



КОД  
ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ

**#CODEIB**

# ВАРИАТИВНОСТЬ ИСПОЛЬЗОВАНИЯ DLP-СИСТЕМЫ

**Александр Кулик**

Ведущий специалист

# Falcongaze SecureTower



13 лет на рынке



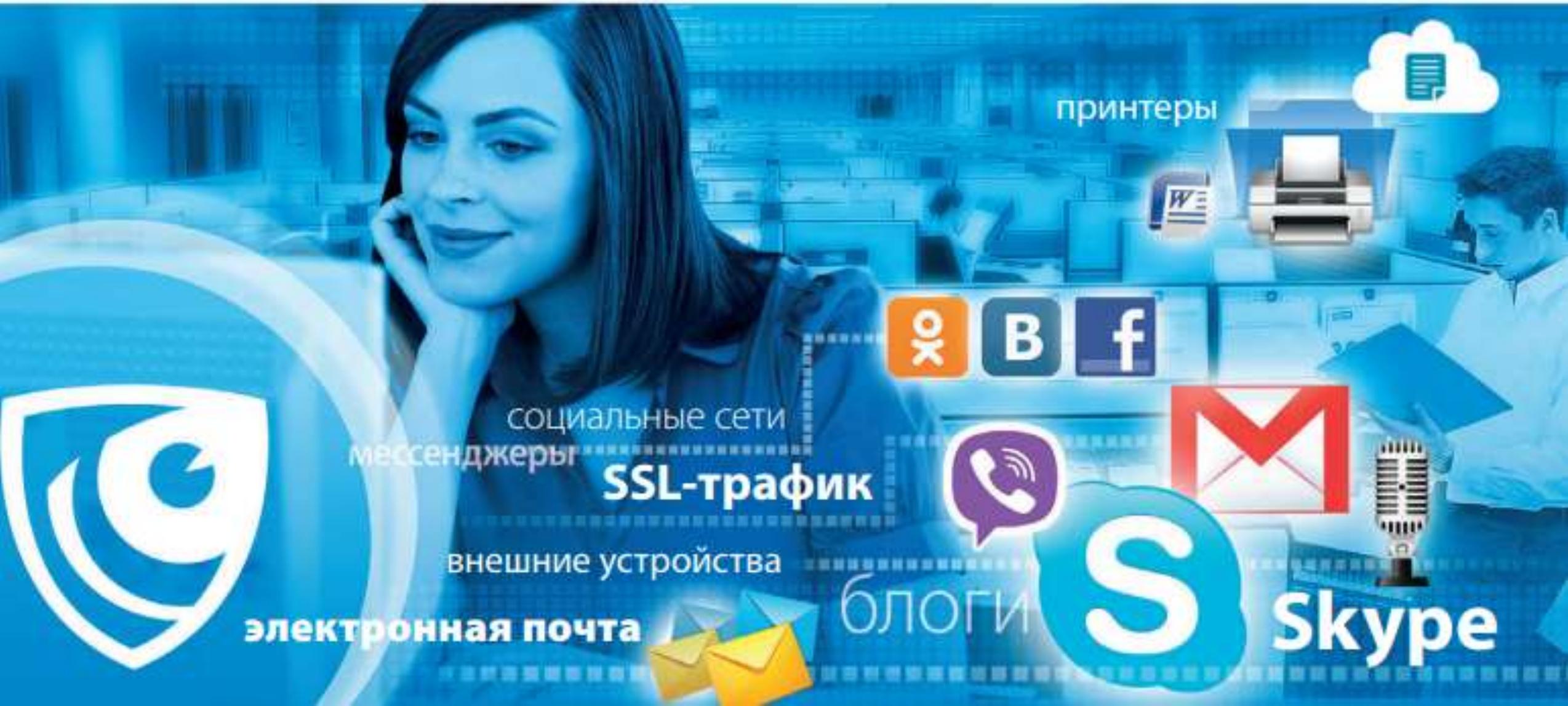
30 стран



1000+ клиентов



# КОНТРОЛИРУЕМЫЕ КАНАЛЫ ПЕРЕДАЧИ ДАННЫХ



A 3D visualization of financial data, including a bar chart, a line graph, and a pie chart, all rendered in shades of blue and white. The pie chart is the central focus, with several slices cut out. The background features a grid and various data points.

# 90% утечек по вине персонала

50% уволенных сотрудников забирают  
конфиденциальные данные

«За любым внешним инцидентом стоит  
внутренняя ошибка»

Панкевич Иван Анатольевич,  
Начальник комплаенс управления ОАО «БНБ-Банк»

# СУЩЕСТВУЕТ ЛИ ЕДИНСТВЕННО ВЕРНЫЙ МЕТОД?

Единое правило?

Четкая инструкция?

Одно решение?

# КОМПЛЕКСНЫЙ ПОДХОД

---

Все методы верны!  
Какой выберете вы?

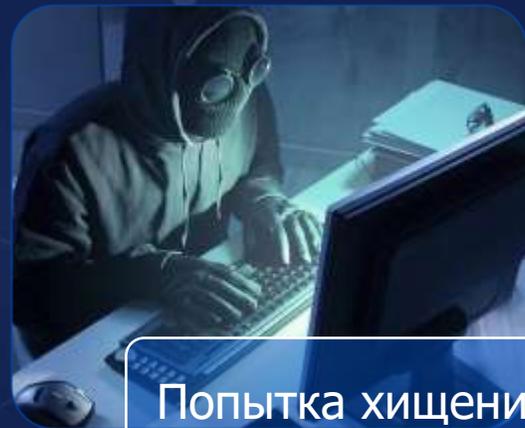
# Кейс: сговор о предоставлении базы данных клиентов компании-конкуренту



