ZECURION

7(+1) историй о внутренних угрозах со счастливым концом

Роман Подкопаев
вице-президент

Ростов на Дону, 2017

ПОГОВОРИМ О ПОНЯТИЯХ

DLP (Data Leak Prevention) – предотвращение утечек информации

Иностранный термин. Обозначает технические решения для защиты конфиденциальной информации от утечек. Наибольшее развитие получили именно в России

Российские продукты доминируют на отечественном рынке DLP

Российские продукты высоко котируются на международном рынке

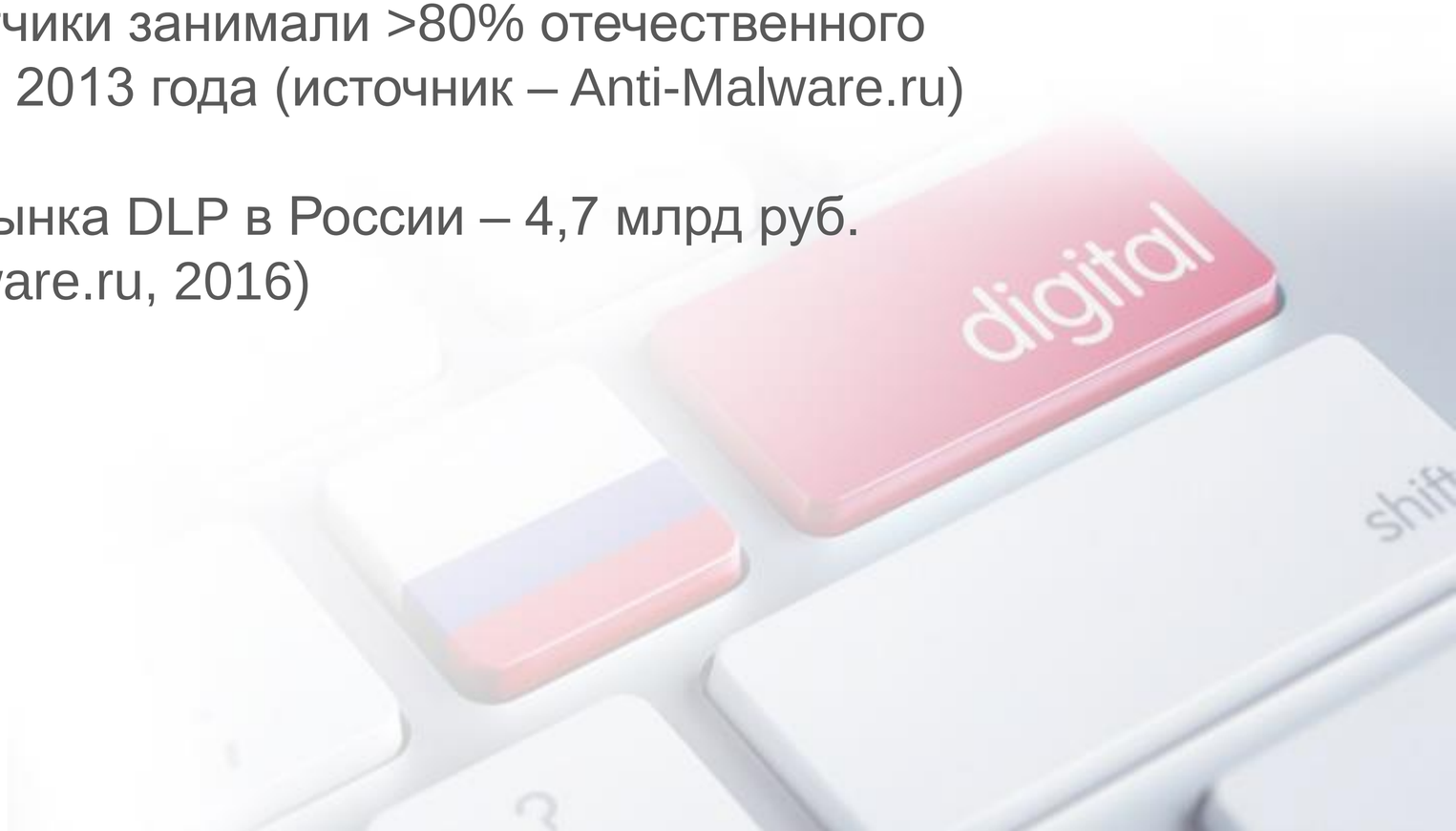
Основной регулятор и лицензиар в России – ФСТЭК

