

MOSCOW FORENSICS DAY '25

АЛЕКСЕЙ ДРОЗД

«ИСПОЛЬЗОВАНИЕ СТЕГАНОГРАФИИ В
РАЗЛИЧНЫХ КАНАЛАХ ДЛЯ УСТАНОВЛЕНИЯ
ИСТОЧНИКА УТЕЧКИ ДАННЫХ»

ООО «СЁРЧИНФОРМ»



MFD

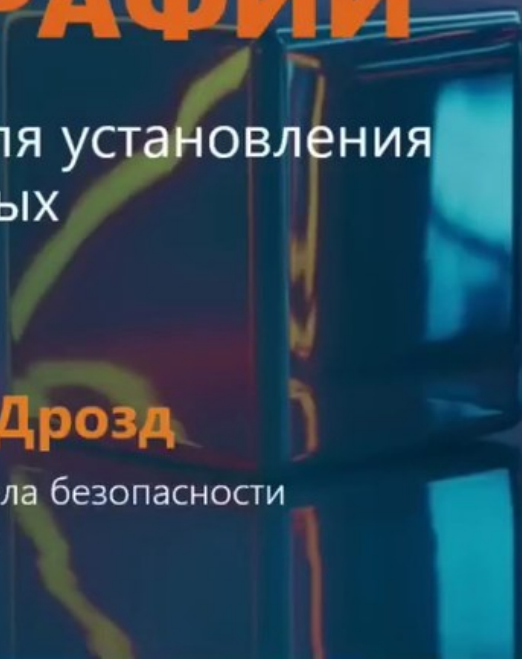
ИСПОЛЬЗОВАНИЕ СТЕГАНОГРАФИИ

в различных каналах для установления
источника утечки данных



Алексей Дрозд

Начальник отдела безопасности
«СёрчИнформ»



ЗАЧЕМ?

Иногда безопаснику хочется дополнительно быть уверенным в том, от кого был слив.

Что может сделать?



Подход от **ИС**



Подход от **Файла**



Подход от **Пользовательской сессии**



ПОДХОД ОТ ИНФОРМАЦИОННОЙ СИСТЕМЫ

SEARCHINFORM

Поиск - Консоль аналитика (1.87.0.11)

Поиск Текущая активность Отчеты Карта расположения сотрудников Карточки пользователей Файловый аудитор Профиль центр Карантин Task Management

Най Поиск 4 X +

Группы: <не выбрано>

Mail Соединить по: ИЛИ

☐ Исключить вложения

☒ Протоколы

☐ Исключая SMTP,IMAP,HTTP,HTTPS

☐ Тип E-mail

☐ Участники переписки

☐ От

☐ Все получатели

☐ Кому

☐ Копия

☐ Скрытая копия

☐ Тема письма

☐ Обратный путь

☐ Дата создания

☐ Имея вложения

☐ Число вложений

☐ Черновики

☐ Цифровая подпись

☒ Шифрованное сообщение

☒ Включая ☐ Исключая

☒ Авто пересылка

☐ Поиск в найденном

Очистить Найти

Показано документов: 1000 (1037)

Фильтр по типам: Все результаты Табличный вид Экспорт списка Поиск похожих Переходы к модулям Свойства пользователя...

