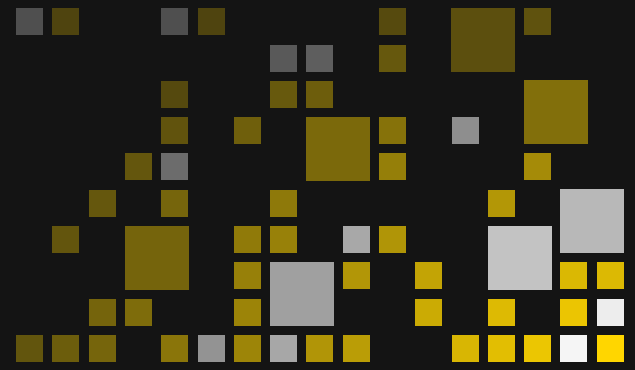
КОД ИБ КАЗАНЬ · 12 НОЯБРЯ 2026

Расследование разглашения коммерческой тайны по цифровым следам

Методика корреляционного таймлайн-анализа по нескольким независимым источникам

Авдошин Антон

IT-эксперт, к.т.н. · Лаборатория Цифровых Экспертиз



Обстоятельства дела

Бизнес компании

- Компания организовывала выдачу банковских гарантий; заявки клиентов поступали в корпоративную CRM
- Сотрудники размещали заявки в банковских системах и собирали пакет документов
- Банк выдавал гарантию → компания получала агентское вознаграждение

Схема нарушения

- Сотрудник получал заказы из корпоративной CRM, но проводил их через личный кабинет — в обход кабинета компании
- Комиссию получала не компания, а сотрудник
- Работодатель увидел падение финансовых показателей и зафиксировал действия на видео

Постановка задачи исследования

01

Обстоятельства

Сотрудник был уволен. В компании был отлажен кадровый документооборот, актуальные должностные инструкции — что позволило возбудить уголовное дело по статье «Разглашение коммерческой тайны»

02

Основное доказательство

Видеозапись действий пользователя на компьютере

03

Задача КТЭ от следователя

Верифицировать и авторизовать действия в интерфейсе операционной системы, зафиксированные на видео

Объекты исследования

01 Видеозапись

02 Моноблок, изъятый следствием

Схема действий пользователя

Корпоративная CRM – система

Распределение заявок по сотрудникам

Расчет метрик эффективности

Клиенты, которым требуются банковские гарантии

Рабочее место пользователя

Обычный режим браузера

- Личный кабинет компании банковской системы 1
- Личный кабинет компании банковской системы 2

Режим браузера «Инкогнито»

- Личный кабинет ИП банковской системы 1
- Личный кабинет ИП банковской системы 2

Основные технические проблемы

01

Юридическое ограничение

Моноблок — вещественное доказательство: изменять его состояние нельзя.

Разрешение на частично разрушающие методы исследования не получено.

02

Аппаратное препятствие

Устройство использовало технологию Intel Optane, поэтому ряд программ создания образа диска работали некорректно.

03

Программное препятствие

ОС использовала BitLocker — для работы с образом диска потребовалось извлечение 48-разрядных ключей

Логика доказывания

Личные кабинеты — только в режиме браузера «Инкогнито»; корпоративный межсетевой экран и прокси-сервер не использовались → действия пользователя зафиксированы только на видеозаписи

Экспертиза видео

Видеозапись исследована на признаки изменения.

Если признаки отсутствуют →

запись оригинальна и неизменна целиком

Кросс-проверка сеансов

Сеансы в CRM и банковских приложениях соответствуют истории браузера на изъятом компьютере →

сеансы «Инкогнито» также проведены на исследуемом компьютере

Таймлайн-шкала



- Фрагменты видеозаписи, не имеющие подтверждения
- Фрагменты видеозаписи, подтвержденные логами банковской системы 1 и историей браузера
- Фрагменты видеозаписи, подтвержденные логами CRM системы
- Фрагменты видеозаписи, подтвержденные логами банковской системы 2 и историей браузера

Информационно-независимые источники

Использованные

Видеозапись
тайминг, дата, время, приложение, логин, выполняемая операция

Сеансы работы в браузере
дата, время, пользователь ОС, адреса посещённых страниц

Сеансы работы в CRM
дата, время, пользователь, выполненные операции

Сеансы в банковских приложениях
дата, время, логин, выполненные операции

Не удалось использовать

Видеозаписи

Данные СКУД

Данные бухгалтерии
выплаты за проводимые сделки

Проведение экспертизы

- Видеозапись анализировалась вручную: тайминг, реальное время, дата, приложения, проведённые действия
- Выгрузки из банковских систем и CRM приведены к единому формату
- Сеансов в информационных системах существенно больше, чем на видеозаписи
- **Гипотеза:** под одной учётной записью работало несколько сотрудников на разных рабочих местах
- **Проверка:** запрошены расширенные выписки с IP-адресами — после сопоставления адресов события на видеозаписях и в логах информационных систем совпали