ИМПОРТОЗАМЕЩЕНИЕ В СЕГМЕНТЕ DLP

Российские разработчики занимают >90% отечественного рынка DLP (источник – Anti-Malware.ru, 2016)

Российские разработчики занимали >80% отечественного рынка DLP по итогам 2013 года (источник – Anti-Malware.ru)

Суммарный объём рынка DLP в России – 4,7 млрд руб. (источник – Anti-Malware.ru, 2016)



ПОЧЕМУ МЫ ОБ ЭТОМ РАССКАЗЫВАЕМ

Zecurion

- Входит в топ-30 российских ИБ-компаний
- Входит в комитет по ИБ при АРПП
- Защищаем от утечек Минобороны, Федеральное казначейство, Сбербанк и др.
- Входит в реестр отечественного ПО Минсвязи
- С 2001 года на рынке информационной безопасности
- Более 10 тысяч корпоративных клиентов

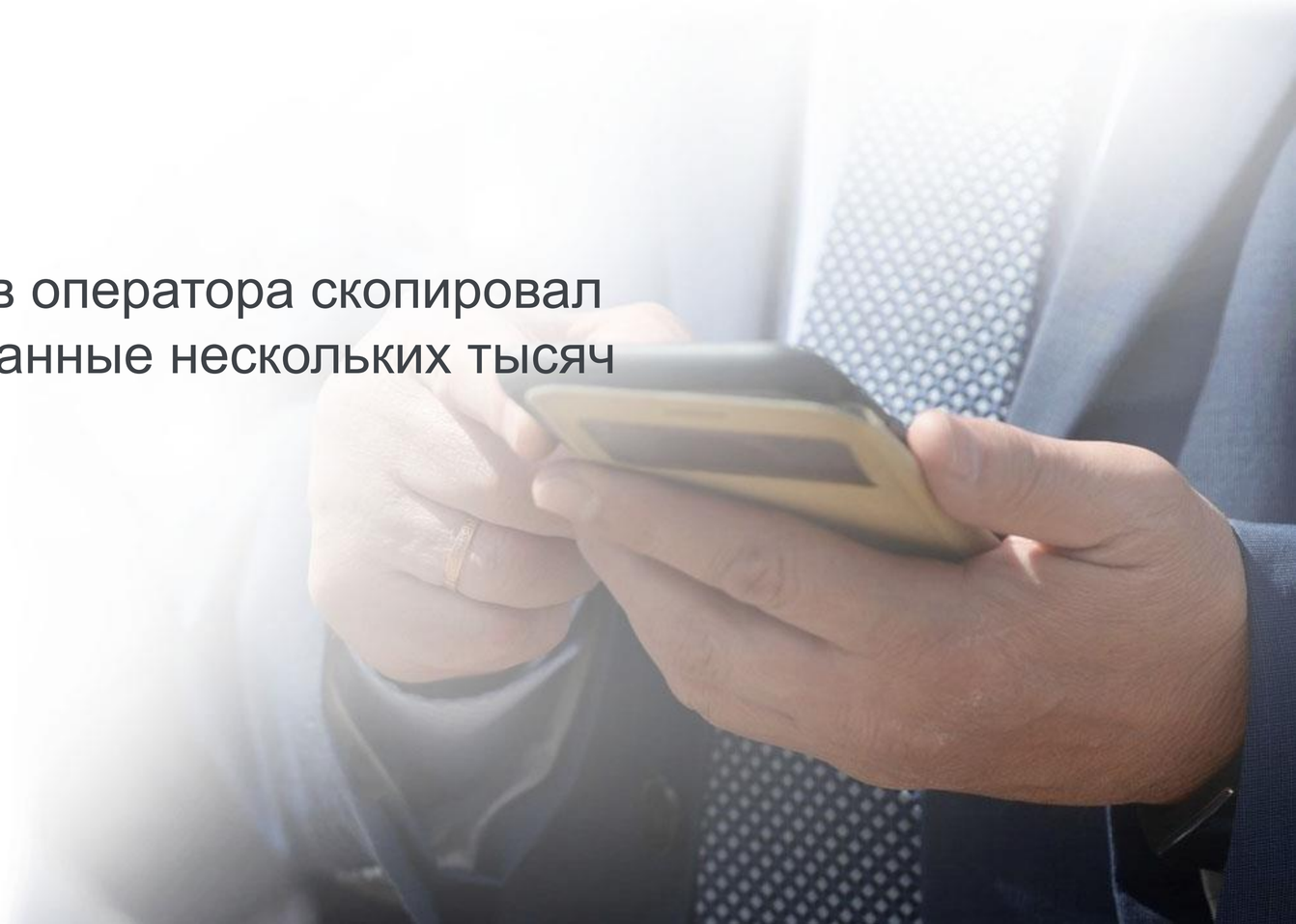
СЛУЧАЙ 1

Сфера деятельности

Оператор мобильной связи

Ситуация

Сотрудник одного из офисов оператора скопировал на флешку персональные данные нескольких тысяч абонентов.



СЛУЧАЙ 1

С помощью чего поймали

Zecurion Device Control, шаблоны данных

Какие политики сработали

Проверка по шаблонам. Система детектировала утечку данных по стандартным (поставляются вместе в системой) шаблонам паспортных данных

Вероятные потери

Нарушение №152-ФЗ «О персональных данных», репутационный вред, переманивание абонентов

СЛУЧАЙ 2