Предложение от компании-конкурентов



Сговор с сотрудниками



Попытка хищения информации

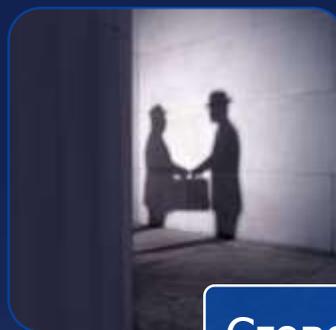
- Правила безопасности:
  - по словарю
  - по цифровому отпечатку
  - статистические

- Граф-анализатор

- Модуль расследований



Предложение от  
компании-конкурентов



Сговор с сотрудниками



Попытка хищения  
информации

- Анализ рисков

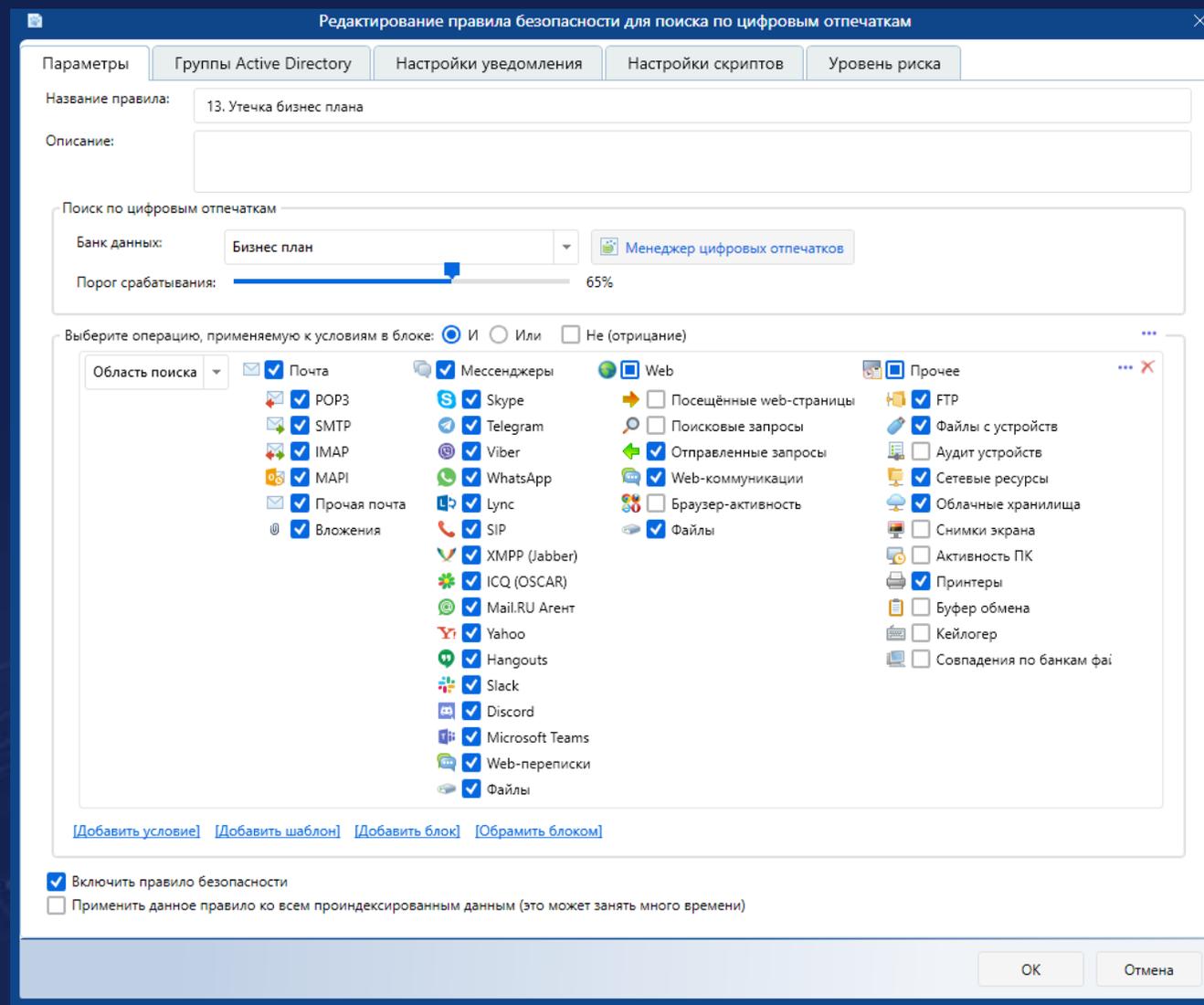
- Поиск

- **Перехват:**

- почты
- **Мессенджеры**

**Голосовых сообщений  
(распознавание)**

# Правило безопасности – по цифровому отпечатку



# Правило безопасности – по цифровому отпечатку

The screenshot displays the FalcoGaze SecureTower Client console interface. The main window is titled "Политики безопасности" (Security Policies) and shows a list of policies. The selected policy is "13. Утечка бизнес плана" (Business Plan Leak), which is highlighted in blue. The console shows the following data for this policy:

Имя	Подписки	Инциденты	Уровень риска	Статус
FalcoGaze SecureTower Security policies Group		966 / 964	73 660 / 73 6	
Samples		966 / 964	73 660 / 73 6	
En		0 / 0	0 / 0	
En		966 / 964	73 660 / 73 6	
01. Контроль локальности сотрудников		60 / 60	3 642 / 3 642	
02. Контроль поиска работы		131 / 131	11 387 / 11 1	
03. Контроль использования облачных хранилищ		0 / 0	0 / 0	
04. Контроль почты		409 / 409	35 154 / 35 1	
05. Расходование ресурсов компании		81 / 81	2 851 / 2 851	
06. Поиск паролей		0 / 0	0 / 0	
07. Нарушение законодательства РФ		133 / 132	10 948 / 10 4	
08. Утечка информации		0 / 0	0 / 0	
09. Утечка ПДн (ФЗ №152)		0 / 0	0 / 0	
10. Утечка бухгалтерской и управленческой докумен		152 / 151	9 673 / 9 475	
01. Бухгалтерский баланс		0 / 0	0 / 0	
02. Отчет о финансовых результатах		0 / 0	0 / 0	
03. Счет о движении денежных средств		0 / 0	0 / 0	
04. Внутренние выплаты денежными средствами		0 / 0	0 / 0	
05. Анализ затрат		0 / 0	0 / 0	
06. Состраение счетов		0 / 0	0 / 0	
07. Ведомость оплаты труда		0 / 0	0 / 0	
08. Выписка ЕГРЮЛ		0 / 0	0 / 0	
09. Контроль движения планов платежей		21 / 21	1 533 / 1 533	
10. Настоящие декларации по налогу на прибыль		0 / 0	0 / 0	
11. Уведомление документи		0 / 0	0 / 0	
12. Контроль отправки почты сотрудников		128 / 128	7 740 / 7 740	
13. Утечка бизнес плана		1 / 0	200 / 0	
14. Утечка счета по прибылям и убыткам		1 / 1	200 / 200	
11. Повышение привилегий / запуск специализирова		0 / 0	0 / 0	

The right-hand pane shows the details of the selected policy, including the document preview. The document is titled "Бизнес план" (Business Plan) and is from the "Исследовательского Фонда Предпринимательства «Бизнес Лаборатория»" (Research Fund of Entrepreneurship «Business Laboratory»).

# Правило безопасности – по словарю

The screenshot displays the Falcongaze Secure Tower Client console interface. The left pane shows a tree view of security policies under 'Falcongaze SecureTower Security policies Group'. The right pane shows search results for a specific policy.

Название	Подписчики	Инциденты	Уровень риска	Статус
Falcongaze SecureTower Security policies Group	978 / 973	75 316 / 74 4		
Samples	978 / 973	75 316 / 74 4		
En	0 / 0	0 / 0		
Ru	978 / 973	75 316 / 74 4		
01. Контроль законности сотрудников	66 / 66	3 642 / 3 642		
02. Контроль поиска работы	131 / 131	11 397 / 11 3		
03. Контроль использования облачных хранилищ	0 / 0	0 / 0		
04. Контроль почты	409 / 409	35 154 / 35 1		
05. Расходование ресурсов клиента	61 / 61	2 851 / 2 851		
06. Поиск паролей	0 / 0	0 / 0		
07. Нарушение законодательства РФ	133 / 132	10 943 / 10 3		
08. Утечка информации	12 / 10	1 556 / 1 256		
1. Контроль утечек конфиденциальных документов	0 / 0	0 / 0	Документы с профи...	
2. Контроль утечек служебных документов	0 / 0	0 / 0	Документы с профи...	
3. Контроль файлов с измененными разрешениями	1 / 1	86 / 86		
4. Контроль зашифрованных файлов	5 / 5	370 / 370		
5. Контроль документов с печатями	0 / 0	0 / 0	Необходимо добави...	
6. Контроль утечки файлов КД (doc, docx)	0 / 0	0 / 0		
7. Утечка клиентской базы	6 / 4	1 200 / 800		
09. Утечки ПИН (03 NR132)	0 / 0	0 / 0		
10. Утечки бухгалтерской и управленческой докумен...	152 / 150	9 673 / 9 271		
11. Повышение привилегий / запуск специализирован...	0 / 0	0 / 0		

