

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

#CODEIB



КАК ЭФФЕКТИВНО НАСТРОИТЬ DLP, ЧТОБЫ НЕ УПУСТИТЬ УТЕЧКУ

Анастасия Завадская
Ведущий специалист

Наша компания с 2007 года занимается разработкой программного обеспечения в сфере информационной безопасности. Флагманский продукт компании — комплексное решение SecureTower, предназначенное для **предотвращения утечек информации и мониторинга деятельности сотрудников.**



**12
ЛЕТ**



**30
СТРАН**



**1000+
КЛИЕНТОВ**

Вопросы при выборе DLP

А НАДО ЛИ?



50%

уволенных
сотрудников забирают
корпоративные данные

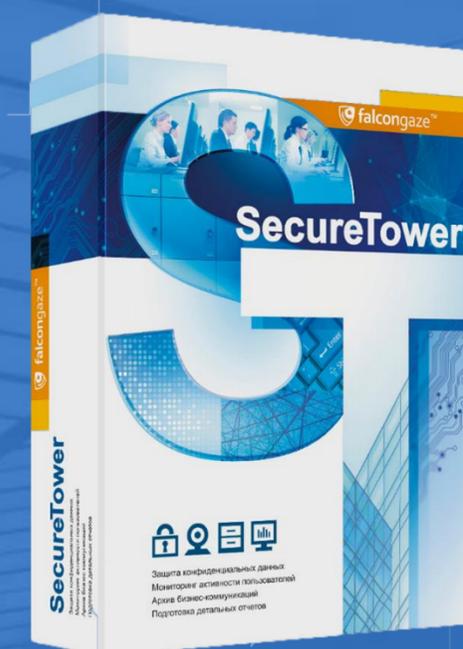
ТОП:

1 место - USB
2 место - Личная почта
3 место – Мессенджер

Немного статистики

Группа риска:

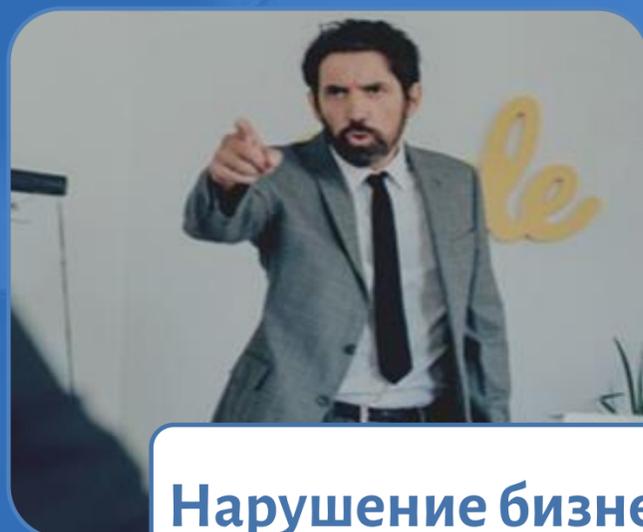
продажи, закупки,
юристы, маркетологи



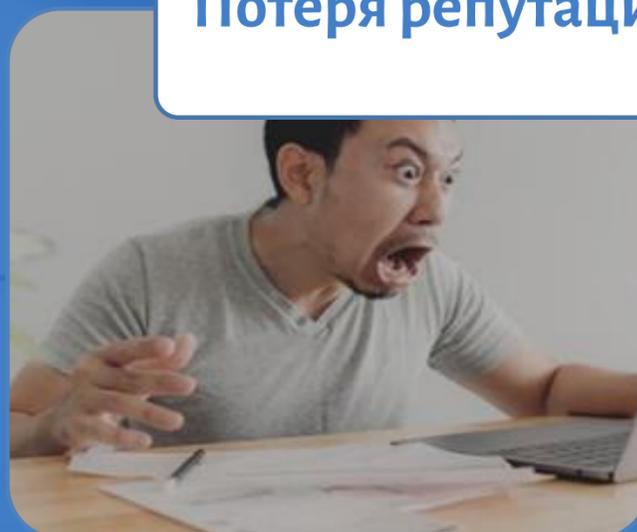
Вопросы при выборе DLP



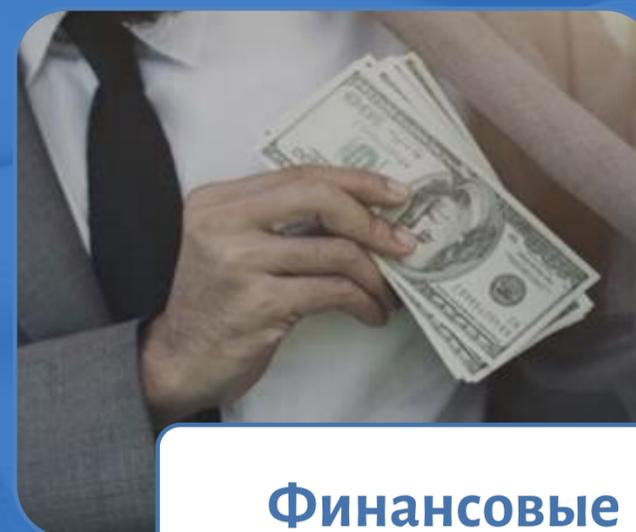
МОЖЕТ ЗАБЛОКИРОВАТЬ?



Нарушение бизнес-процессов



Потеря репутации



Финансовые потери



Мысли в голове не остановишь.

Если сотрудник понял, что ему заблокировали один канал связи, он пойдет искать другой

КАКИЕ ЗАДАЧИ МОЖЕТ РЕШИТЬ СИСТЕМА?

*контроль чертежей

*общение со СМИ

*Контроль файлов с измененным расширением

*передача данных об основной деятельности компании (планы, отчёты)

