проверки Роскомнадзора в случае утечек ПДн

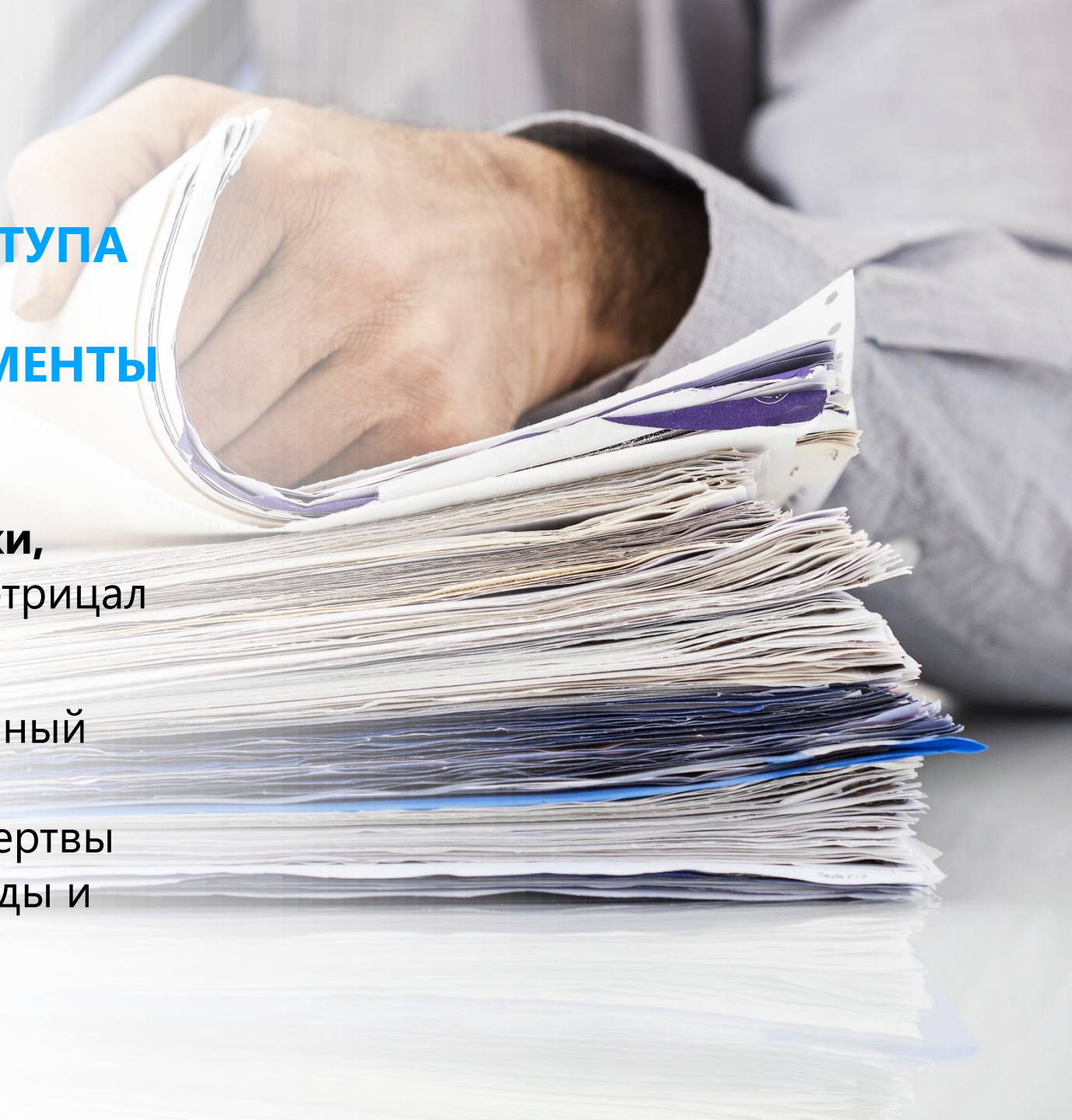
ТОП-7 ПРОБЛЕМ

В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:

1. Утечки персданных, клиентских баз, коммерческой тайны и др.;
2. Работа на сторону/ на конкурентов
3. Фирмы-боковики
4. Откаты
5. Удаленная работа
6. Безделье на работе
7. Негативные высказывания о компании и руководстве в соцсетях и др.