Сфера деятельности

Агропромышленный холдинг

Ситуация

Директор по развитию бизнеса скопировал на флешку рабочую базу. Модуль криптопериметр автоматически зашифровал файлы при копировании, и сотрудник не смог их открыть дома. Позже служба безопасности выяснила, что топ-менеджер готовился покинуть компанию.

СЛУЧАЙ 2

С помощью чего предотвратили

Zecurion Device Control, модуль криптопериметр

Какие политики сработали

Конфиденциальный характер информации был выявлен по цифровому отпечатку базы, снятому на этапе внедрения системы

Вероятные потери

15 млн руб., нарушение №98-ФЗ «О коммерческой тайне», нарушение №152-ФЗ «О персональных данных»

СЛУЧАЙ 3

Сфера деятельности

Торговля промышленным оборудованием

Ситуация

Менеджер по продажам пневматических приводов договорился о работе в конкурирующей компании. Не дожидаясь выхода на новое место, по электронной почте предложил своим клиентам (около 20 заказчиков) сменить поставщика, обещая лучшие условия.

СЛУЧАЙ 3

С помощью чего поймали

Zecurion Traffic Control, ключевые слова

Какие политики сработали

Поиск по словарю ключевых слов. Кастомизированный словарь «Мошенничество» был доработан под конкретного заказчика с учётом специфики бизнеса

Вероятные потери

24 млн руб.