Результаты поиска сообщений, реле для группировки

№	Тема	От кого	Кому	Пользователь	Размер	Копия	Скрытая копия
1	unknown	report.yandex.ru		Мария Соколова (sokolova@khd...)	10.8 KB		
2	Годовой отчет	Мария Соколова (m.sokolova.accountant@yandex.ru)	Мария Соколова (sokolova@khd...)	Мария Соколова (sokolova@khd...)	308 bytes		
3	Годовой отчет	Мария Соколова (m.sokolova.accountant@yandex.ru)	Мария Соколова (sokolova@khd...)	Мария Соколова (sokolova@khd...)	74.5 KB		
4	Re: Годовой отчет	Мария Соколова (m.sokolova.accountant@yandex.ru)	Мария Соколова (sokolova@khd...)	Мария Соколова (sokolova@khd...)	3.35 KB		
5	Годовой отчет	Мария Соколова (m.sokolova.accountant@yandex.ru)	Мария Соколова (sokolova@khd...)	Мария Соколова (sokolova@khd...)	77.2 KB		m.sokolova.accountant@yandex.ru
6	Re: Годовой отчет	Мария Соколова (m.sokolova.accountant@yandex.ru)	Мария Соколова (sokolova@khd...)	Мария Соколова (sokolova@khd...)	80.8 KB		
7	RE: Годовой отчет	Мария Соколова (m.sokolova.accountant@yandex.ru)	Мария Соколова (sokolova@khd...)	Мария Соколова (sokolova@khd...)	75.7 KB		m.sokolova.accountant@yandex.ru
8	Код подтверждения kspu@yandex.ru		Мария Соколова (sokolova@khd...)	Александр Петров (petrov@khd...)	27.4 KB		
9	Отчет новая реда...	Мария Соколова (m.sokolova.accountant@yandex.ru)	Мария Соколова (sokolova@khd...)	Мария Соколова (sokolova@khd...)	106 KB		
10	Ваше сообщение не было доставлено по адресу: m.sokolova.accountant@yandex.ru	Мария Соколова (m.sokolova.accountant@yandex.ru)	Мария Соколова (sokolova@khd...)	Мария Соколова (sokolova@khd...)	192 KB		

Страница: 1 / 2

От кого: m.sokolova.accountant@yandex.ru Мария Соколова

Кому: m.sokolova.accountant@yandex.ru

Скрытая копия: m.sokolova.accountant@yandex.ru

Тема письма: RE: Годовой отчет

Сообщение: годовой отчет 2016 (1.docx)

0 из 0

Отправлено: 21 апреля 2022 г. в 17:40

Кому: Мария Соколова

Тема: Re: Годовой отчет

Маш, я не понимаю, файл не открывается. Перешли ещё раз, пожалуйста.

вт, 21 апр. 2022 г., 17:37 Мария Соколова <m.sokolova.accountant@yandex.ru>

Родной формат Только текст Атрибуты

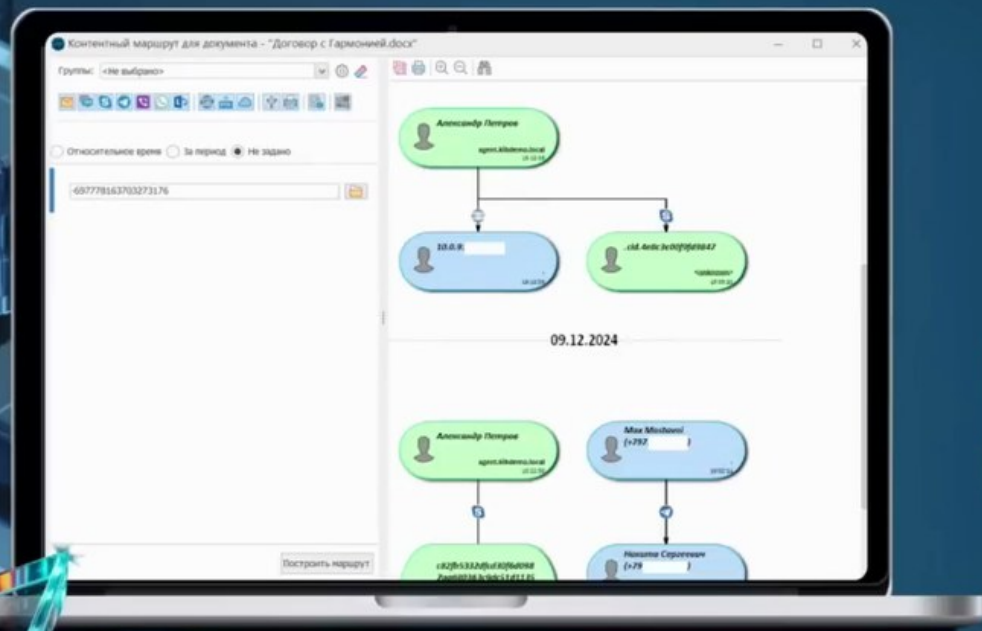
Выделенные строки: 1

Время отбора: 4 сек.



