SEARCHINFORM
INFORMATION SECURITY

ПРЕДУПРЕЖДЕНИЕ
корпоративного мошенничества на всех этапах:

от приема на работу до увольнения

Сергей Ананич
Начальник отдела продаж
«СёрчИнформ»

Инцидент – на любом этапе

Испытательный срок

Карьера

Подготовка к увольнению

Инцидент

Инцидент

Инцидент

Увольнение

Склонности

Работа в команде

Сбор приданого

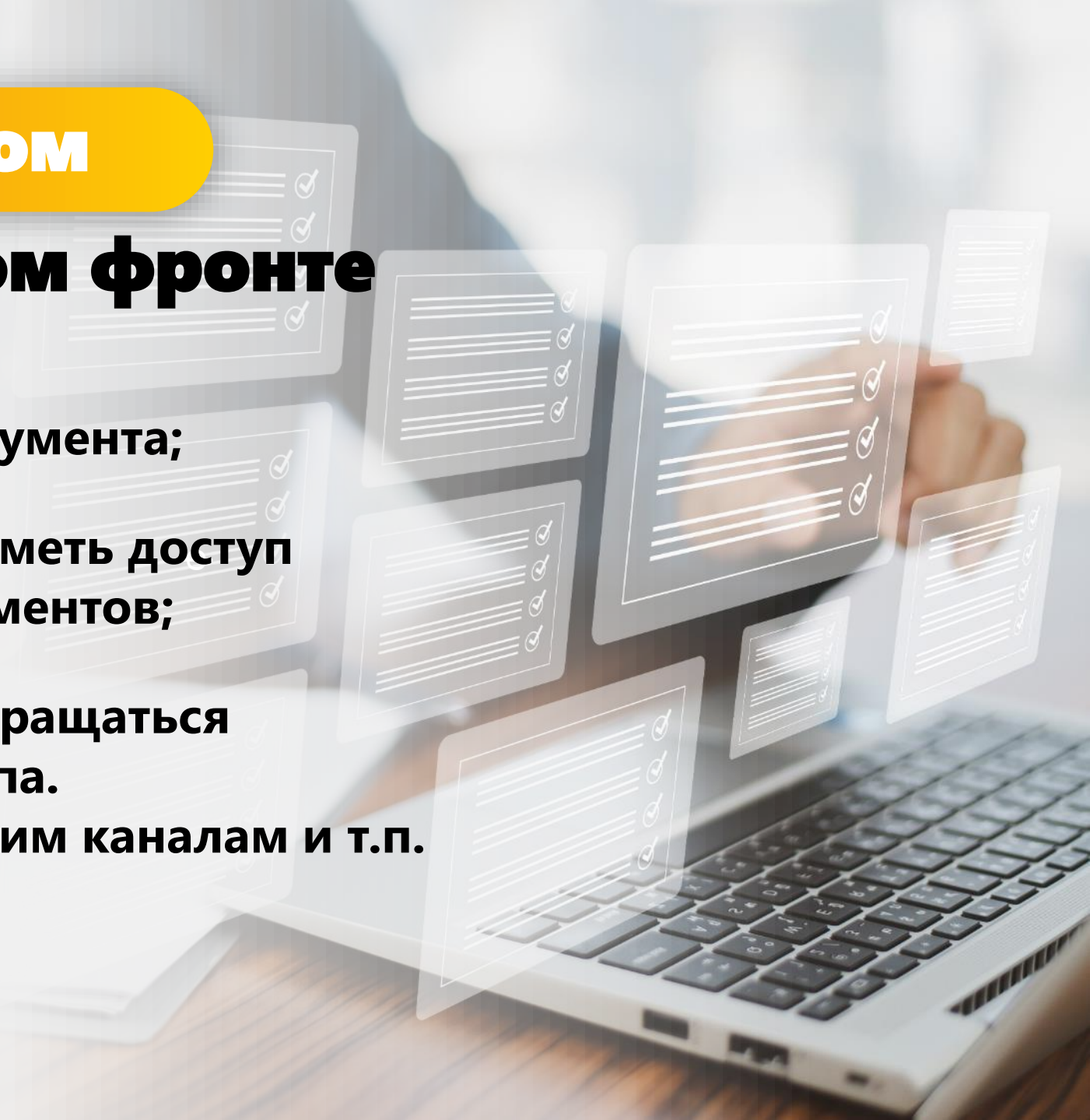
Общение с экс-коллегами

SEARCHINFORM

Борьба с инцидентом

на информационном фронте

- Определяем класс/тип документа;
- Определяем, кто должен иметь доступ к такому классу/типу документов;
- Определяем, как может обращаться документ такого класса/типа. Кому пересылаться, по каким каналам и т.п.