*контроль персональных данных

*информация о коммерческих предложениях

*выявление мошеннических схем

*перехват голосовых сообщений

* копирование данных на USB-устройства

*использование сотрудниками личной почты

*контроль использования USB

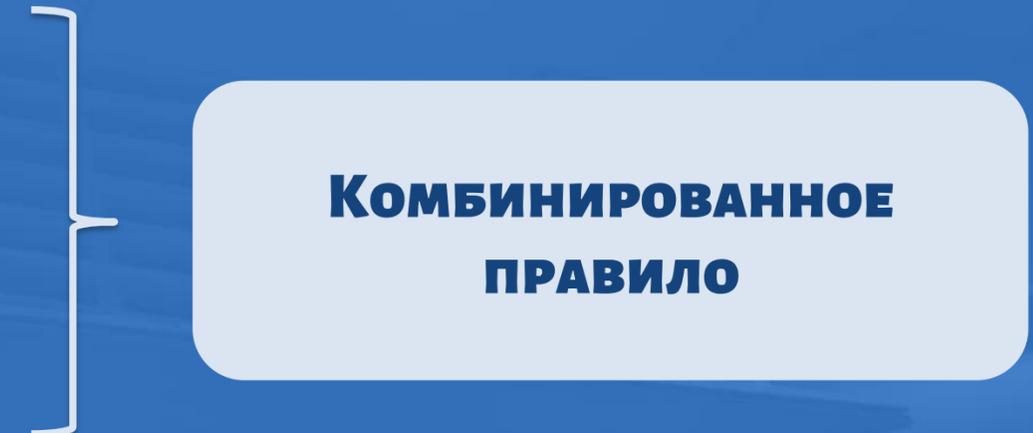
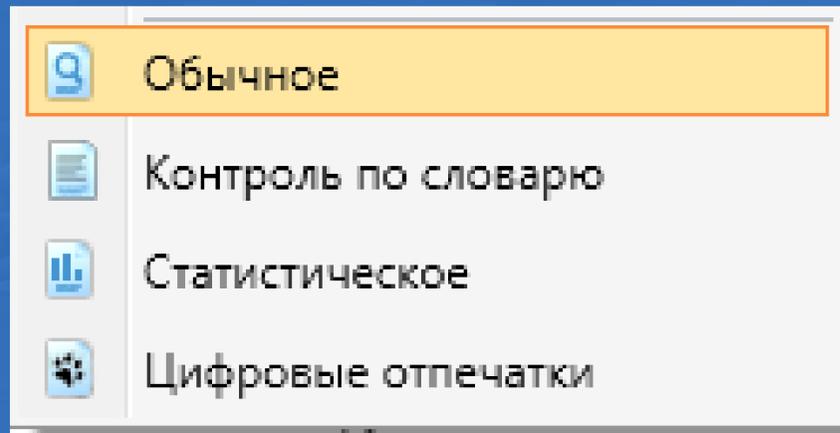
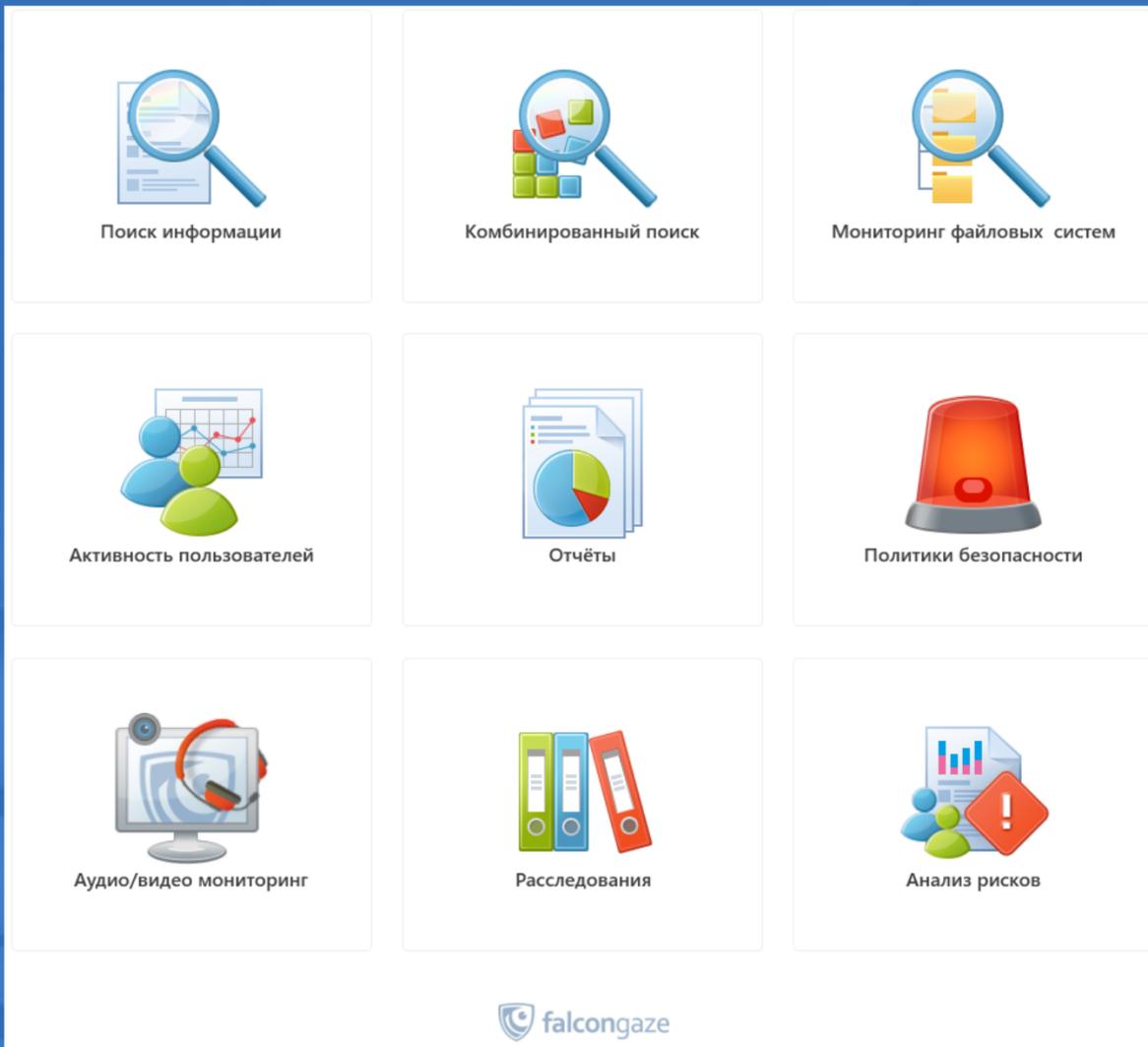
*контроль зашифрованных документов

*поиск работы, нецелевое использование рабочего времени

*распространение ложной информации

*Контроль всех подключаемых устройств





“ **Эффективное правило** - число ложных срабатываний стремится к 0

Отдел проектирования

Контроль файлов формата .DWG

18

Файл | Расширение файла | Равно | .dwg

И

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

Пользователь | Карточки | Локальный или удалённый | Не равно | Белкин Андрей

И

Пользователь | Карточки | Локальный или удалённый | Не равно | Ветров Федор

[\[Добавить условие\]](#) [\[Добавить блок\]](#) [\[Обрамить блоком\]](#)