ПОДХОД ОТ ИНФОРМАЦИОННОЙ СИСТЕМЫ

SEARCHINFORM



ПОДХОД ОТ ИНФОРМАЦИОННОЙ СИСТЕМЫ

SEARCHINFORM

служебная записка.docx71,99 KB09.07.2025 17:1709.07.2025 17:1725.07.2ДСП документПоиск ДСП

пример накладной.docx12,08 KB10.07.2025 11:0810.07.2025 11:1302.08.2

Операции - Дата обновления файла: 13.05.2025 15:12:20

За дату с01.01.2024по30.06.2025 23:59:59Не выбраноНайтиОчистить

Перетаскийте сюда заголовок поля для группировки

Начало операции	Операция	Компьютер	Пользователь	Размер	Имя файла	Старое имя	Конец операции	Процесс	Образ
09.06.2025 17:57:19	Чтение agent.kibdemo.l	администратор@kibden	42,76 KB	C:\Users\Администр		09.06.2025 17:57:19	browser.exe	C:\Users\Администр	
22.05.2025 17:13:37	Смена расширения agent.kibdemo.l	администратор@kibden	42,76 KB	C:\Users\Администр	C:\Users\Администр	22.05.2025 17:13:37	explorer.exe	C:\Windows\explorer	
22.05.2025 17:07:43	Чтение agent.kibdemo.l	администратор@kibden	42,76 KB	C:\Users\Администр		22.05.2025 17:07:43	explorer.exe	C:\Windows\explorer	
13.05.2025 19:38:44	Чтение agent.kibdemo.l	администратор@kibden	42,76 KB	C:\Users\Администр		13.05.2025 19:38:44	explorer.exe	C:\Windows\explorer	
13.05.2025 17:41:53	Чтение agent.kibdemo.l	администратор@kibden	42,76 KB	C:\Users\Администр		13.05.2025 17:41:53	explorer.exe	C:\Windows\explorer	
13.05.2025 17:16:11	Чтение agent.kibdemo.l	администратор@kibden	42,76 KB	C:\Users\Администр		13.05.2025 17:16:11	explorer.exe	C:\Windows\explorer	
13.05.2025 17:05:53	Чтение agent.kibdemo.l	администратор@kibden	42,76 KB	C:\Users\Администр		13.05.2025 17:05:53	explorer.exe	C:\Windows\explorer	
13.05.2025 15:19:30	Чтение agent.kibdemo.l	администратор@kibden	42,76 KB	C:\Users\Администр		13.05.2025 15:19:30	explorer.exe	C:\Windows\explorer	
13.05.2025 15:11:56	Чтение agent.kibdemo.l	администратор@kibden	0 В	C:\Users\Администр		13.05.2025 15:11:56	WINWORD.EXE	C:\Program Files	
13.05.2025 15:11:50	Чтение agent.kibdemo.l	администратор@kibden	0 В	C:\Users\Администр		13.05.2025 15:11:50	explorer.exe	C:\Windows\explorer	
13.05.2025 15:11:48	Смена расширения agent.kibdemo.l	администратор@kibden	0 В	C:\Users\Администр	C:\Users\Администр	13.05.2025 15:11:48	explorer.exe	C:\Windows\explorer	