SEARCHINFORM

Определение класса\типа документа

450+

предустановленных шаблонов

SEARCHINFORM

FileAuditor. Шаблоны

Создание предустановленных условий поиска, которые могут быть использованы при настройке правил классификации данных

Добавить | Изменить | Удалить | Экспорт | Импорт | Добавить группу

Имя	Объекты	Условия поиска	Действие	Сканирование
Интеллектуальная собственность				
Техническая документация	*.001,*.7Z,*.AR...	Сложный запрос	Аудит	На агенте и сервере
Исходный код	*.CPP,*.DPR,*.P...		Аудит	На агенте и сервере
Цифровые сертификаты (цифровые подписи)	*.CRT,*.CER,*.0...	По атрибутам фай...	Аудит	На агенте и сервере
Файлы DWG	*.DWG,*.001,*....	По атрибутам фай...	Аудит	На агенте и сервере
Комплект ФСТЭК	*.001,*.7Z,*.AR...	По тексту | По те...	Аудит	На агенте и сервере
Персональные данные сотрудников				
Мобильные телефоны РФ > 10	*.001,*.7Z,*.AR...	По регулярным вы...	Аудит	На агенте и сервере
Номера телефонов > 10	*.001,*.7Z,*.AR...	По регулярным вы...	Аудит	На агенте и сервере
ФИО > 20	*.001,*.7Z,*.AR...	По регулярным вы...	Аудит	На агенте и сервере
ФИО + паспорт РФ	*.001,*.7Z,*.AR...	По регулярным вы...	Аудит	На агенте и сервере
ФИО + мобильный телефон РФ	*.001,*.7Z,*.AR...	По регулярным вы...	Аудит	На агенте и сервере
ФИО + паспорт РФ + банковская карта	*.001,*.7Z,*.AR...	По регулярным вы...	Аудит	На агенте и сервере
ФИО + паспорт РФ + мобильный телефон РФ	*.001,*.7Z,*.AR...	По регулярным вы...	Аудит	На агенте и сервере
ФИО + СНИЛС	*.001,*.7Z,*.AR...	По регулярным вы...	Аудит	На агенте и сервере
Скан паспорта РФ	*.001,*.7Z,*.AR...	Сложный запрос	Аудит	На агенте и сервере
ИНН физлица	*.001,*.7Z,*.AR...	По регулярным вы...	Аудит	На агенте и сервере
Военный билет	*.001,*.7Z,*.AR...	По регулярным вы...	Аудит	На агенте и сервере
Диплом	*.001,*.7Z,*.AR...	Сложный запрос	Аудит	На агенте и сервере
Свидетельство о браке	*.001,*.7Z,*.AR...	По тексту & По те...	Аудит	На агенте и сервере
Свидетельство о рождении	*.001,*.7Z,*.AR...	По тексту & По те...	Аудит	На агенте и сервере
Документы воинского учета	*.001,*.7Z,*.AR...	По тексту	Аудит	На агенте и сервере
Банковские реквизиты сотрудника	*.001,*.7Z,*.AR...	Сложный запрос	Аудит	На агенте и сервере
Трудовой договор	*.001,*.7Z,*.AR...	По тексту & По те...	Аудит	На агенте и сервере
Уведомление для миграционной службы	*.001,*.7Z,*.AR...	По тексту & По те...	Аудит	На агенте и сервере
Личная карточка сотрудника	*.001,*.7Z,*.AR...	По тексту & По те...	Аудит	На агенте и сервере
Персональные данные общие				
Клиентские базы	*.001,*.7Z,*.AR...	Сложный запрос	Аудит	На агенте и сервере
Табель	*.001,*.7Z,*.AR...	Сложный запрос	Аудит	На агенте и сервере
Штатное расписание	*.001,*.7Z,*.AR...	По атрибутам фай...	Аудит	На агенте и сервере
Финансовая информация и платежные документы				
Персональная финансовая информация				
Подозрительная активность				
Без группы				