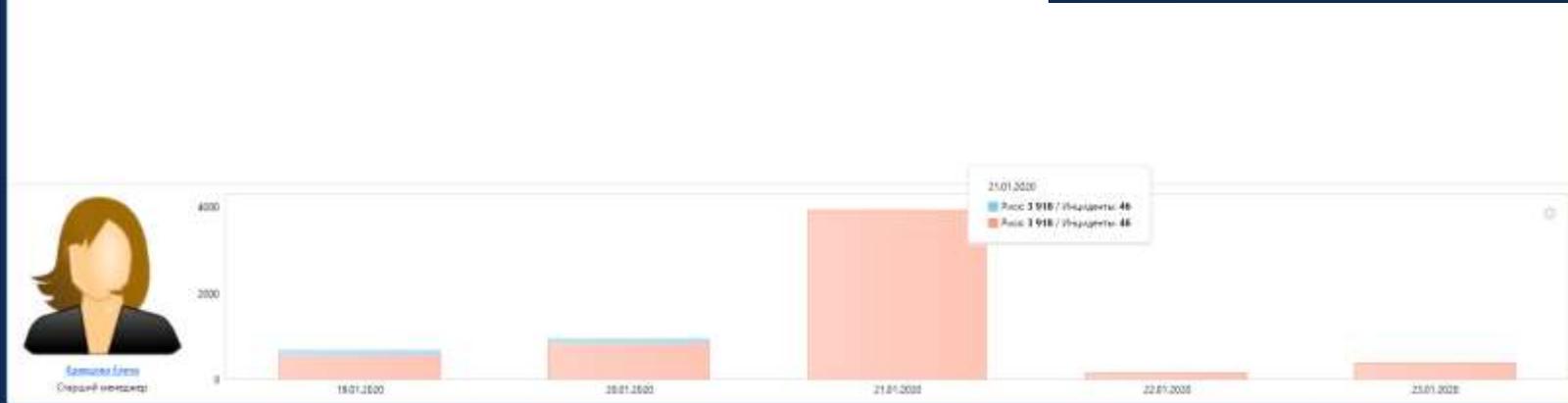
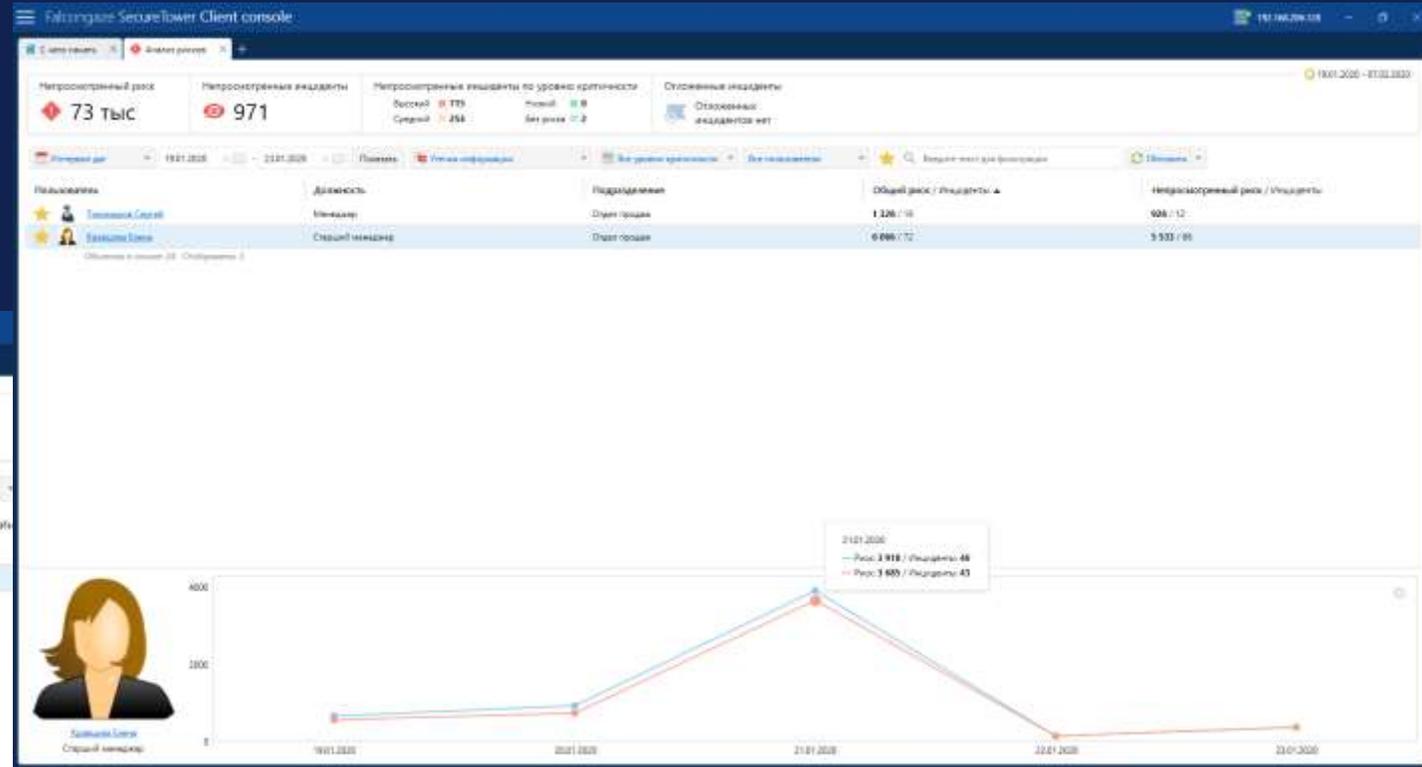
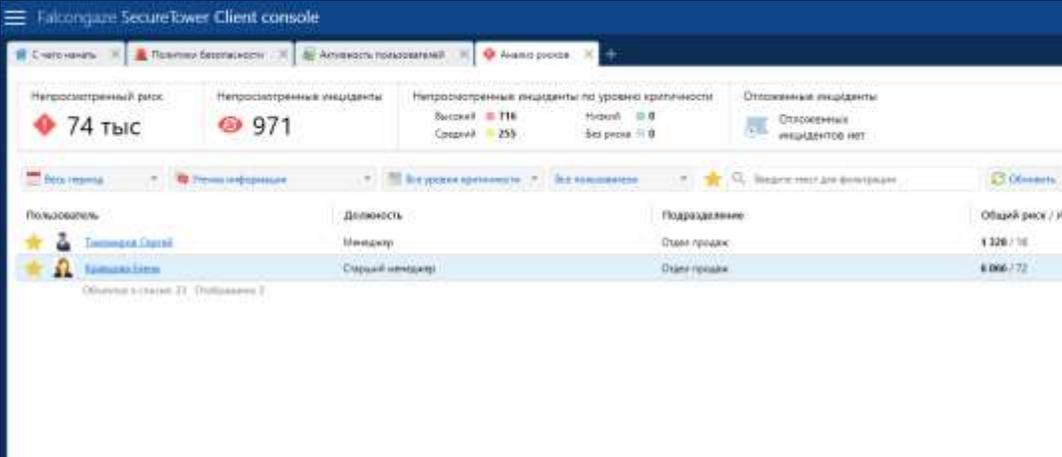
Search results for 'Утечка клиентской базы' (Incident ID: 16.01.2020 10:25:53):

№	Состояние	Тип данных	Локальный пользователь	Удаленный пользователь	Переведено	Размер	Прим...
1	?	File Skype	Красилова Елена	elena_krasilova	16.01.2020 10:25:53	21,7 KB	
2	?	File Telegram	Красилова Елена	elena_krasilova	20.01.2020 14:55:00	21,7 KB	
3	?	Файл с USB устройств	Тимошенко Сергей	sergey.timoshenko	20.01.2020 11:30:15	9,17 KB	
4	?	FTP-файл	Тимошенко Сергей	sergey.timoshenko	20.01.2020 13:04:19	16,5 KB	
5	?	FTP-файл	Красилова Елена	elena_krasilova	21.01.2020 16:30:00	16,5 KB	
6	?	Почтовое вложение	Красилова Елена	elena_krasilova	20.01.2020 16:22:38	9,51 KB	

Details for incident 7: 'Утечка клиентской базы' (Уровень риска: 200). Local user: Красилова Елена. Remote user: elena\_krasilova. File name: Customer Database\_ver.Lata. Path: \\net.lenta.lenta...share\pub\ -> \\Customer Database\_ver.Lata.