СПЕЦИАЛИСТЫ

ЗАДАЧА

ПРАВИЛО

МОНИТОРИМ

ОПТИМИЗИРУЕМ

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

Файл | Расширение файла | Равно | .dwg

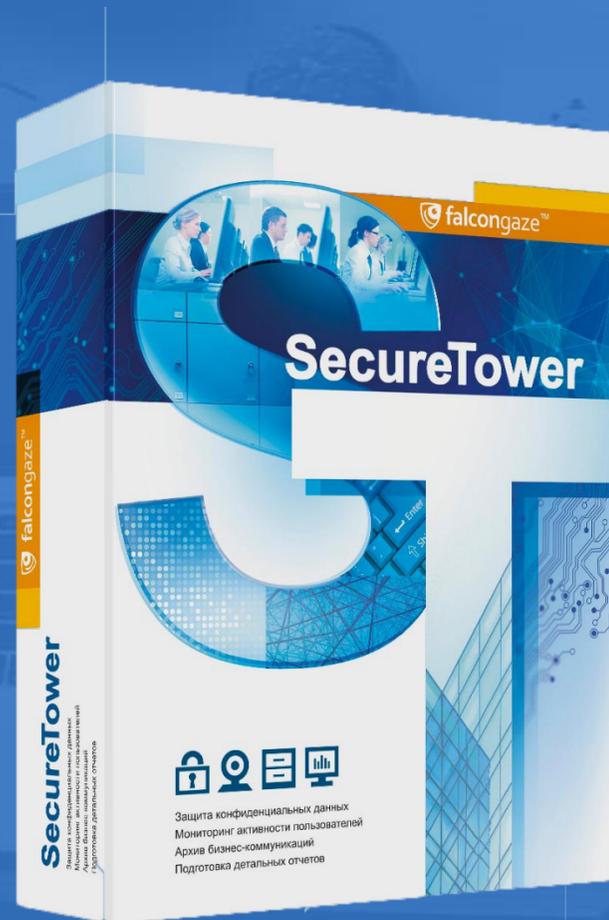
[\[Добавить условие\]](#) [\[Добавить блок\]](#) [\[Обрамить блоком\]](#)

188



КЕЙС #1





Добавление правила безопасности

Укажите список поисковых условий, при достижении которых будет формироваться уведомление

Параметры | Группы Active Directory | Настройки уведомления | Настройки скриптов | Уровень риска

Название правила: Новое правило безопасности

Описание:

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

Распознанное содержимое | Распознанные печати | Любая печать

[\[Добавить условие\]](#) [\[Добавить блок\]](#) [\[Обрамить блоком\]](#)

Печать 1

The stamp is circular with a blue border. The text inside the stamp reads: 'БАШКОРТОСТАН РЕСПУБЛИКАНЫ БЭРӘ КАДЫ. * "БУМТОРГ" * ОГРН 3060000090000 ИНН 025700000000 * ИМЕНИНВАРИАНТНЫЙ ПРЕДПРИНИМАТЕЛЬ ФАМИЛИИ ИМЯ ОТЧЕСТВО * БАШКОРТОСТАН РЕСПУБЛИКА БАШКОРТОСТАН ГОРОД БИРСК *'. The stamp is centered on a white background within a preview window.



Общество с ограниченной ответственностью

«Моя компания»

Директору ООО "Ромашка"
Сидорову Петру Валерьяновичу

КОММЕРЧЕСКОЕ ПРЕДЛОЖЕНИЕ

№ 1 от 29.07.2015

на поставку торгового оборудования

Общество с ограниченной ответственностью «Моя компания» направляет Вам на рассмотрение коммерческое предложение на оборудование, приведенное в таблице:

№	Наименование	Цена	Количество	Сумма
1	Витрина В-102Н	5 350,00	2	10 700,00
2	Стеллаж Чарли - 7	4 235,00	3	12 705,00
3	Кассовый аппарат Меркурий 115	3 400,00	1	3 400,00

Общая стоимость: 26 805* (двадцать и

*Предложение действительно до 28.08.2015

С уважением,
Генеральный директор



*Чем больше власть, тем больше
опасность злоупотребления ею*

Эдмунд Берк

И

Распознанное содержимое | **Распознанные печати** | БУМТОРГ | Менеджер печатей

Почта | Получатель | **Содержит** | @konkurent.ru

Локальный пользователь: ООО "Моя компания" - Удалённый пользователь: konkurent@mail.ru

Основные поля

Отправитель: <mycompany@gmail.com>
Получатель: <konkurent@mail.ru>
Тема: Коммерческое предложение

Дополнительные поля

Вложения (1)
Коммерческое предложение.docx
64,0 КБ

Добрый день!
Коммерческое предложение во вложении.