Настраиваем блокировки (при необходимости)

Редактирование правила. Файлы по классификации (FileAuditor)

Имя правила: Rule 12

Действие: Разрешено Запрещено Аудит: Выключено Поиск:

Объекты | Файлы | Метки | Пользователи и группы | Компью

Приложения | Процессы

- **Пользовательские**
  - Word *\winword.e
- **Системные**
  - Browser *\browser.e
  - Cloud *\applephot
  - ICQ/MMP *\icq.exe;*
  - Jabber *\ciscojabbe
  - Lync *\lync.exe;
  - Mail *\outlook.e
  - Messengers *\slack.exe
  - Remote Control *\radmin.ex
  - Skype *\Skype.exe
  - Teams *\teams.exe
  - Telegram *\telegram.exe
  - Viber *\Viber.exe
  - WhatsApp *\WhatsApp.exe

Изменить | Добавить | Удалить

OK | Отмена

Редактирование приложений и процессов

Имя приложения: UserApp

Процессы: *\userapp.exe

Очистить | Изменить | Добавить | Удалить

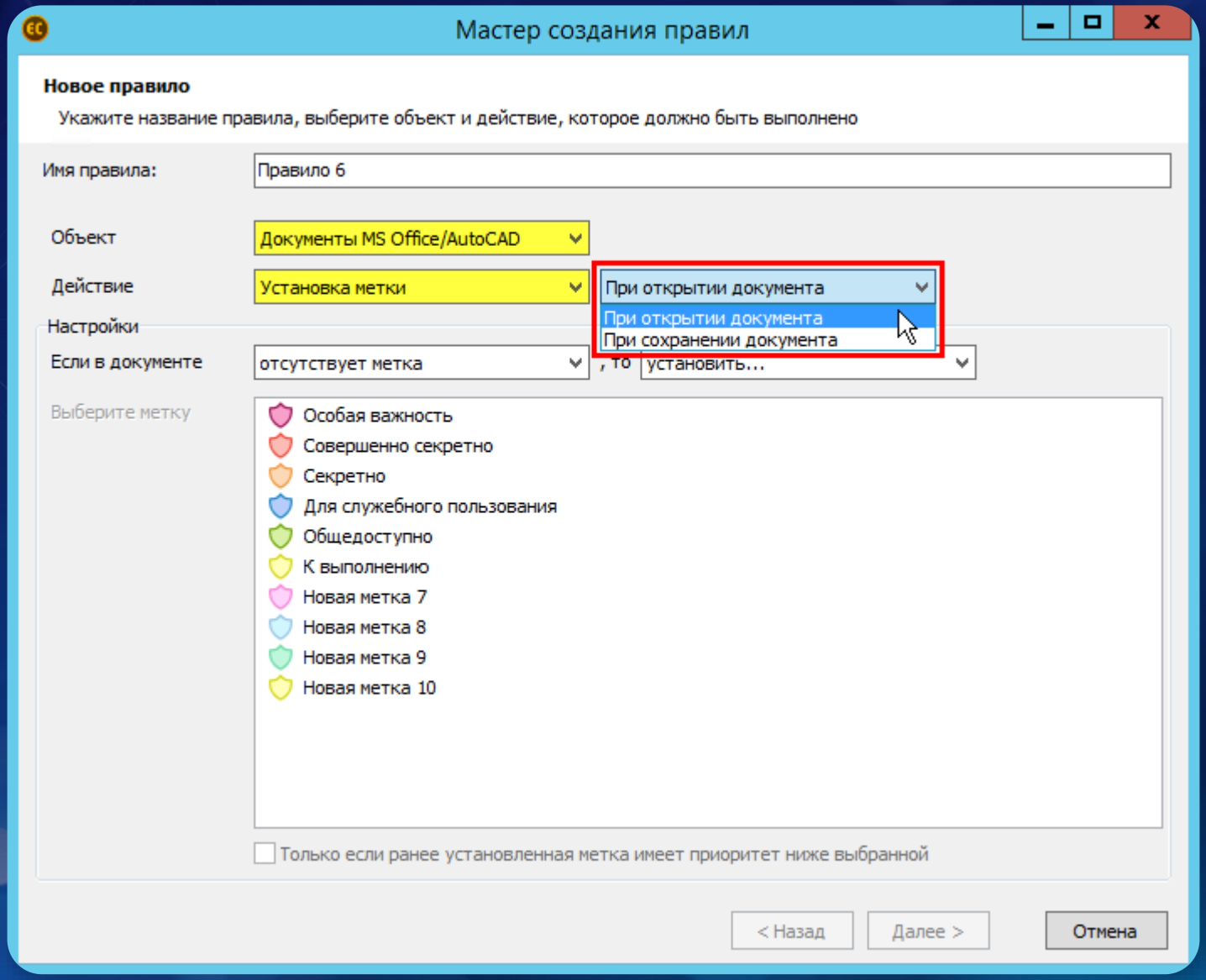
OK | Отмена

Ответственность сотрудника

SEARCHINFORM

Открытый контроль с метками ручной классификации:

- Кастомизация отображения ручной метки в колонтитулах
- Рекомендации пользователю по замене ручной метки
- Автоматическое управление ручными метками (исправление ошибок пользователя)
- Уведомления