СЛУЧАЙ 4

Сфера деятельности

НИИ

Ситуация

Ответственный за снабжение договорился с руководителями двух крупных отделов о создании фиктивных заявок на закупку мебели и канцелярских принадлежностей. Лишняя продукция реализовывалась через ИП, открытое родственником снабженца. Детали схемы вскрылись при анализе переписки по ICQ

СЛУЧАЙ 4

С помощью чего поймали

Zecurion Traffic Control, ключевые слова

Какие политики сработали

Поиск по словарю ключевых слов «Сговор». Словарь не входит в стандартную поставку системы

Вероятные потери

Около 400 тыс. руб. в год

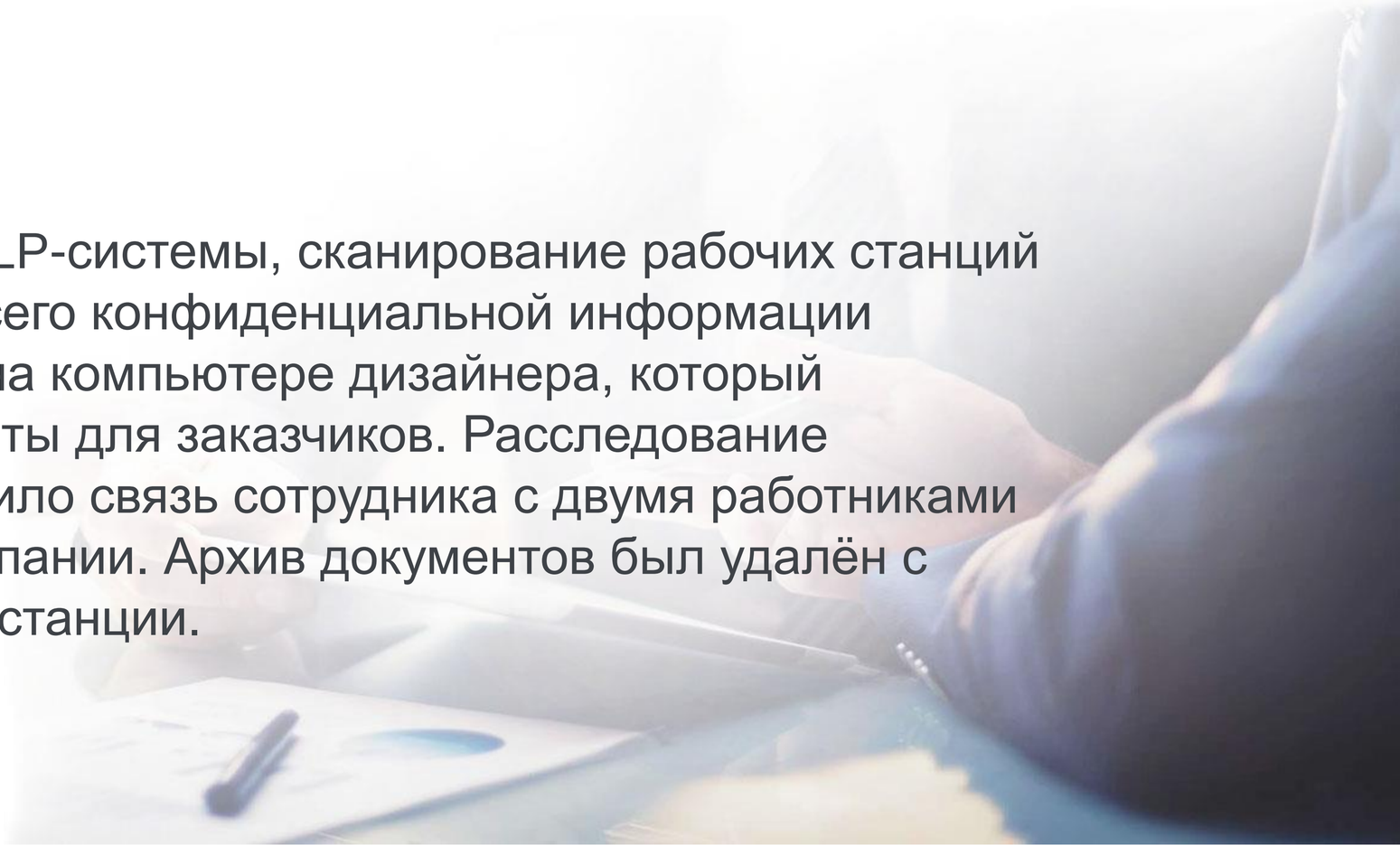
СЛУЧАЙ 5

Сфера деятельности

Аудит и консалтинг

Ситуация

После внедрения DLP-системы, сканирование рабочих станций выявило: больше всего конфиденциальной информации клиентов хранится на компьютере дизайнера, который оформляет документы для заказчиков. Расследование инцидента обнаружило связь сотрудника с двумя работниками конкурирующей компании. Архив документов был удалён с локальной рабочей станции.



СЛУЧАЙ 5

С помощью чего выявили

Zecurion Discovery, цифровые отпечатки

Какие политики сработали

Сканирование компьютера обнаружило большое количество совпадений по базе цифровых отпечатков, снятых с конфиденциальных документов

Вероятные потери

40 млн руб., нарушение NDA с партнёрами, нарушение №98-ФЗ «О коммерческой тайне»

СЛУЧАЙ 6

Сфера деятельности

Банк

Ситуация

Сотрудник обратился к руководству с просьбой об увеличении зарплаты в связи с постоянными переработками. При проведении расследования служба безопасности обратила внимание на аномально высокую интенсивность использования принтера. Как выяснилось, сотрудник в рабочее время писал свою книгу и использовал принтер для печати черновиков.

СЛУЧАЙ 6

С помощью чего поймали

Zecurion Device Control, контроль принтеров

Какие политики сработали

Сработала собственная политика заказчика «перерасход бумаги», в основе которой заложены формальные признаки файлов. Политика учитывает частоту и объём распечатываемых документов