Наименование организации	Сумма сделки, руб	количество сотрудников	Наименование организации	Сотрудники, участвующие в презентации, ФИО	Наименование ср...			
mobilitycenter (РО)	>30	Завод металлоконструкций (РФ)	Иванов Алексей Иванович	Брянский завод металлоконструкций (РО)	70%	30		
Экспрест (ур)	100	АСТАНОПОЛИНГ	Гальцев Петр Васильевич	Текно-Трейд	90%	170	22.000.000	Текно-Трейд
Матвильн "Кооператур", ООО "Кооператур" (РФ)	>25	ПАНЧЕВАРИЙСКИЙ БАНК	Панков Глеб Васильевич	Синимекс-ПР	50%	350	38.000.000	
Бедеральная коллегия по налогам (РФ)	>50	МАРА	Рапулов Илья Петрович	Синимекс-Коллекс	60%	96	12.000.000	
ПЕРВЫЙ ПОЛЬСКО-РОССИЙСКИЙ БАНК (ПРБ банк)	300	Центрифастрой	Арсений Васильевич Зудин	БАНК ТЕЛЕКОМ	Азаматос Эман Эдуардович			
БАНК ТЕЛЕКОМ	100	Центрифастрой	Арсений Васильевич Зудин	БАНК ТЕЛЕКОМ	Азаматос Эман Эдуардович			
Завод металлоконструкций (РО)	300	Текно Трейд	Басюков Дмитрий Валерьевич					
Детектообработывающий завод №8	>25	Текно Трейд	Басюков Дмитрий Валерьевич					
Органик-Конлайн	>25							
Синимекс-ПР	>25							
Центрифастрой	>25							
СВК (Смоленский завод керамических изделий)	100							
НИИ Автоматизации и стандартизации	100							
АГАТЭЖ	50							
МАРА	100-150							
Текно Трейд	250							
Убинский Масскомбинат	70							

# Анализ рисков



Вариативность отображения отчета

# Анализ рисков

**Falcongaze SecureTower Client console**

Кравцова Елена  
Специальный менеджер,  
Отдел продаж

46  
Высокий 45  
Средний 1  
Низкий 0  
Без риска 0

21 января 2020 г. 16:30:00  
Кравцова Елена  
Правило безопасности: 7. Утечка клиентской базы  
Локальный адрес: 192.168.0.14  
Имя переданного файла: Customer Database.xls  
Тип: FTP-файл. Размер: 10.5 KB

21 января 2020 г. 18:35:26  
Кравцова Елена - Васильева Надежда  
Правило безопасности: 08. Контроль движения планов платежей  
Локальный адрес: 192.168.1.75  
Локальный имя пользователя: удаленный\_пользователь4  
Удаленный\_адрес: удаленный\_адрес  
Количество сообщений: 301  
Тип: Передача базы

21 января 2020 г. 12:24:33  
Кравцова Елена  
Правило безопасности: 08. Контроль движения планов платежей  
Локальный адрес: 192.168.0.14  
Программа: Microsoft Office Word  
Принтер: HP Color LaserJet 3700 PCL 6  
Количество страниц: 10  
Тип: Принтер. Размер: Количество страниц: 10

21 января 2020 г. 16:44:23  
Кравцова Елена  
Правило безопасности: 12. Контроль отправки ссылки сотрудникам  
Локальный адрес: 192.168.0.14  
Количество ссылок: 43  
Тип: HTTP-ссылка

21 января 2020 г. 15:25:26  
Кравцова Елена - jobu@oobio.ru  
Правило безопасности: 2. Контроль исходящей почты на внешние провайдеры адреса  
Локальный адрес: 192.168.0.14  
Локальный\_адрес: Елена Кравцова <elena.kravtsova@falcongaze.com>  
Удаленный\_адрес: jobu@oobio.ru  
Тема: Кравцова Елена резюме  
Тип: Почтовое сообщение (Почтовый SMTP). Размер: 61.8 KB

Создать | Удалить | Поиск | Открыть во внешней программе | Добавить в дело | Детальная информация

Принято: 21.01.2020 16:30:00 | С IP: 192.168.0.14 | Протокол: FTP | Размер: 10.5 KB

7. Утечка клиентской базы | Уровень риска: 200 | Текущий статус инцидента: ?

Локальный пользователь: Кравцова Елена

Информация

Текущий документ может быть найден по следующему пути:

Аудит FTP-файла: 192.168... -> Customer Database.xls

Подсказка: найдено 0/3

Page 1

Список клиентов. Экспорт

Software and Technology

SAP
Microsoft
BEA Systems
Oracle
ATG
Thomson Reuters
Sun Microsystems
Consola CRM
Intelligence
LogicLibrary, Inc.
Misys
Datalex
i-many
Highlight
Idiom
Instant Information
Connotate Technologies
Wildnet Group

Healthcare and insurance

CareFirst BlueCross BlueShield
SBU USA Mutual Life Insurance Company
BlueCross BlueShield of Minnesota

# Анализ рисков

The screenshot displays the FalcoSecure Client console interface. At the top, the user profile for Elena Kravtsova is shown, including her name, role (Senior Manager, Sales Department), and a risk score of 72. Below this, a list of security incidents is visible, with the most recent one dated January 19, 2020, at 16:25:53. The incident details show a file transfer from a local user to a remote user, with the file name 'Customer Database\_ver1.xlsx'. The right-hand pane provides a detailed view of this incident, including the file name, local and remote user information, and a list of associated incidents. A table at the bottom right of the console lists various entities and their associated risk scores.