Текст письма | Коммерческое предложение.docx

Правило безопасности: Пересылка коммерческих предло
Локальный адрес: 192.168.59.31 (w7client)
Локальный: <mycompany@gmail.com>
Удалённый: <konkurent@mail.ru>
Тема: Коммерческое предложение
Тип: Почтовое сообщение (Протокол MAPI) Размер: 91,1 КБ

11:10:19 (1 ч назад)
ООО "Моя компания" - konkurent@mail.ru

Правило безопасности: Пересылка коммерческих предло
Локальный адрес: 192.168.59.31 (w7client)
Локальный: <mycompany@gmail.com>
Удалённый: <konkurent@mail.ru>
Тема: Коммерческое предложение
Тип: Почтовое сообщение (Протокол MAPI) Размер: 91,1 КБ

11:04:46 (1 ч назад)
ООО "Моя компания" - konkurent@mail.ru

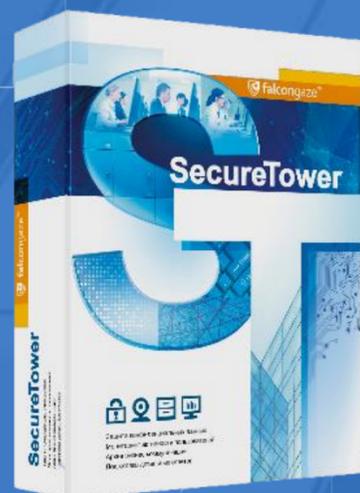
Правило безопасности: Пересылка коммерческих предло
Локальный адрес: 192.168.59.31 (w7client)
Локальный: <mycompany@gmail.com>
Удалённый: <konkurent@mail.ru>
Тема: Коммерческое предложение
Тип: Почтовое сообщение (Протокол MAPI) Размер: 91,1 КБ

11:03:30 (1 ч назад)
ООО "Моя компания" - konkurent@mail.ru

Правило безопасности: Пересылка коммерческих предло
Локальный адрес: 192.168.59.31 (w7client)
Локальный: <mycompany@gmail.com>
Удалённый: <konkurent@mail.ru>
Тема: Коммерческое предложение
Тип: Почтовое сообщение (Протокол MAPI) Размер: 91,1 КБ

11:02:10 (1 ч назад)
ООО "Моя компания" - konkurent@mail.ru

Правило безопасности: Пересылка коммерческих предло
Локальный адрес: 192.168.59.31 (w7client)





КЕЙС #2



Редактирование правила безопасности

Редактирование правила безопасности
Укажите список поисковых условий, при достижении которых будет формироваться уведомление

Параметры | Группы Active Directory | Настройки уведомления | Настройки скриптов

Название правила: Контроль лояльности, обсуждению руководителей

Описание: Негативные настроения в коллективе

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

Текст | Любое из перечисленных слов | надоел уволюсь ухожу жалеть невыносимо терпеть подсуетить кидать болтать "в шоке" "не по телефону" "не здесь" "не тут" "не в почте" "давай в скайп" "при встрече" "обсудим голосом" "не в скайп" "на телефон" "по мобиле" Иванов Смирнов "Иван Васильевич"

И

Область поиска | Почта | Мессенджеры | Web | Прочее

[\[Добавить условие\]](#) [\[Добавить блок\]](#) [\[Обрамить блоком\]](#)

Включить правило безопасности
 Применить данное правило ко всем проиндексированным данным (это может занять много времени)

OK Отмена



Упс, а я не
знал!

Falcongaze SecureTower Client console

С чего начать × Активность пользователей × Результаты поиска (2) × Политики безопасности × Комбинированный поиск ×

Просмотр уведомлений + Добавить Изменить Удалить Настройки

Операции над списком Фильтр: ? (43) ✓ [красный] [желтый] [серый]

Введите текст для фильтрации результатов

Результаты поиска

Тема: Кравцова Елена резюме
Тип: Почтовое сообщение (Протокол SMTP) Размер: 93,6 КБ

Название	Подпись	Инцидентов
Falcongaze SecureTower Security policies Group		204 / 162
Samples		204 / 162
En		0 / 0
Rus		204 / 162
01. Контроль лояльности сотрудников		48 / 23
1. Обсуждение компании		8 / 0
2. Негативные настроения в коллективе		24 / 22
3. Переписки, вызывающие подозрение		3 / 0
4. Обсуждение руководителей		13 / 1
02. Контроль поиска работы		43 / 39
1. Поиск новой работы		43 / 39
03. Контроль использования облачных хранилищ		21 / 16
1. Поиск паролей к Dropbox		0 / 0
2. Поиск паролей к десктоп-приложениям облач		0 / 0
2. Рассылка резюме		21 / 16
04. Контроль почты		0 / 0
1. Контроль спам-рассылки		0 / 0
2. Контроль исходящей почты на внешние почто		0 / 0
3. Поиск паролей к внешним почтовым ящикам		0 / 0
4. Контроль блокировки почтовых сообщений		0 / 0
05. Расходование ресурсов компании		85 / 81
1. Бездействие пользователя более 3 часов в ден		1 / 0
2. Посещение социальных сетей		80 / 77

38 14 мая 2019 г. 15:25:26 87 [красный] [серый] [красный] [серый]

Кравцова Елена – contact@govjob.ru

Правило безопасности: 1. Поиск новой работы ?