1. СЛИВ ДАННЫХ

КЕЙС: У СОТРУДНИКА БЕЗ ДОСТУПА К ДАННЫМ НАЙДЕНЫ КОНФИДЕНЦИАЛЬНЫЕ ДОКУМЕНТЫ



DLP обнаружила на ПК сотрудника **документы по оценке геомеханики, разведочным работам**. Работник отрицал причастность.

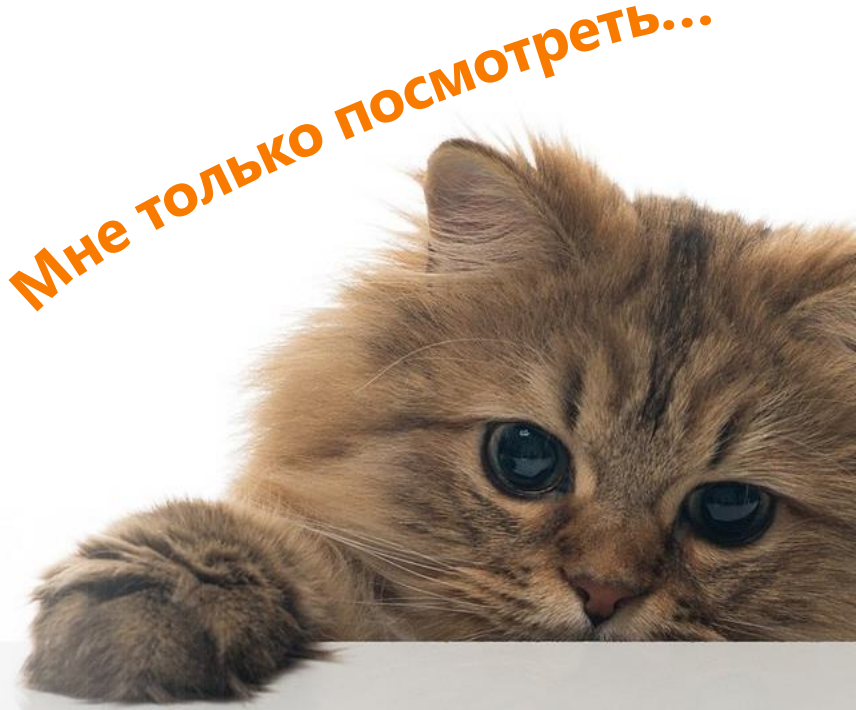
Расследование показало, что системный администратор с помощью средств удаленного доступа хранил на ПК жертвы информацию – с целью замести следы и **передать данные третьим лицам**.

2. РАБОТА НА КОНКУРЕНТОВ

IT-СПЕЦИАЛИСТ «ЗЕРКАЛИЛ» ПОЧТУ ТОП-МЕНЕДЖЕРОВ

Что произошло: IT-специалист подключил дополнительный e-mail к корпоративной почте. На его ящик «зеркалились» письма двух топ-менеджеров – коммерческого и генерального директоров.

Расследование: оказалось, что доступ к ящику был еще у прямых конкурентов. Они знали о каждом шаге и стратегическом решении руководства компании.