Entity	Score
3 Магистр "Кoopресурс", ООО "Кoopресурс" (РР)	25
4 Федеральная комиссия по налогам (РР)	50
5 ПЕРВЫЙ ПОЛЬСКО-РОССИЙСКИЙ БАНК (ПРР-банк)	300
6 БАНК ТЕЛЕКОМ	100
7 Завод металлоконструкций (РР)	300
8 Зернообработательский завод (РР)	300
9 Орбис-Суперст	+25
10 Орбис-ПН	+25
11 Центрифрост	+25
12 СЭМ (Системный центр коммерчески отдел)	100
13 НИИ Автоматизации и стандартизации	100
14 АГАТЭК	50
15 МАРА	100-150
16 Техно-Трейд	250
17 Урэнский Мастеробитум	30

# Граф-анализатор

## Привязка информации к пользователям

Укажите привязку информации к пользователям для идентификации пользователей

Доступная информация:

oleg\_prozоров

Олег Прозоров

Введите текст для фильтрации пользователей:

Введите текст

Пользователь	Организация	Подразделение
Халтурин Вадим	БизнесПро	Технический от,
Тихомиров Сергей	БизнесПро	Отдел продаж
Олег Прозоров		
Кравцова Елена	БизнесПро	Отдел продаж
Коваленко Марина	БизнесПро	Отдел по работ
Казаков Денис	БизнесПро	Отдел по работ
Иванов Александр	БизнесПро	Отдел продаж
Зубарева Инна	БизнесПро	Отдел по работ
Зверев Николай	БизнесПро	Отдел продаж
Жухов Михаил	БизнесПро	Управление
Жданова Юлия	БизнесПро	Бухгалтерия
Дроздов Алексей	БизнесПро	Отдел продаж
Голубцов Антон	БизнесПро	Технический от,
Говорухина Анна	БизнесПро	Юридический о
Волков Иван	БизнесПро	Отдел продаж
Ветров Федор	БизнесПро	Юридический о
Васильева Надежда	БизнесПро	Отдел кадров
Бурковский Георгий	БизнесПро	Управление
Белкин Андрей	БизнесПро	Отдел по работ

< Привязать

Отказать >

Добавить пользователя

Закрыть

Привязка информации к пользователям

Укажите привязку информации к пользователям для идентификации пользователей

Доступная информация: oleg\_prozоров (нет привязки)

Введите текст для фильтрации пользователей:

Пользователь	Организация	Подразделение
Administrator		
Scarekin910 scare		
Андреева Татьяна	БизнесПро	Управление
Белкин Андрей	БизнесПро	Отдел по работ
Бурковский Георгий	БизнесПро	Управление
Васильева Надежда	БизнесПро	Отдел кадров
Ветров Федор	БизнесПро	Юридический о
Волков Иван	БизнесПро	Отдел продаж
Говорухина Анна	БизнесПро	Юридический о
Голубцов Антон	БизнесПро	Технический от,
Дроздов Алексей	БизнесПро	Отдел продаж
Жданова Юлия	БизнесПро	Бухгалтерия
Жухов Михаил	БизнесПро	Управление
Зверев Николай	БизнесПро	Отдел продаж
Зубарева Инна	БизнесПро	Отдел по работ
Иванов Александр	БизнесПро	Отдел продаж
Казаков Денис	БизнесПро	Отдел по работ
Коваленко Марина	БизнесПро	Отдел по работ
Кравцова Елена	БизнесПро	Отдел продаж

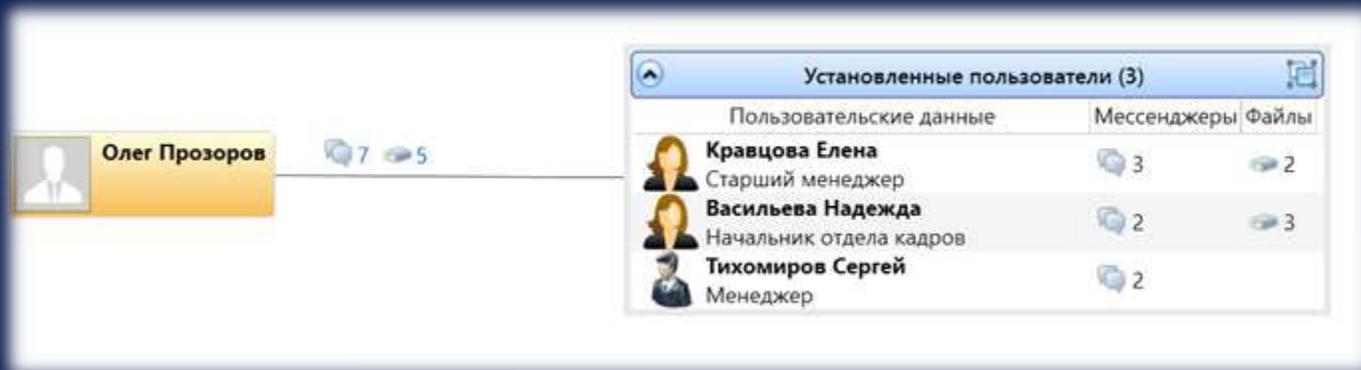
< Привязать

Отказать >

Добавить пользователя

Закрыть

# Граф-анализатор



The screenshot displays a user profile for **Олег Прозоров** with 7 outgoing and 5 incoming connections. A table titled "Установленные пользователи (3)" lists three users with their roles and connection counts.

Установленные пользователи (3)		
Пользовательские данные	Мессенджеры	Файлы
 <b>Кравцова Елена</b> Старший менеджер	3	2
 <b>Васильева Надежда</b> Начальник отдела кадров	2	3
 <b>Тихомиров Сергей</b> Менеджер	2	



# Граф-анализатор

The screenshot displays the Falcongaze SecureTower Client console interface. The main window is titled "Falcongaze SecureTower Client console" and shows a search results table on the left and a detailed chat view on the right.