Локальный адрес: 192.168.0.14

Локальный: Елена Кравцова <lena_kravz@gmail.com>

Удалённый: contact@govjob.ru

Тема: Кравцова Елена резюме

Тип: Почтовое сообщение (Протокол SMTP) Размер: 93,6 КБ

39 14 мая 2019 г. 15:25:26 87 [красный] [серый] [красный] [серый]

Кравцова Елена – resume@vakansii.ru

Правило безопасности: 1. Поиск новой работы ?

Локальный адрес: 192.168.0.14

Локальный: Елена Кравцова <lena_kravz@gmail.com>

Удалённый: resume@vakansii.ru

Тема: Кравцова Елена резюме

Тип: Почтовое сообщение (Протокол SMTP) Размер: 93,6 КБ

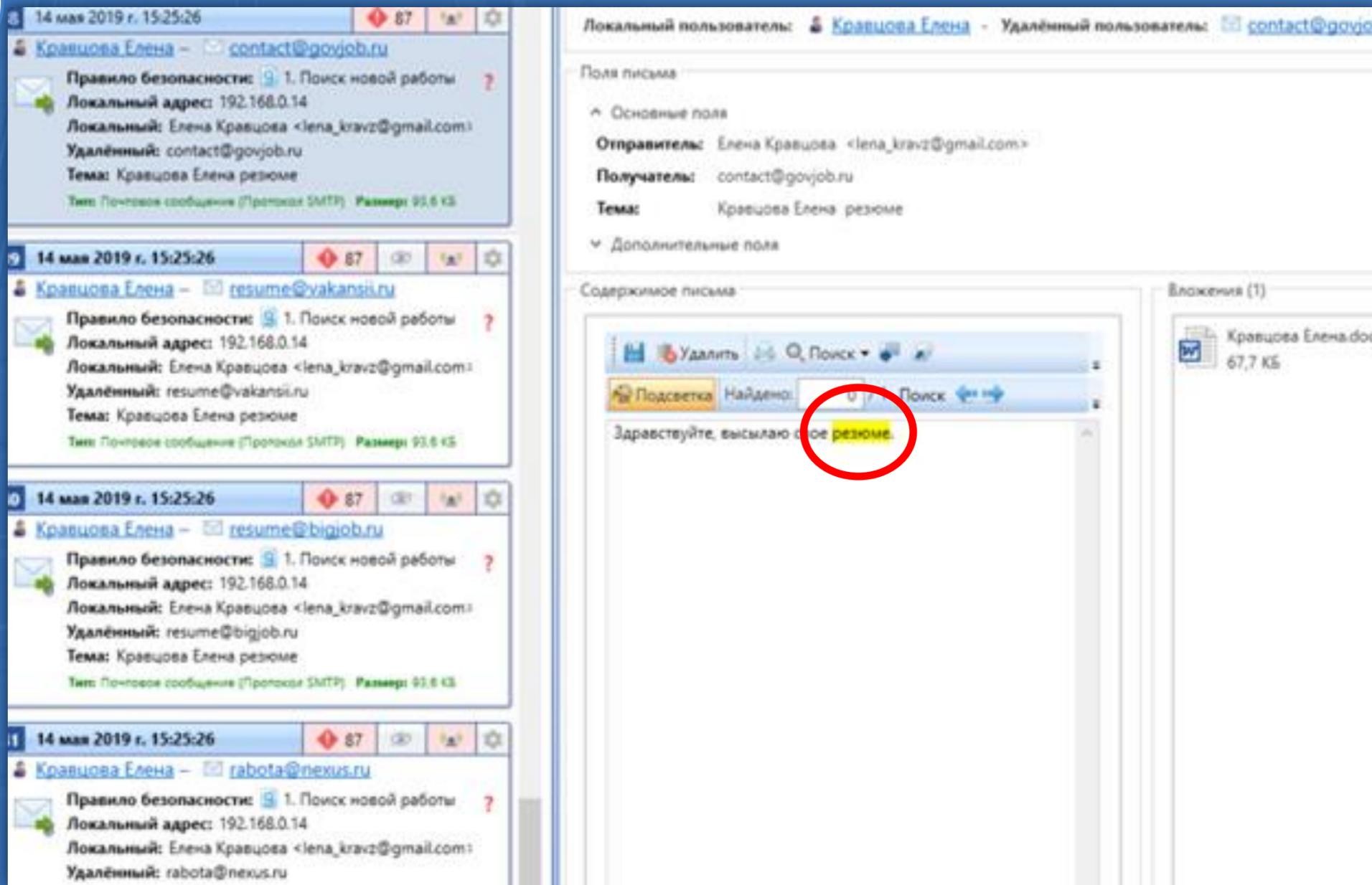
40 14 мая 2019 г. 15:25:26 87 [красный] [серый] [красный] [серый]