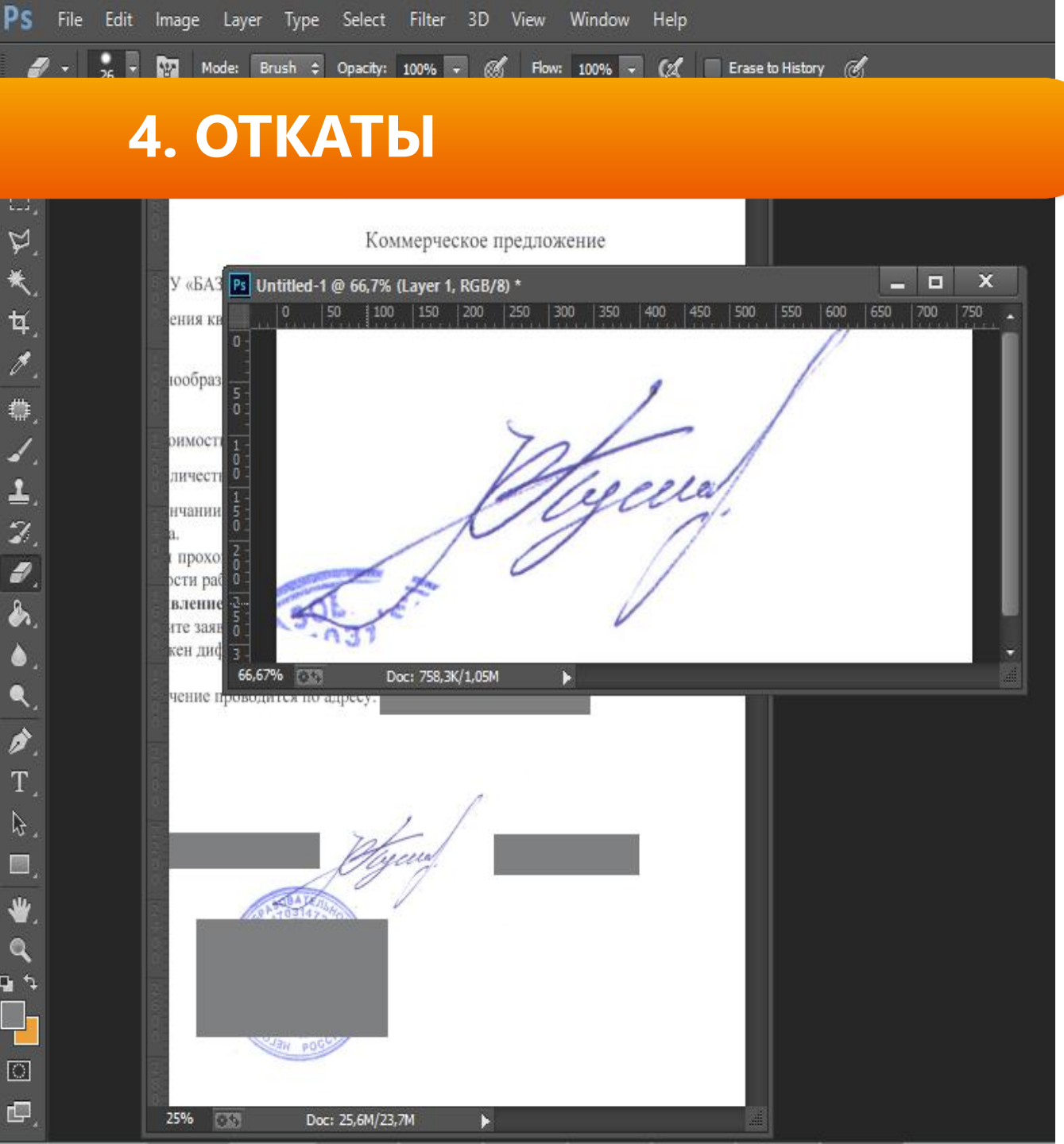
3. ФИРМЫ-БОКОВИКИ

БОКОВИК В ПРОЕКТНО-АРХИТЕКТУРНОЙ КОМПАНИИ

Что произошло: обнаружили, что один из сотрудников сохранил в личной почте на mail.ru черновик с уставом чужой компании.

Расследование: выяснилось, что эту почту специалист использовал вместе с двумя коллегами. Они открыли конкурентную фирму и уводили клиентов, предлагая им лучшие условия.

4. ОТКАТЫ



КЕЙС: ПОДДЕЛКА КОММЕРЧЕСКИХ ПРЕДЛОЖЕНИЙ

Один из клиентов обнаружил менеджера, который подделывал ценовые предложения других поставщиков, чтобы лоббировать «своих».