Вероятные потери

Более 1,5 млн руб. в год на зарплате неадекватного сотрудника

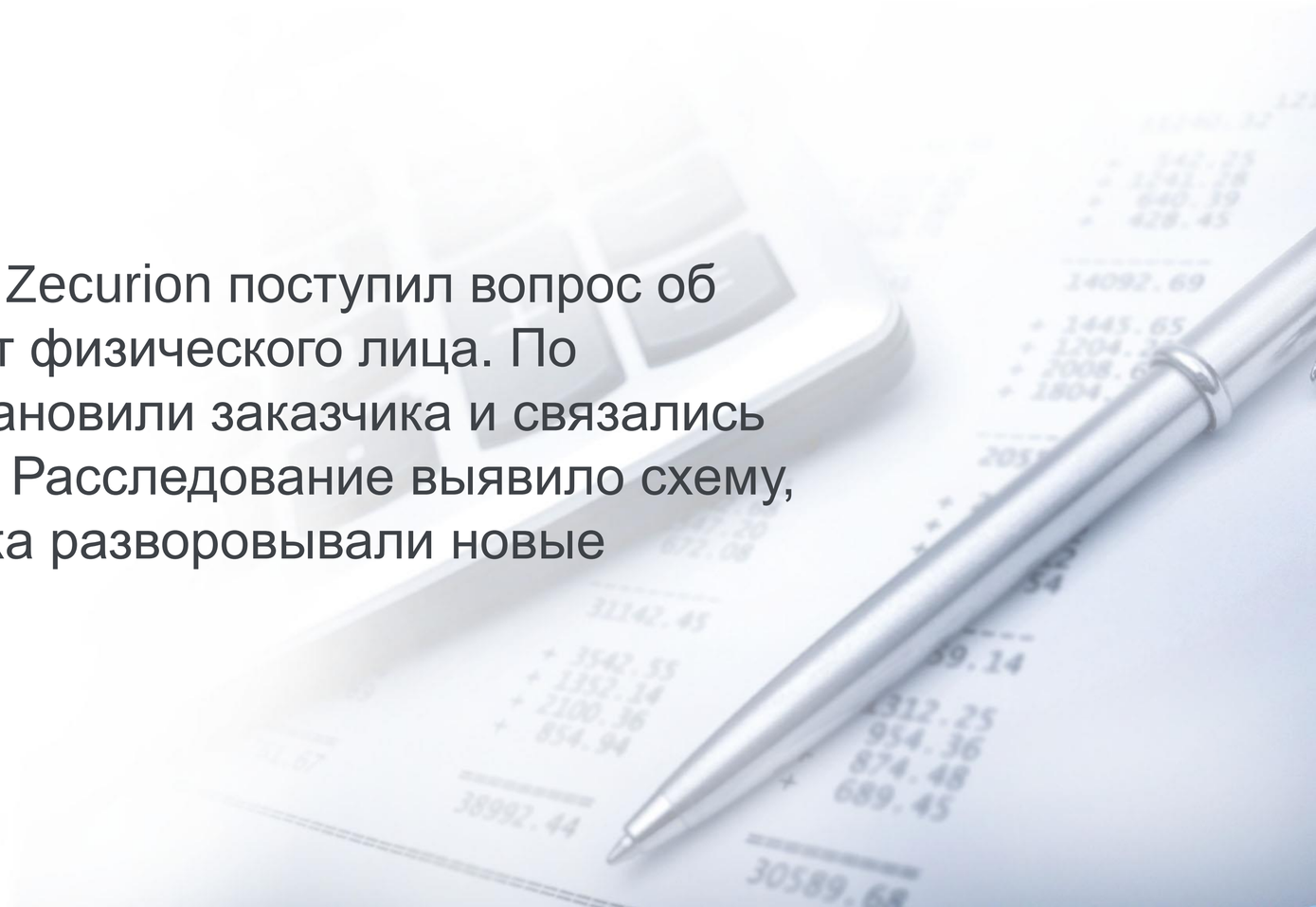
СЛУЧАЙ 7

Сфера деятельности

Финансовые услуги

Ситуация

В техническую поддержку Zecurion поступил вопрос об удалении Device Control от физического лица. По лицензионному ключу установили заказчика и связались со службой безопасности. Расследование выявило схему, в которой сотрудники банка разворовывали новые компьютеры.



СЛУЧАЙ 7

С помощью чего поймали

Zecurion Device Control, служба безопасности заказчика

Какие политики сработали

Регламент обращения в техническую поддержку Zecurion

Ориентировочные потери

Около 2 млн руб. ежегодно.

БОНУСНЫЙ СЛУЧАЙ

Сфера деятельности

Бизнес-разведка и аналитика

Ситуация

Конкуренты прислали сотрудников собственного ЧОПа, переодетых в форму правоохранительных органов, для изъятия серверов. Переодетые злоумышленники беспрепятственно прошли в серверную и забрали оборудование. Воспользоваться данными конкуренты не смогли, диски были зашифрованы, а ключи своевременно уничтожены дежурной сменой.

С помощью чего предотвратили

Zecurion Storage Security

Вероятные потери

Более 100 млн руб., закрытие бизнеса

БОРЬБА С ВНУТРЕННИМИ УГРОЗАМИ

Zecurion Traffic Control

Контроль трафика на шлюзе сети

Zecurion Staff Control

Контроль рабочего времени

Zecurion Device Control

Контроль перемещения информации на рабочих станциях

Zecurion PAM

Контроль привилегированных пользователей

Zecurion UTM

Прокси, URL-фильтрация, предотвращение проникновения вредоносного ПО

Zecurion Discovery

Поиск конфиденциальной информации на рабочих станциях и серверах

СПАСИБО ЗА ВНИМАНИЕ!

129164, Российская Федерация, Москва, Ракетный бульвар, 16

www.zecurion.ru

welcome@zecurion.com

+7 495 221-21-60