Кравцова Елена – resume@bigjob.ru

Правило безопасности: 1. Поиск новой работы ?



Написал резюме и
расплакался...
Я такой классный..



Интервал поиска
 За все время
 Доступный интервал поиска: 12.05.2019 - 16.05.2019

Количество результатов
 500 результатов

Группы Active Directory

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

Пользователь: Кравцова Елена

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 Агент
- Yahoo
- Hangouts
- Slack
- Web-переписки
- Файлы
- Посещённые 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 фай

2 14 мая 2019 г. 16:28:19 - 16:30:25

Кравцова Елена

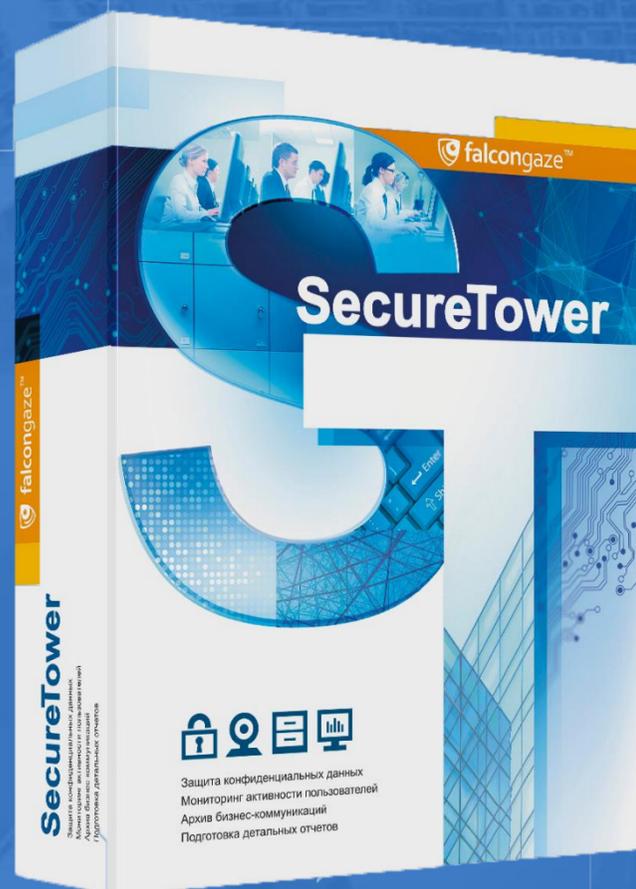
Локальный адрес: 192.168.0.14
 Количество файлов: 2
 Тип: Аудит файлов с USB устройств