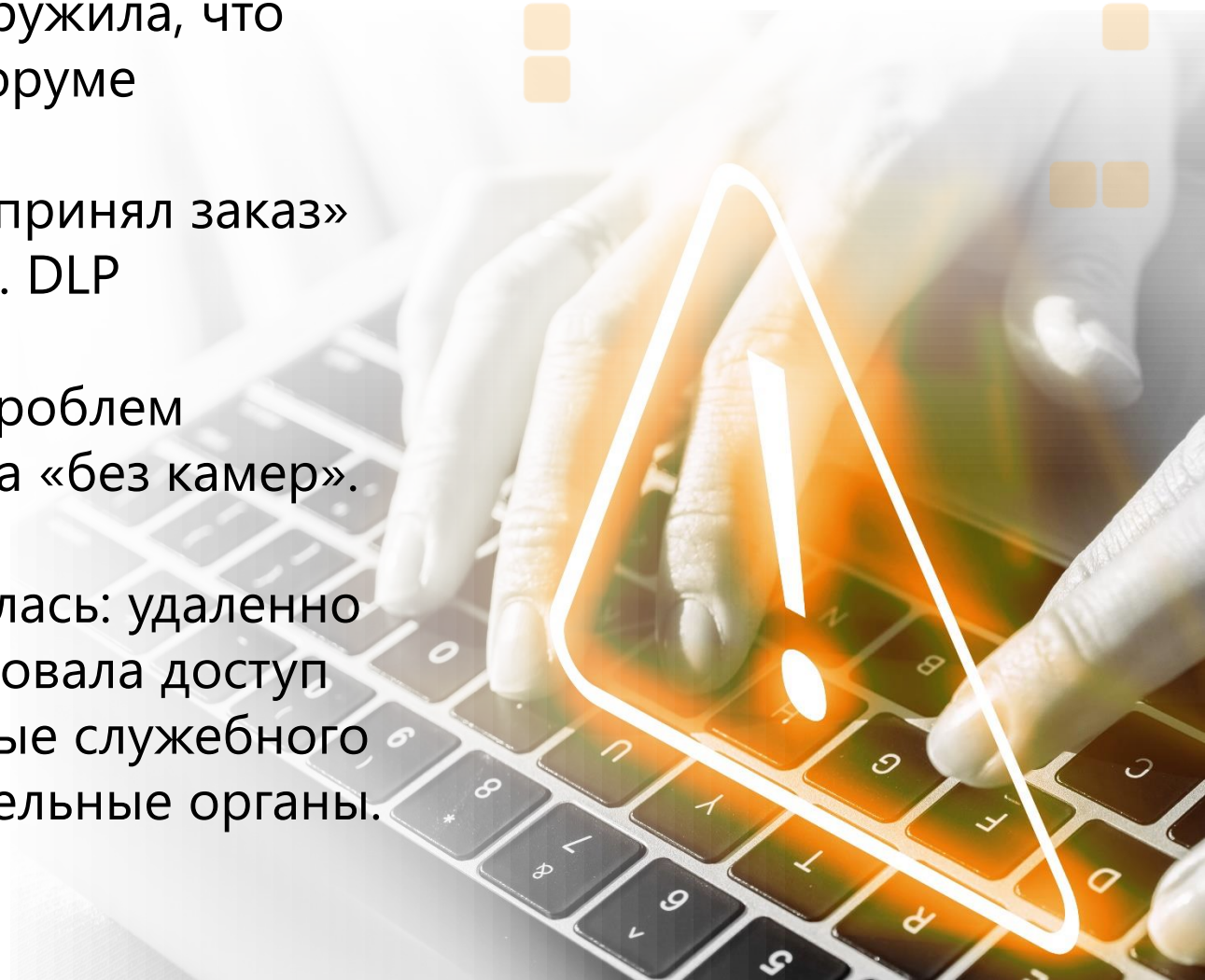
Сотрудник службы безопасности заметил, что работник часто запускает процесс Photoshop. Посмотрели скриншоты, видео с монитора – и обнаружили, что менеджер занимался подделкой.