1 из 11

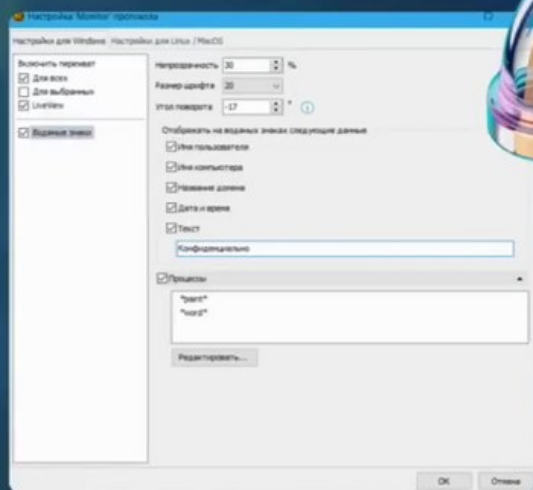
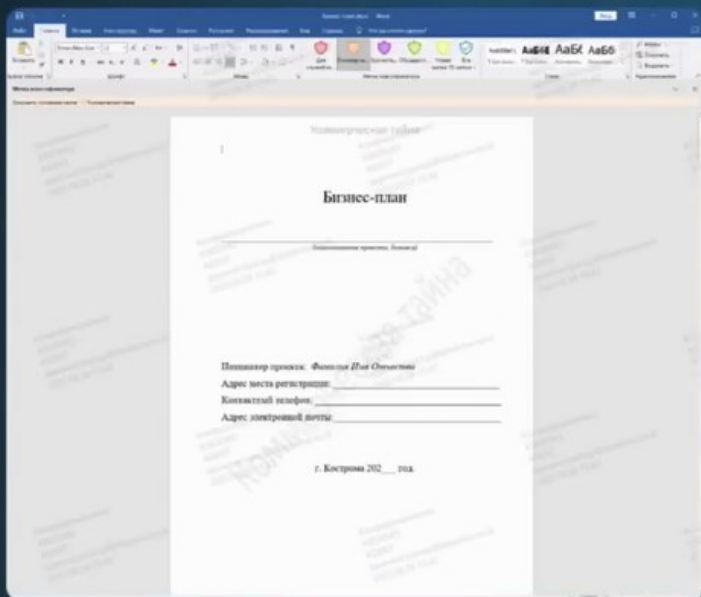
Просмотр файловОперацииТолько текстАтрибутыПравилаРезультат поискаДубликаты



ПОДХОД ОТ ПОЛЬЗОВАТЕЛЬСКОЙ СЕССИИ

Зачем?

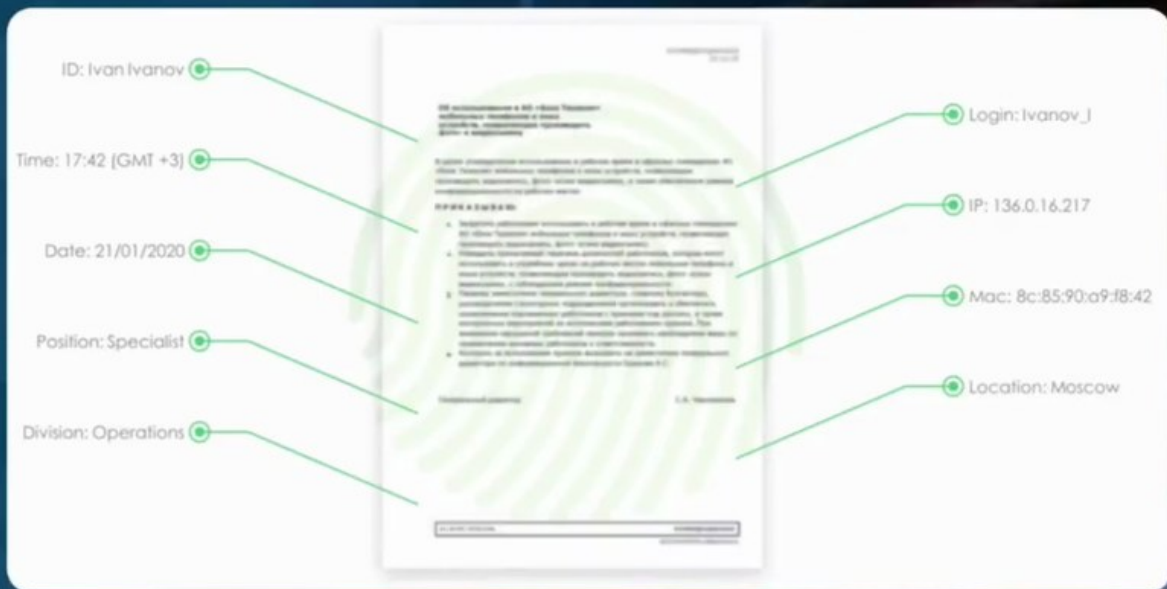
Выявление источника утечки данных, если кто-то снимал экран на камеру или сделал скриншот.