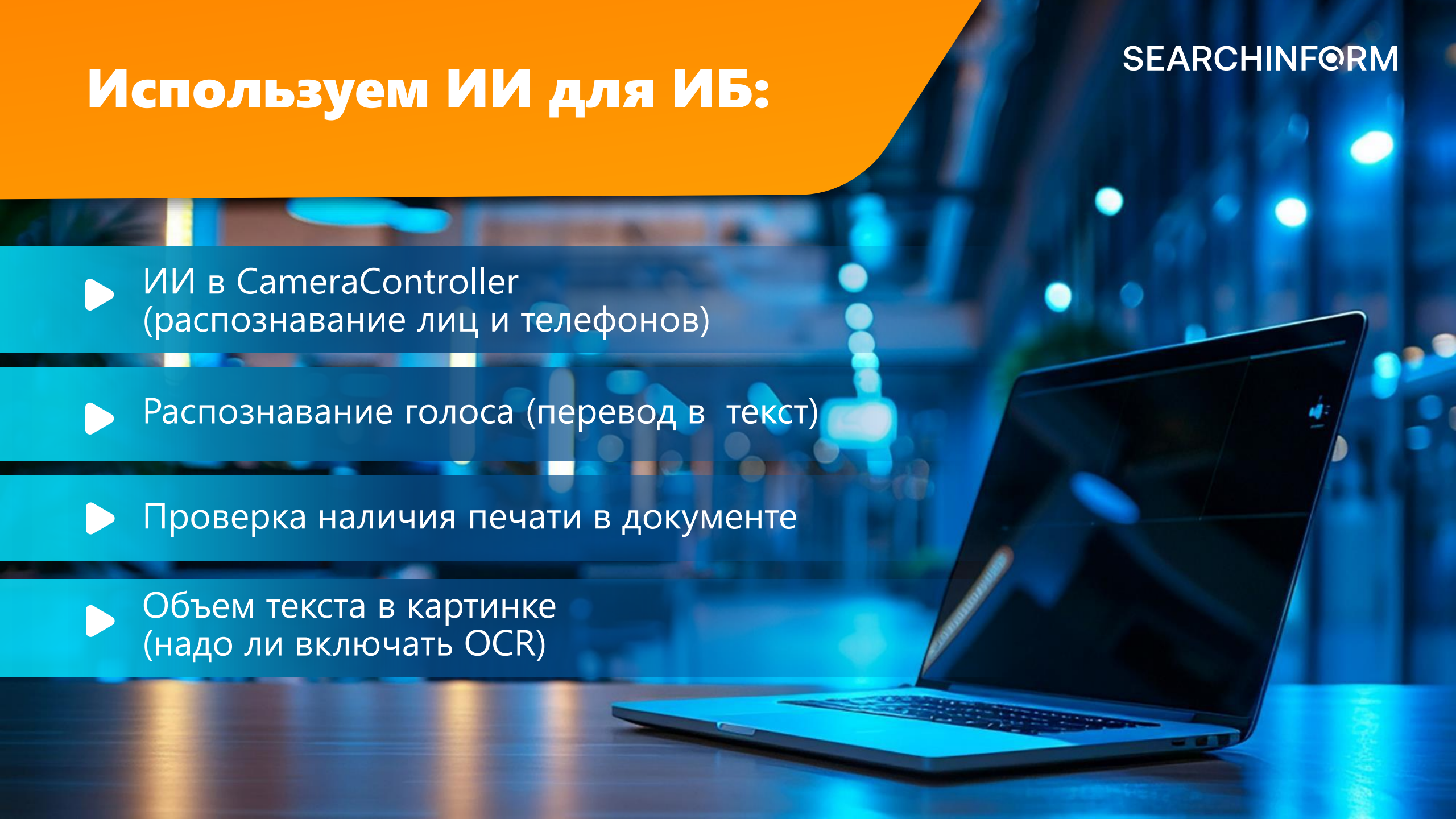
Контроль гибридной инфраструктуры

Удаленная... работа?

Используем ИИ для ИБ:

SEARCHINFORM

- ИИ в CameraController (распознавание лиц и телефонов)
- Распознавание голоса (перевод в текст)
- Проверка наличия печати в документе
- Объем текста в картинке (надо ли включать OCR)



КЕЙС

Окопавшийся «крот»

Что произошло: компания установила системы ИБ и выяснила, что сотрудник крадет почту руководителя, чтобы пересылать конкурентам.

Как выяснили: в SIEM сработало правило «Доступ к почтовому ящику не владельцем». Расследование в DLP показало, что зеркалирование почты коллеги инсайдер настроил втайне.

Ущерб компании: ~ 2 млн $

SEARCHINFORM

КЕЙС

Окопавшийся «крот»

Что в итоге: Нарушителя уволили на основании п. «в» ч. 6 ст. 81 ТК РФ (разглашение охраняемой законом коммерческой тайны).

Инсайдера осудили по ч. 1 и 2 ст. 183 УК РФ.

Наказание – 1 год 9 месяцев исправительных работ с удержанием 15% зарплаты в доход государства.

SEARCHINFORM

КЕЙС

Промышленный шпионаж

Что произошло: промышленная компания стала проигрывать тендеры, конкуренты вывели на рынок аналогичную продукцию.

Что узнали: сотрудник отдела продаж пересылал конкурентам коммерческую и конструкторскую документацию. Выяснилось, что его перекупили и затем шантажировали. По переписке стало понятно, что он действует не один.

SEARCHINFORM

КЕЙС

Промышленный шпионаж

Что в итоге: с результатами расследования обратились к деловым партнерам. Показали, какими методами действует их нынешний поставщик, отношения восстановили.

За несколько месяцев конкурирующая фирма потеряла финансирование и была закрыта.