5. УДАЛЕННАЯ РАБОТА

«ПРОБИВ ДАННЫХ»

В телеком-операторе часть персонала работала удаленно
На корпоративных ПК. DLP-система обнаружила, что сотрудник проводит рабочее время на форуме с подозрительной тематикой.
Расследование показало, что сотрудник «принял заказ» на «пробив» данных по номеру телефона. DLP перехватила содержание переписки с заказчиком: сотрудник объяснял, что «проблем не будет», потому что он работает из дома «без камер».

Служба безопасности оперативно вмешалась: удаленно подключилась к ПК сотрудника, заблокировала доступ к базе. Сотрудника решили уволить, данные служебного расследования передали в правоохранительные органы.



6. БЕЗДЕЛЬЕ НА РАБОТЕ

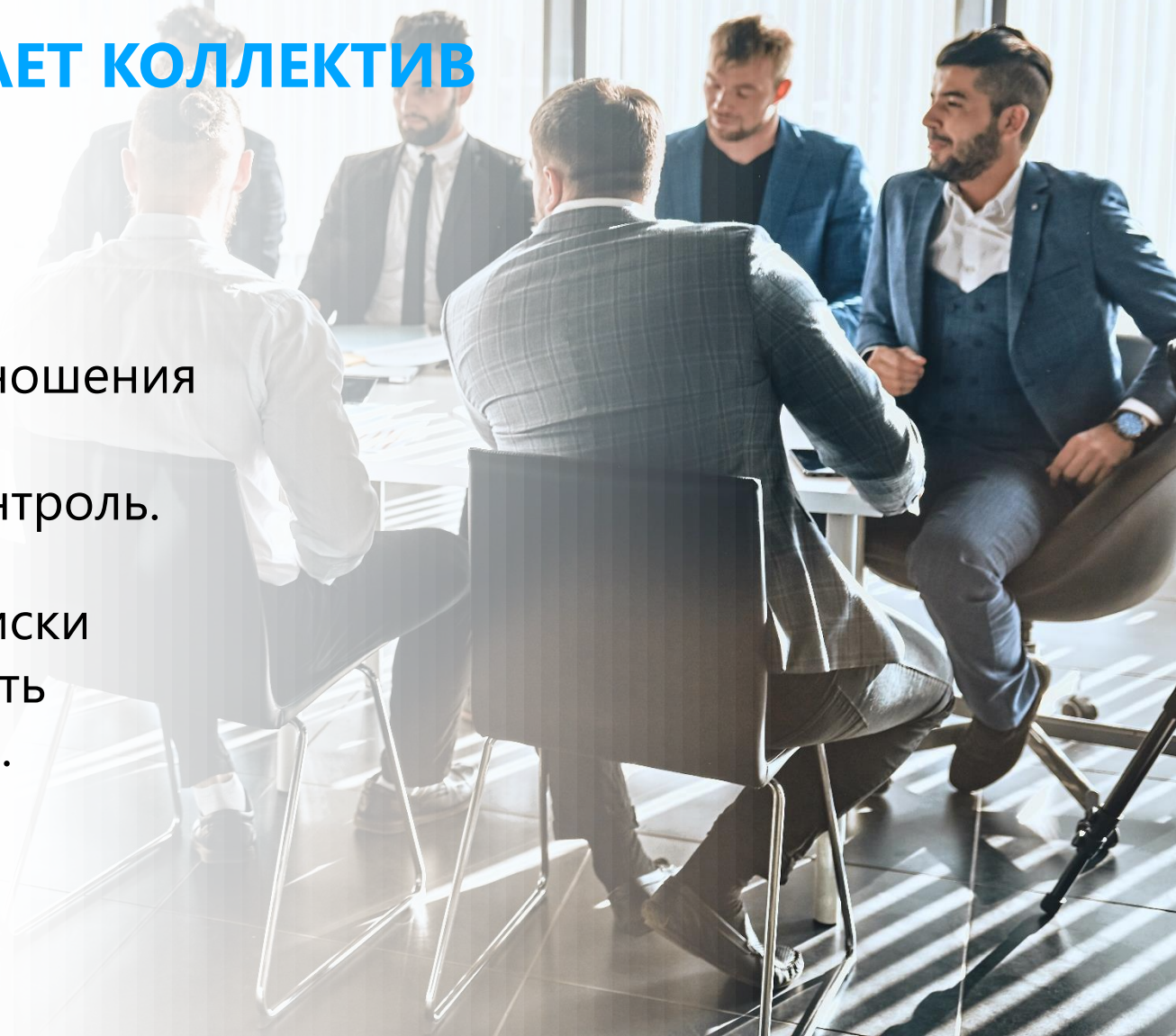
ЛИНЕЙНЫЙ РУКОВОДИТЕЛЬ – БЕЗДЕЛЬНИК

Что произошло: линейному руководителю поставили задачу по повышению продаж. Для достижения результата он просил подкрепление.

Расследование: анализ активности самого линейного руководителя показал, что он тратит 89% времени на развлекательные сайты. Сотрудника уволили, силами его подчиненного достигли перевыполнения плана продаж.

7. Негативные высказывания о компании и руководстве

СОТРУДНИК НАСТРАИВАЕТ КОЛЛЕКТИВ ПРОТИВ РУКОВОДСТВА