**Search Results Table:**

Идентификатор	Локальный пользователь	Удаленный пользователь	Тип
1	Кравцова Елена	Олег Прозоров	Текстовый диалог
2	Кравцова Елена	Олег Прозоров	Текстовый диалог
3	Кравцова Елена	Олег Прозоров	Текстовый диалог

**Chat View Details:**

**Переконен:** 19.01.2020 (10:15:53 - 10:25:53) | С IP: 192.168.0.14 | Мессенджер

**Локальный пользователь:** Кравцова Елена | **Удаленный пользователь:** Олег Прозоров

**Информация о локальном пользователе:**  
Пользователи: lela\_kravc  
IP-адрес: 192.168.0.14

**Информация об удаленном пользователе:**  
Пользователи: oleg\_prozov

**Содержимое переписки (Сообщений: 2):**

- Кравцова Елена (19.01.2020 10:15:53)  
Имя файла: Описание проекта\_moa.docx | Размер: 22,7 КБ  
[Открыть в новой вкладке](#) | [Открыть во внешней программе](#)
- Кравцова Елена (19.01.2020 10:25:53)  
Имя файла: Customer Database\_ver1.xlsx | Размер: 21,7 КБ  
[Открыть в новой вкладке](#) | [Открыть во внешней программе](#)

# Перехват почты

The screenshot displays the Falcongaze SecureTower Client console interface. The left pane shows a tree view of security policies under 'Falcongaze SecureTower Security policies Group'. The right pane shows search results for a specific policy, '7. Утечка клиентской базы'.

Название	Подключки	Инцидентов	Уровень риска	Статус
Falcongaze SecureTower Security policies Group	978 / 967	75 316 / 73 1		
Samples	978 / 967	75 316 / 73 1		
Без	0 / 0	0 / 0		
Лин	978 / 967	75 316 / 73 1		
01. Контроль активности сотрудников	80 / 80	3 642 / 3 642		
02. Контроль поиска работы	131 / 131	11 297 / 11 2		
03. Контроль использования облачных хранилищ	0 / 0	0 / 0		
04. Контроль почты	409 / 400	35 154 / 35 1		
05. Распределение ресурсов компании	81 / 81	2 851 / 2 851		
06. Поиск паролей	0 / 0	0 / 0		
07. Нарушение законодательства РФ	133 / 132	10 943 / 10 9		
08. Утечка информации	12 / 6	1 656 / 456		
1. Контроль утечек конфиденциальных документов	0 / 0	0 / 0	Документы с грифами	
2. Контроль утечек служебных документов	0 / 0	0 / 0	Документы с грифами	
3. Контроль файлов с изменением разрешений	1 / 1	86 / 86		
4. Контроль зашифрованных файлов	5 / 5	370 / 370		
5. Контроль документов с печатками	0 / 0	0 / 0	Необходимо добавить	
6. Контроль утечки файлов XLS (xlsx, xls)	0 / 0	0 / 0		
7. Утечка клиентской базы	6 / 0	1 200 / 0		
09. Утечки ПДн (ФЗ №152)	0 / 0	0 / 0		
10. Утечки бухгалтерской и управленческой документов	152 / 148	9 673 / 9 146		
11. Повышение привилегий / запуск специализированных	0 / 0	0 / 0		

№	Состояние	Тип данных	Локальный пользователь	Удаленный пользователь	Перехвачено	Размер	Права
1	И	Файл Skype	Кравцова Елена	Олег Плосколов	19.01.2020 10:25:53	21,7 KB	7.1
2	И	Файл Telegram	Кравцова Елена	20986718	20.01.2020 14:55:00	21,7 KB	7.1
3	И	Файл с USB устройств	Тупомяров Сергей		20.01.2020 11:30:15	8,17 KB	7.1
4	И	FTP-файл	Тупомяров Сергей		20.01.2020 13:04:19	10,5 KB	7.1
5	И	FTP-файл	Кравцова Елена		21.01.2020 16:30:00	10,5 KB	7.1
6	И	Почтовые вложения	Кравцова Елена	oleg.ploskolov@gmail.com	20.01.2020 14:22:38	9,51 KB	7.1

Отправлено: 20.01.2020 14:22:38 С ID: 192.168.0.14 Протокол SMTP Размер: 9,51 KB

Локальный пользователь: Кравцова Елена Удаленный пользователь: oleg.ploskolov@gmail.com

Информация

Текущий документ может быть найден по следующему пути:

Активы -> Information.ua -> Customer Database.xlsx

Лист 1

Customer List
Software and Technology
SAP
Microsoft
BEA Systems
Oracle
ATG
Thomson Reuters
Sun Microsystems
Consona CRM
Intelliparc
LogicLibrary, Inc.
Minys
Datalex

# Поиск

**Поиск**

Все перечисленные слова:

Пользователи:

Интервал поиска:

**Область поиска**

**Общие параметры поиска**

**Дополнительные параметры поиска**

**Почта**

Отправитель:

Получатель: oleg\_prozorov@gmail.com

Прочие параметры в заголовке:

Вложения:

**Web**

**Мессенджеры**

**Файлы и т.**

Falcongaze SecureTower Client console

С чего начать | Политики безопасности | Активность пользователей | Поиск информации | Комбинированный поиск

Искать | Добавить в избранное | Показать избранное | Экспорт/Импорт

Интервал поиска: За последние 30 дней

Количество результатов: 500 результатов

Доступный интервал поиска: 19.01.2020 - 23.01.2020

Группы Active Directory

**Условия поиска**

Поиск по словарю

Словари: База клиентов (19)

Порог срабатывания: 3 из 19

Будут найдены документы, содержащие как минимум заданное количество слов или выражений из выбранного словаря. Обработка правила может занять продолжительное время.