Имя страницы	Ссылка	Дата	Время	Пользователь	Тайминг
Феникс - Главная страница	https://lk.fenix-bg.ru/	24.07.2024	11:17:42	mlykova//urls	0:01
Феникс - Банковские гарантии	https://lk.fenix-bg.ru/Guarantees/Registry	24.07.2024	11:17:44	mlykova//urls	
Феникс - Банковские гарантии	https://lk.fenix-bg.ru/Guarantees/Registry?Demandl	24.07.2024	11:17:48	mlykova//urls	
Феникс - Заявка №1565986	https://lk.fenix-bg.ru/Guarantees/BankGuaranteeUp	24.07.2024	11:20:19	mlykova//urls	
ВБЦ	https://vbankcenter.ru/resources/secured/app/entry	24.07.2024	11:33:16	mlykova//urls	0:17
ВБЦ	https://vbankcenter.ru/resources/secured/app/	24.07.2024	11:33:16	mlykova//urls	
ВБЦ	https://vbankcenter.ru/resources/secured/app/agent	24.07.2024	11:33:16	mlykova//urls	
ВБЦ	https://vbankcenter.ru/resources/secured/app/entry	24.07.2024	11:33:17	mlykova//urls	
ВБЦ	https://vbankcenter.ru/resources/secured/app/agent	24.07.2024	11:33:33	mlykova//urls	
ВБЦ	https://vbankcenter.ru/resources/secured/app/agent	24.07.2024	11:33:33	mlykova//urls	
Феникс - Банковские гарантии	https://lk.fenix-bg.ru/Guarantees/Registry	24.07.2024	11:36:45	mlykova//urls	
Феникс - Банковские гарантии	https://lk.fenix-bg.ru/Guarantees/Registry?Demandl	24.07.2024	11:48:04	mlykova//urls	
ВБЦ	https://vbankcenter.ru/resources/secured/app/agent	24.07.2024	12:09:38	mlykova//urls	
Единое окно	https://partners.dasreda.ru/ibro/requests	24.07.2024	12:12:08	mlykova//urls	
Единое окно	https://partners.dasreda.ru/auth	24.07.2024	12:12:12	mlykova//urls	0:55
Единое окно	https://partners.dasreda.ru/	24.07.2024	12:12:16	mlykova//urls	
Единое окно	https://partners.dasreda.ru/ibro_neo/requests	24.07.2024	12:12:18	mlykova//urls	
Единое окно	https://partners.dasreda.ru/ibro_neo/requests/2097	24.07.2024	12:15:08	mlykova//urls	0:59

Имя страницы	Ссылка	Дата	Время	Тайминг	Компания	№ сделки
Файл 22.07.2024.webm размер 416,4 Мб HASH MD5 a2f7cf7d0c21162a2e2b67cb8d4581a6						
Единое окно	https://partners.dasreda.ru/auth	22.07.2024	10:42:58	0:07	Деловая среда	Вход
Единое окно	https://partners.dasreda.ru/ibro_neo/requests/209884	22.07.2024	10:43:07	0:08	Деловая среда	209884
Единое окно	https://partners.dasreda.ru/ibro_neo/requests/209838	22.07.2024	10:44:43	0:09	Деловая среда	209838
Единое окно	https://partners.dasreda.ru/ibro_neo/requests/209777	22.07.2024	10:45:38	0:10	Деловая среда	209777
Единое окно	https://partners.dasreda.ru/ibro_neo/requests/209792	22.07.2024	10:50:35	0:15	Деловая среда	209792
Единое окно	https://partners.dasreda.ru/ibro_neo/requests/209838	22.07.2024	10:53:13	0:18	Деловая среда	209838
Единое окно	https://partners.dasreda.ru/ibro_neo/requests/209777	22.07.2024	10:54:43	0:19	Деловая среда	209777
Единое окно	https://partners.dasreda.ru/ibro_neo/requests/209838	22.07.2024	10:58:08	0:23	Деловая среда	209838
Феникс - Вход в ЛК	https://lk.fenix-bg.ru/Account/Login?ReturnUrl=/Guarantees/Regist	22.07.2024	10:59:58	0:24	Феникс	Вход
Единое окно	https://partners.dasreda.ru/ibro_neo/requests/209777	22.07.2024	13:09:26	1:19	Деловая среда	209777
Феникс - Главная страница	https://lk.fenix-bg.ru/	22.07.2024	13:38:58	1:49	Феникс	Вход
Феникс - Заявка №1563650	https://lk.fenix-bg.ru/Guarantees/BankGuaranteeUpdate/1563650	22.07.2024	13:39:36	1:50	Феникс	1563650
ВБЦ	https://vbankcenter.ru/resources/secured/app/entry/login/agent?t	22.07.2024	14:57:02	2:29	ВБЦ	Вход

Результаты

Срок экспертизы: ≈ 1 месяц

≈ 1 неделя

Технические проблемы

разбирать или нет, подбор ПО под Intel Optane, извлечение ключей BitLocker

≈ 2 недели

Анализ данных

формирование таймлайна по независимым источникам

≈ 1 неделя

Оформление заключения

4 независимых источника — верификация и авторизация действий сотрудника

Заключение эксперта принято следователем и легло в основу обвинения

Выводы по итогам

Что сработало

- **Документы и ознакомление** — Сотрудник ознакомлен с должностными инструкциями и ответственностью за разглашение; рабочее место и логин переданы под роспись
- **Метрики в CRM** — CRM отслеживает метрики производительности сотрудников; руководство регулярно принимает по ним решения
- **Запись действий** — Развёрнута система записи действий пользователя — видно, чем сотрудник занимается на рабочем месте

Технологические и организационные пробелы

- **Управление ИБ инцидентами отсутствует** — нет модели угроз, матрицы рисков, соответствующего ПО, документации и протоколов реагирования
- **Домена нет** — учётные записи локальные
- **Интернет не контролируется** — ни прокси-сервера, ни межсетевого экрана, ни правил, ни логирования
- **DLP не развёрнута** — каналы связи не контролируются, утечки не предотвращаются

Спасибо за внимание!

Авдошин Антон

IT-эксперт, к.т.н.

+7 917 103 43 34

Лаборатория Цифровых Экспертиз

fastcom-samara@yandex.ru