Что произошло: сотрудник компании недоволен системой премирования, отношения с начальством накалялись.
ИБ-служба взяла его под усиленный контроль.

Расследование: перехват Skype-переписки показал, что сотрудник начал настраивать против руководства других сотрудников.
Компания попрощалась с агитатором.

КАК ЗАЩИТИТЬСЯ?

4 СОСТАВЛЯЮЩИЕ ЗАЩИТЫ ОТ ВНУТРЕННИХ ИБ-УГРОЗ

1. Понять что и где хранится
2. Контроль движения информации по всем каналам
3. Контроль рабочего времени сотрудников
4. Повышение осведомленности сотрудников

http://ибграмотность.рф

5 КЕЙСОВ ИЗ ПРАКТИКИ ЗАКАЗЧИКОВ В РИТЕЙЛЕ

1 Передача баз данных

Санкт-петербургскому ретейлеру автомобильных шин и запчастей, руководитель отдела продаж нанесла ущерб в несколько сотен миллионов рублей. Базы данных клиентов и номенклатуру цен сотрудница передавала через своего мужа, который был в сговоре с конкурентами компании.

Руководство провело служебное расследование и обнаружило нарушителей. Результаты внутрикорпоративного расследования передали оперативным органам, а те возбудили уголовное дело. Ретейлеру удалось возместить через суд больше 70% признанных судом убытков — их в виде штрафа взыскали с виновницы инцидента.