С учетом морфологии

Выберите операцию, применяемую к условиям в блоке: И Или Не (отрицание)

Область поиска: Почта | Мессенджеры | Web | Прочее

- POP3
- SMTP
- IMAP
- MAPI
- Прочая почта
- Вложения
- Skype
- Telegram
- Viber
- WhatsApp
- Lync
- SIP
- XMPP (Jabber)
- ICQ (OSCAR)
- Mail.RU Agent
- Yahoo
- Hangouts
- Slack
- Discord
- Microsoft Teams
- Web-переписки
- Файлы
- Посещенные web-страницы
- Поисковые запросы
- Отправленные запросы
- Web-коммуникации
- Браузер-активность
- Файлы
- FTP
- Файлы с устройств
- Аудит устройств
- Сетевые ресурсы
- Облачные хранилища
- Снимки экрана
- Активность ПК
- Принтеры
- Буфер обмена
- Кейлоггер
- Совпадения по банкам файлов

Принятые файлы

Отправленные файлы

# Модуль расследований

192.168.206.128

Поиск информации | Комбинированный поиск | Расследования | Анализ рисков

## Утечка конфиденциальной информации

Дата инцидента: 01.02.2020

Дело: **Материалы расследования (10)** | Журнал событий

Информация об инциденте

Старший менеджер отдела продаж **Сергей Тихомиров** в беседе в мессенджере Skype с удаленным пользователем получил предложение о работе в компании-конкуренте на условии предоставлении базы данных клиентов компании **ООО "БизнесПро"**. На данное событие сработало правило безопасности "Поиск работы". Собеседник Тихомирова представился Олегом Прозоровым из компании HighTechSolutions (учетная запись Skype: oleg\_prozorov).

Вовлеченные лица (3)

[+](#) Добавить | [✎](#) Изменить | [✖](#) Удалить

ФИО	Организация	Подразделение	Должность	Роль в деле	Контактные данные	
<a href="#">Тихомиров Сергей</a>	БизнесПро	Отдел продаж	Менеджер	согласился передать конфиденциальные данные	+79631619878	<a href="#">⚙</a>
<a href="#">Кравцова Елена</a>	БизнесПро	Отдел продаж	Старший менеджер	передала конфиденциальные данные	+145665555	<a href="#">⚙</a>
<a href="#">Олег Прозоров</a>				Получатель конфиденциальной информации		<a href="#">⚙</a>

Мероприятия и их результаты

- Изучение переписки выявило возможность потенциальной передачи конфиденциальных данных конкурирующей компании.
- Были проведены мероприятия по установлению действий, вовлеченных в инцидент информационной безопасности лиц. Выявление, сбор и фиксацию доказательств по делу производились средствами DLP-системы SecureTower.
- В результате проведения мероприятий установлено, что в компании произошло несколько связанных инцидентов информационной безопасности.
- Представитель компании HighTechSolutions Олег Прозоров, контактировал посредством мессенджера Skype и электронной почты с менеджером отдела продаж Сергеем Тихомировым и его непосредственным руководителем Еленой Кравцовой по вопросам предоставления инсайдерской информации.

Выводы по результатам расследования

В результате проведенного расследования установлено, что:

- Старший менеджер отдела продаж Елена Кравцова передала представителям компании HighTechSolutions конфиденциальные данные компании БизнесПро (список клиентов и проектные документы);
- Менеджер отдела продаж Сергей Тихомиров согласился передать представителям компании HighTechSolutions конфиденциальные данные компании БизнесПро, произвел копирование файлов на USB-носитель (база клиентов), распечатал бизнес-план компании и последний финансовый отчет. Факт передачи данных третьим лицам не установлен.

Таким образом, факты неправомерного обращения с конфиденциальной информацией установлены.

# Модуль расследований

The screenshot displays the Falcongaze SecureTower Client console interface. The top navigation bar includes tabs for 'Политики безопасности', 'Активность пользователей', 'Олег Прозоров - (09.01.20 - 24.01.20)', 'Поиск информации', 'Комбинированный поиск', 'Расследования', and 'Анализ рисков'. The main content area is divided into two panels. The left panel, titled 'Список дел', shows a list of cases with columns for 'Название', 'Вовлеченные лица', and 'Дата инцидента'. The right panel, titled 'Утечка конфиденциальной информации', displays details for a specific incident on 01.02.2020. It lists several events with timestamps and details about the involved parties (Кравцова Елена and Олег Прозоров), local and remote addresses, and file names like 'Customer Database\_ver1.xlsx'.

Название	Вовлеченные лица	Дата инцидента
Утечка конфиденциальной информации	Пользователей: 3	01.02.2020
Нарушение трудового распорядка		

Дата и время	Локальный адрес	Удаленный адрес	Тема	Тип	Размер
19 января 2020 г. 10:25:53	192.168.0.14	oleg_prozorov	Customer Database_ver1.xlsx	Файл	21.7 KB
20 января 2020 г. 11:27:26	111.111.111.14	oleg_prozorov@gmail.com	entertainment	Почтовое сообщение (Протокол POP3)	3.88 KB
20 января 2020 г. 14:22:38	192.168.0.14	oleg_prozorov@gmail.com	документы	Почтовое сообщение (Протокол SMTP)	464 KB
20 января 2020 г. 14:22:38	192.168.0.14	oleg_prozorov@gmail.com	документы	Почтовое сообщение (Протокол SMTP)	9.51 KB
20 января 2020 г. 14:22:38	192.168.0.14	oleg_prozorov@gmail.com	документы	Почтовое сообщение (Протокол SMTP)	9.51 KB

**#CODEIB**

**СПАСИБО ЗА ВНИМАНИЕ**



**АЛЕКСАНДР КУЛИК**  
**a.kulik@falcongaze.ru**  
**+7(962)8568588**