ПОДХОД ОТ **ФАЙЛА**

Зачем?

Выявление источника утечки данных, если кто-то снимал экран на камеру или сделал скриншот.



ОГРАНИЧЕНИЯ

SEARCHINFORM

Технические
по форматам

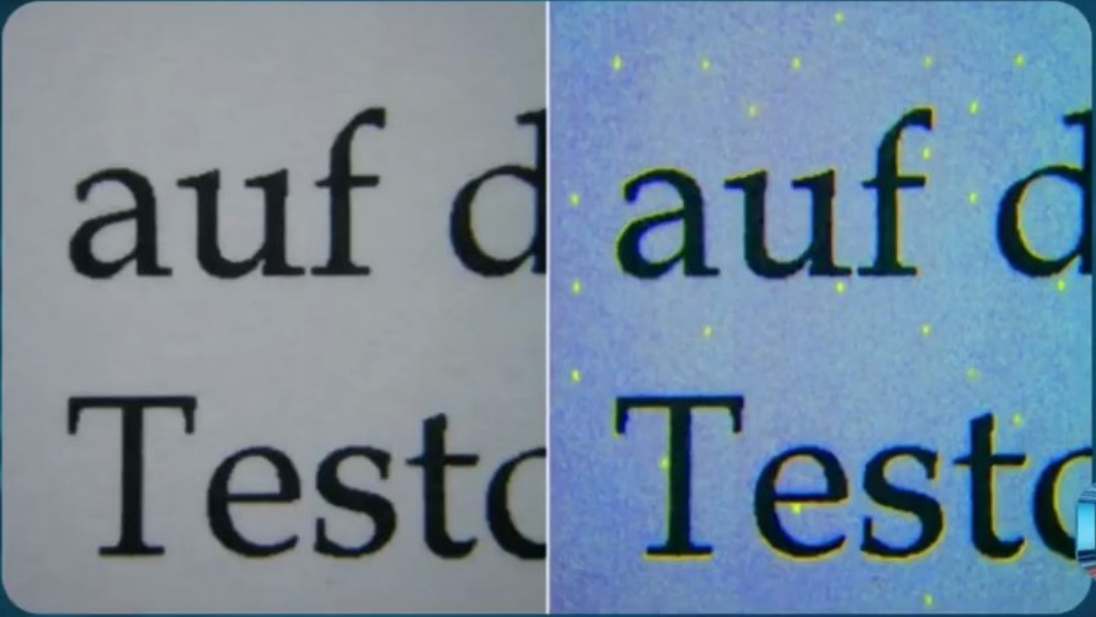
Технические
по обнаружению
меток

Технические
по архитектуре

Технические
по исключительным
ситуациям

ВЫВОД

SEARCHINFORM



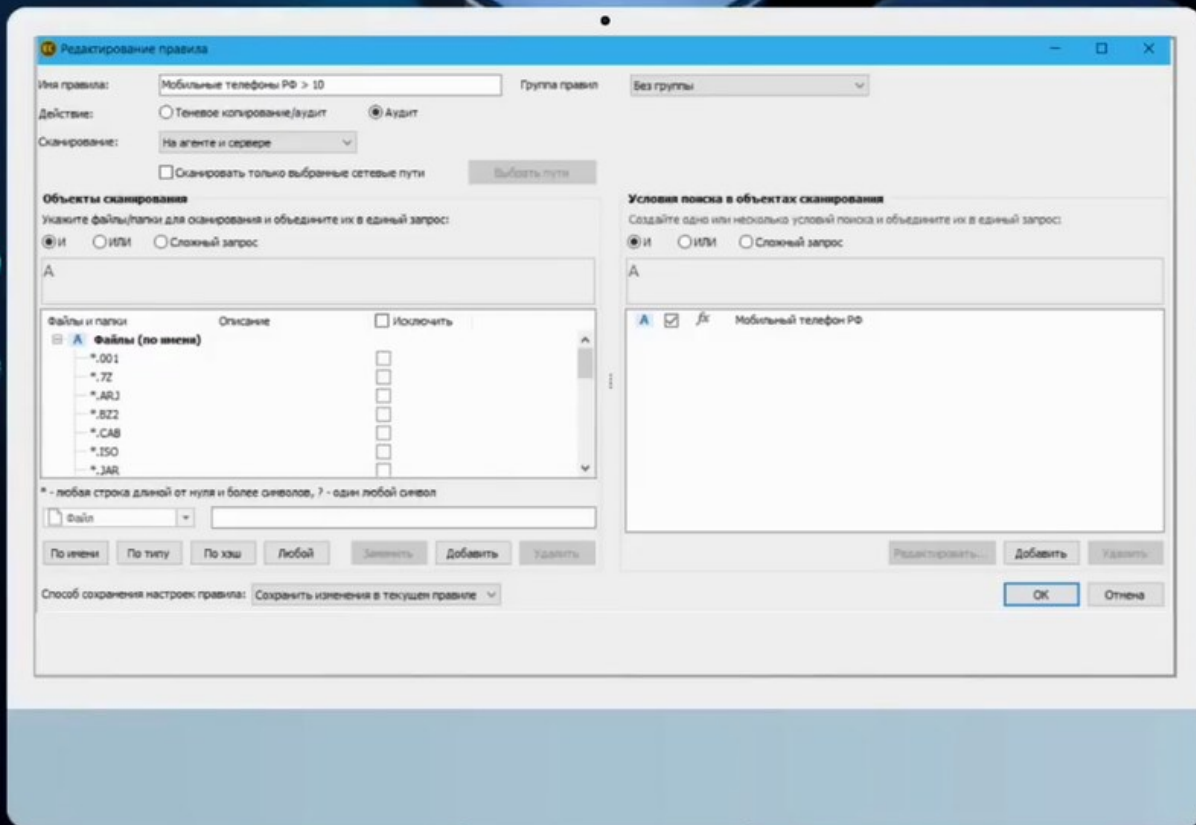
auf d auf d
Testo Testo

Стоит использовать
разные методы
стеганографии
в зависимости
от канала передачи
данных **и от типа**
передаваемых данных.



ВЫВОД

Но можно
придумать
и **что-то**
универсальное



ПЕРСПЕКТИВЫ

SEARCHINFORM

Редактирование правила. Документы MS Office/AutoCAD - Установка метки

Новое правило
Укажите название правила и выберите действие, которое должно быть выполнено с документом MS Office/AutoCAD

Имя правила: Автоматическая установка метки

Объект: Документы MS Office/AutoCAD

Действие: Установка метки При сохранении документа

Настройки

Если в документе: отсутствует метка, то: установить...

Выберите метку

- Строго конфиденциально
- Для служебного пользования
- Секретно
- Коммерческая тайна
- Бухгалтерия
- Общедоступно
- Коммерческая тайна
- Новая метка 8
- Новая метка 9
- Новая метка 10

☐ Только если ранее установленная метка имеет приоритет ниже выбранной

< Назад Далее > Отмена

Но можно придумать что-то более-менее универсальное с движением в сторону RMS и ABAC



СПАСИБО ЗА ВНИМАНИЕ!

SEARCHINFORM



<https://t.me/searchinform>



[https://vk.com/
securityinform](https://vk.com/securityinform)

ПРАКТИКА И АНАЛИТИКА



[https://searchinform.ru/
practice-and-analytics/](https://searchinform.ru/
practice-and-analytics/)