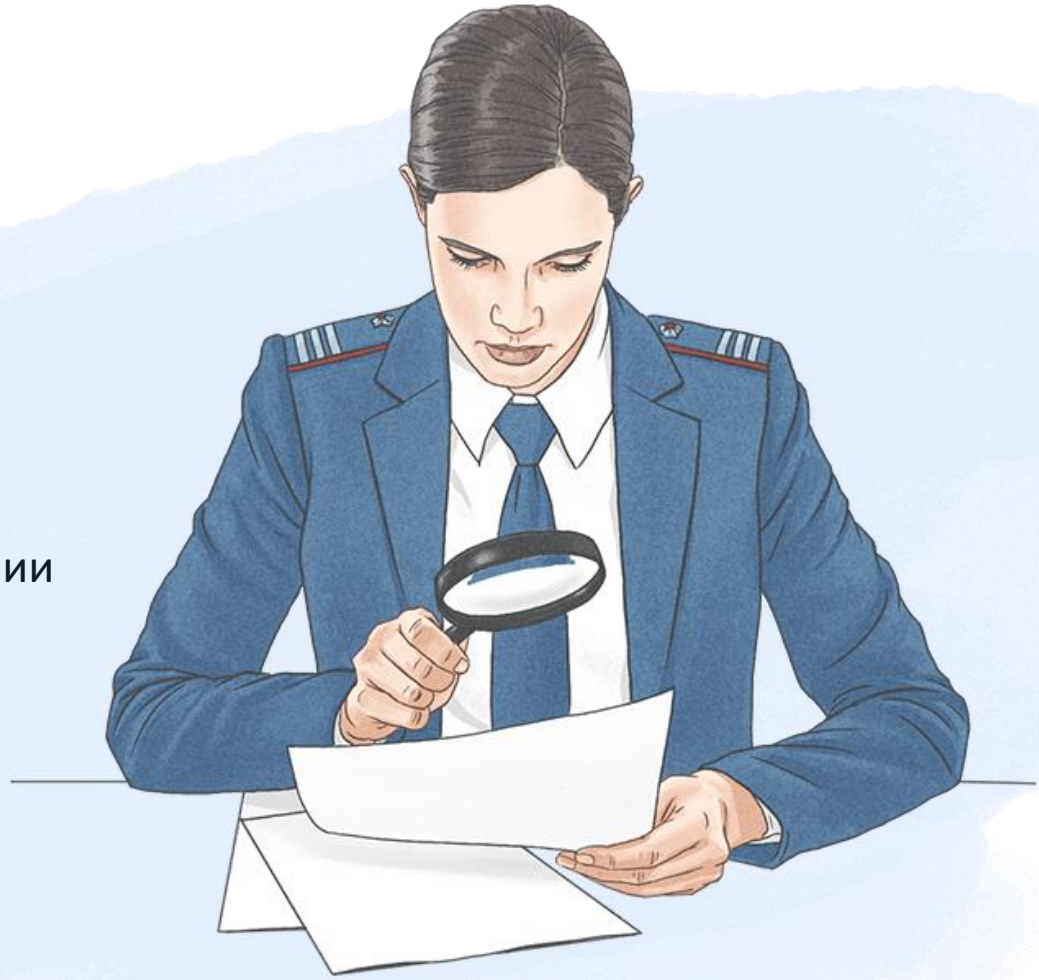
Источник: http://www.rbc.ru/business/28/11/2016/582dbbb99a7947a46c6ca65b

2 Увод сотрудников и клиентов

Служба безопасности оптового поставщика стройматериалов обнаружила в перехвате DLP-системы свои уставные документы. Выяснилось, что использовал их заместитель коммерческого директора: второй месяц он конфликтовал с руководством компании и, в конце концов, решил открыть свою.

Бдительность безопасников помешала увести другую ценную информацию, но без потерь все равно не обошлось. Бывший замдиректора успел «обработать» часть персонала и, уволившись, забрал подчиненных с собой.

Источник: http://e.gd.ru/article.aspx?aid=568740



3 ТРИ ПИШЕМ – ДВА В УМЕ

В компании, занимающейся закупками комплектующего оборудования для производства, «СёрчИнформ КИБ» позволил установить, что бухгалтер закупала товары не у официального поставщика, а через стороннюю организацию, которой руководил ее родственник.

Вывод: Итоговая цена получалась в среднем ниже на 10%, однако сотрудница не отображала этот факт в отчете и оставляла разницу себе.