Предотвращенный ущерб: > 100 млн $

SEARCHINFORM

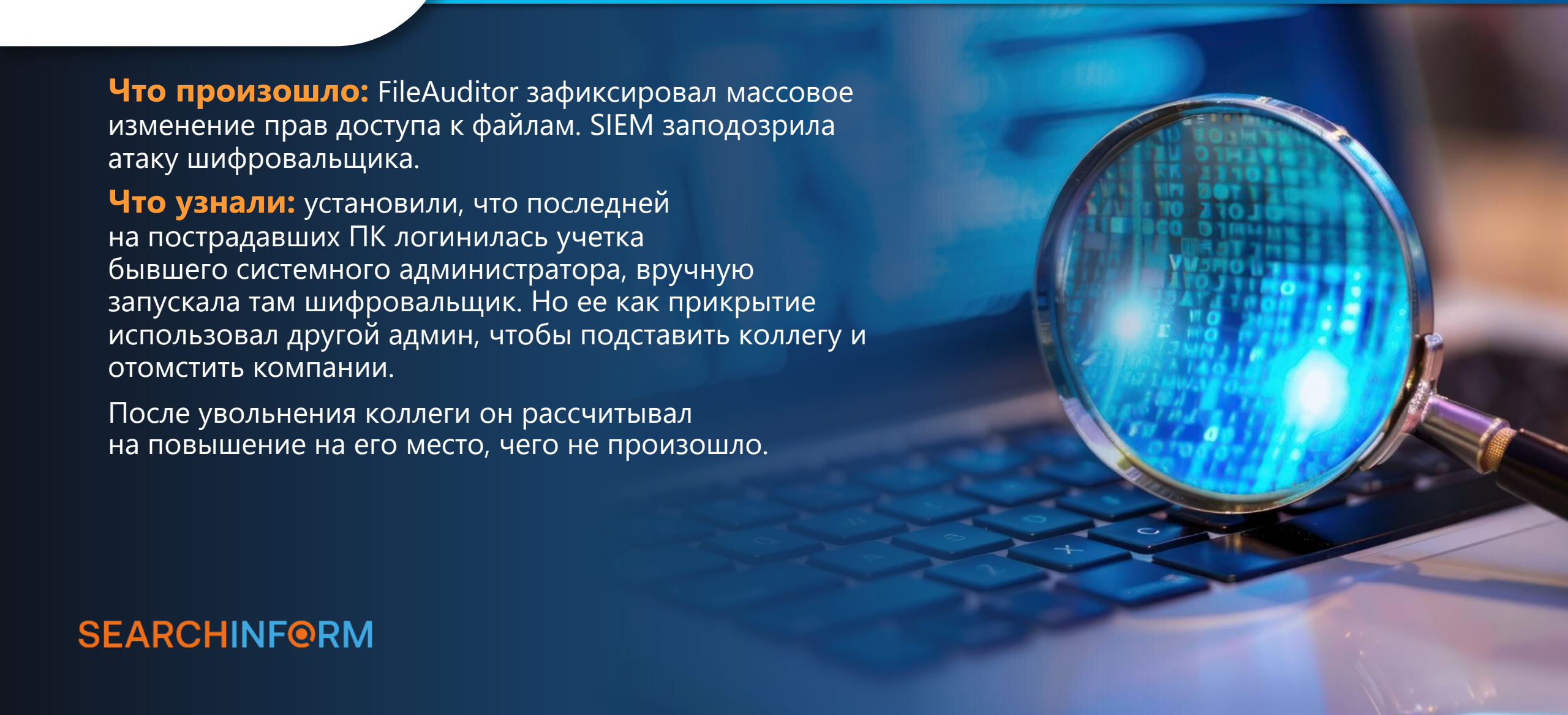
КЕЙС

Инсайдер-вымогатель

Что произошло: FileAuditor зафиксировал массовое изменение прав доступа к файлам. SIEM заподозрила атаку шифровальщика.

Что узнали: установили, что последней на пострадавших ПК логинилась учетка бывшего системного администратора, вручную запускала там шифровальщик. Но ее как прикрытие использовал другой админ, чтобы подставить коллегу и отомстить компании.

После увольнения коллеги он рассчитывал на повышение на его место, чего не произошло.



SEARCHINFORM

КЕЙС

Инсайдер-вымогатель

Что в итоге: атаку успели остановить, данные восстановили из теневых копий. Установили, что внутренний нарушитель планировал потребовать выкуп за дешифровку данных. Его уволили.

Предотвращенный ущерб: > 500 тыс $
(из расчета среднего размера запрашиваемого выкупа при атаке шифровальщика в России – **данные F.A.C.C.T.**, 2023 г.)

SEARCHINFORM

Важный урок для бизнеса

Кейс: Инсайдер-вымогатель

Пароли – это важно.
Еще важнее – многофакторная защита.

- Блокируйте аккаунты бывших сотрудников.
- Контролируйте «угон» и расшаривание аккаунтов.
- Сбрасывайте пароли.
- Вводите второй фактор аутентификации.
- Не делайте исключений для привилегированных сотрудников.

SEARCHINFORM

КЕЙС

Мошенничество и откаты

Что произошло: в топливной компании сотрудник отдела опломбирования договаривался на «свой процент» от продажи топлива с коллегой из подразделения по устранению нарушений опломбирования.

Что узнали: сотрудник намеренно ставил неверную пломбу, чтобы машина с топливом отправилась в отдел по устранению нарушений. Там из машин сливали топливо для последующей перепродажи.

SEARCHINFORM

КЕЙС

Мошенничество и откаты

Что в итоге: заказчик устранил схему и усовершенствовал процесс контроля за количеством топлива. Нарушителей наказали.

Предотвращенный ущерб:
до 100 тыс $

SEARCHINFORM

Спасибо за внимание!

SEARCHINFORM
INFORMATION SECURITY

https://t.me/searchinform

https://vk.com/
securityinform

Практика и аналитика

https://searchinform.ru/
practice-and-analytics/