4 КЕЙС: большой архив

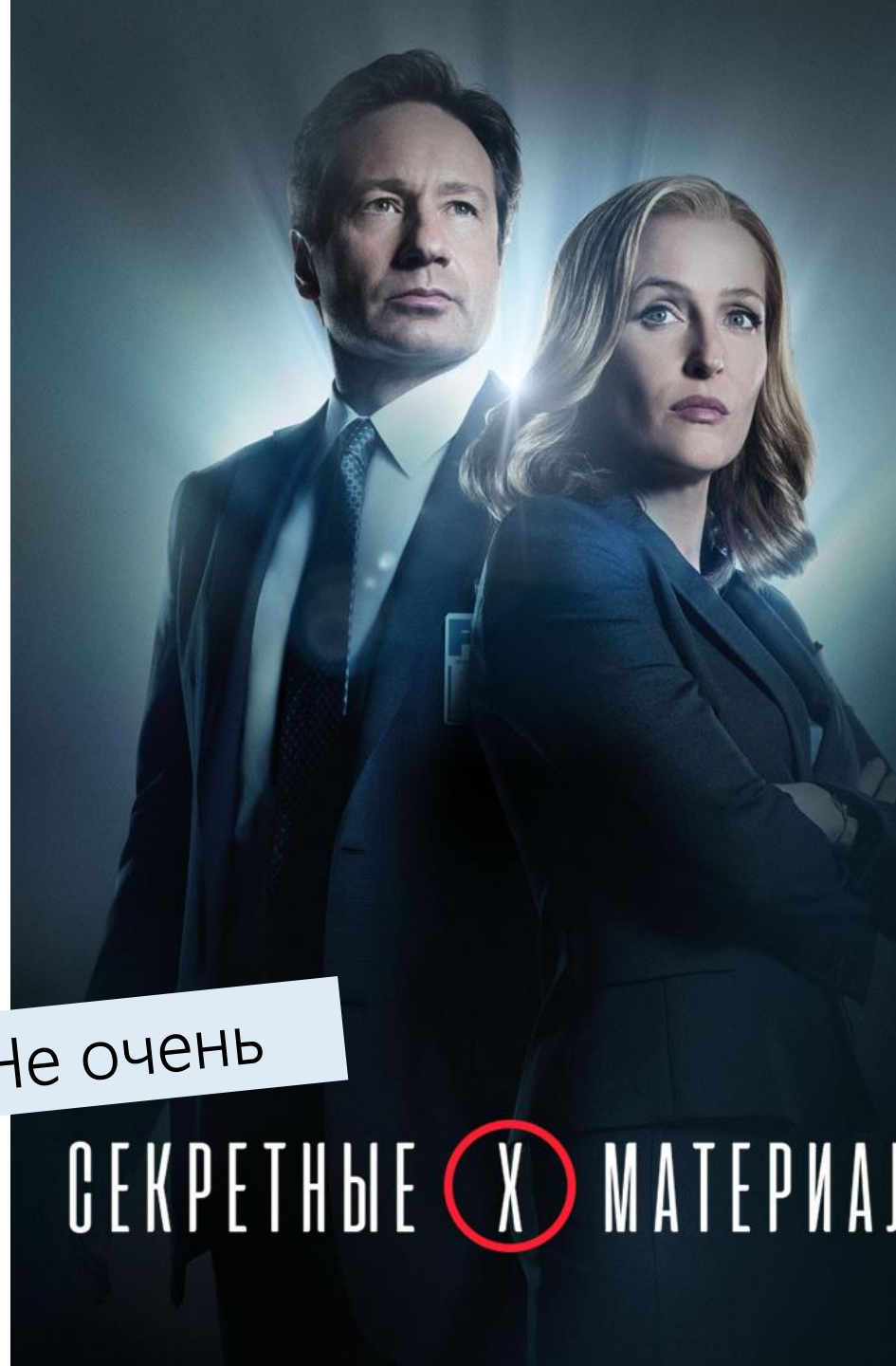
Сотрудница торгового предприятия перед увольнением загрузила на сторонний облачный ресурс большой архив весом в 900 Мб. Такой большой объем передаваемых данных привлек внимание службы безопасности. Дальнейший анализ установил, что передаваемый архив – проект всех исследований московского рынка. Благодаря своевременному выявлению инцидента архив был удален из открытого источника.

Вывод. Стоимость подобной информации с учетом разработки документации, недополученной прибыли и раскрытия внутренней себестоимости продукции информации о клиентах – около 100 млн. рублей.

5 ТРЕТЬ ДОКУМЕНТОВ В ОБЩЕМ ДОСТУПЕ

Что произошло: после аудита ИБ-служба торговой компании обнаружила, что на сервере нарушается политика разграничения доступа.

Расследование: дальнейший анализ показал, что в общем доступе хранится до трети конфиденциальных файлов компании. Данные классифицировали и навели порядок в файловой системе.



Благодарю за внимание

Павел Карасев
+7 (963) 644 9223