Дайлинг	Номер заявки	ФИО	День рождения	Телефоны	Ссылка	Лимит	Регион	Карта
http://dialing3.bin.bank/	6965008	ОНИДОВНА	1986 7923		http://app.binbank.ru/g/8nrNUUUn	94416	Новосибирская обл.	MasterCard Standart
http://dialing3.bin.bank/	6965009	ОВНА	1963 7913		http://app.binbank.ru/g/2kbnkqCE	33319	Новосибирская обл.	MasterCard Standart
http://dialing3.bin.bank/	6965010	ДИМИРОВНА	1984 7903		http://app.binbank.ru/g/9HtTTaya	164441	Кемеровская обл.	MasterCard Standart
http://dialing3.bin.bank/	6965011	АНДРОВНА	1973 7913		http://app.binbank.ru/g/2kbnkWEk	200000	Новосибирская обл.	MasterCard Standart
http://dialing3.bin.bank/	6965012	АДИМИРОВНА	1978 7902		http://app.binbank.ru/g/7apAAWEA	190532	Челябинская обл.	MasterCard Standart
http://dialing3.bin.bank/	6965013	ЛЕНТИНОВНА	1973 7905		http://app.binbank.ru/g/7apAAPAU	106113	Кемеровская обл.	MasterCard Standart
http://dialing3.bin.bank/	6965014	ЛАДИМИРОВ	1964 7913		http://app.binbank.ru/g/4uzMuTnu	180000	Новосибирская обл.	MasterCard Standart
http://dialing3.bin.bank/	6965015	ЛЬЕВНА	1960 7917		http://app.binbank.ru/g/4uzMuxnn	50000	Волгоградская обл.	MasterCard Standart
http://dialing3.bin.bank/	6965016	СОВНА	1953 7913		http://app.binbank.ru/g/2kbnkEqb	50000	Новосибирская обл.	MasterCard Standart
http://dialing3.bin.bank/	6965017	ЛАДИЛЕНОВНА	1958 7912		http://app.binbank.ru/g/8nrNnnZR	50000	Свердловская обл.	MasterCard Standart
http://dialing3.bin.bank/	6965018	ЛЕРЬЕВИЧ	1951 7921		http://app.binbank.ru/g/1KwzbzK	50000	г. Санкт-Петербург и /	MasterCard Standart
http://dialing3.bin.bank/	6965019	ИКТОРОВИЧ	1984 7908		http://app.binbank.ru/g/7apAapUW	30000	Кемеровская обл.	MasterCard Standart
http://dialing3.bin.bank/	6965020	ЗЕЛ ВЛАДИМИ	1956 7950		http://app.binbank.ru/g/2kbnEwmp	50000	Кемеровская обл.	MasterCard Standart
http://dialing3.bin.bank/	6965021	КСАНДРОВИЧ	1970 7914		http://app.binbank.ru/g/9HtTHNTy	200000	Иркутская обл.	MasterCard Standart
http://dialing3.bin.bank/	6965022	Л АЛЕКСАНДР	1990 7913		http://app.binbank.ru/g/5cezcdze	200000	Новосибирская обл.	MasterCard Standart
http://dialing3.bin.bank/	6965023	ТОРОВИЧ	1974 7962		http://app.binbank.ru/g/2kbnEcbz	160000	Омская обл.	MasterCard Standart



КЕЙС #3





Искать ▾ | Добавить в избранное | Показать избранное | Экспорт\Импорт ▾

Интервал поиска **Количество результатов**

За все время ▾ 500 результатов ▾

i Доступный интервал поиска: 12.05.2019 - 16.05.2019

▾ **Группы Active Directory**

Условия поиска

Поиск по словарю

Словарь: Список сотрудников компании (25) ▾ Менеджер словарей

Порог срабатывания: 4 ↕ из 25

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

С учетом морфологии



Операции над списком ▾ Фильтр: [Почта] [Мессенджеры (1)] [Web] [Прочее (1)] [Режим просмотра ▾] [Сортировка ▾]

Введите текст для фильтрации результатов

результаты поиска

1 14 мая 2019 г. 16:28:19

Андреева Татьяна

Локальный адрес: 192.168.0.14
 Имя переданного файла: E:\work\Сотрудники.docx
 Тип USB устройства: Silicon-Power16G
 Идентификатор продукта (ProductID): 4096
 Идентификатор производителя (VendorID): 2316
 Тип: Файл с USB устройства Размер: 14,0 КБ

1 16 мая 2019 г. 17:27:08

Андреева Татьяна – Бурковский Георгий

Локальный адрес: 192.168.0.22
 Локальный: juliesweet
 Удалённый: g_burkov
 Имя переданного файла: pics.jpeg
 Направление: Отправлено
 Тип: Файл Skype Размер: 11,8 КБ

Сохранить Удалить Распечатать Поиск Открыть во внешней программе Добавить в дело

Отправлено: 16.05.2019 17:27:08 С IP: 192.168.0.22 Мессенджеры Размер: 11,8 КБ

Информация о пользователях

Локальный пользователь: **Андреева Татьяна** - Удалённый пользователь: **Бурковский Георгий**

Информация

Имя переданного файла: pics.jpeg
 Направление: Отправлено

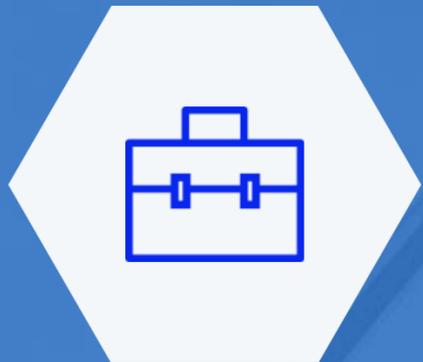
Путь вложенности документа

Текущий документ может быть найден по следующему пути:
 Чат juliesweet - g_burkov -> pics.jpeg

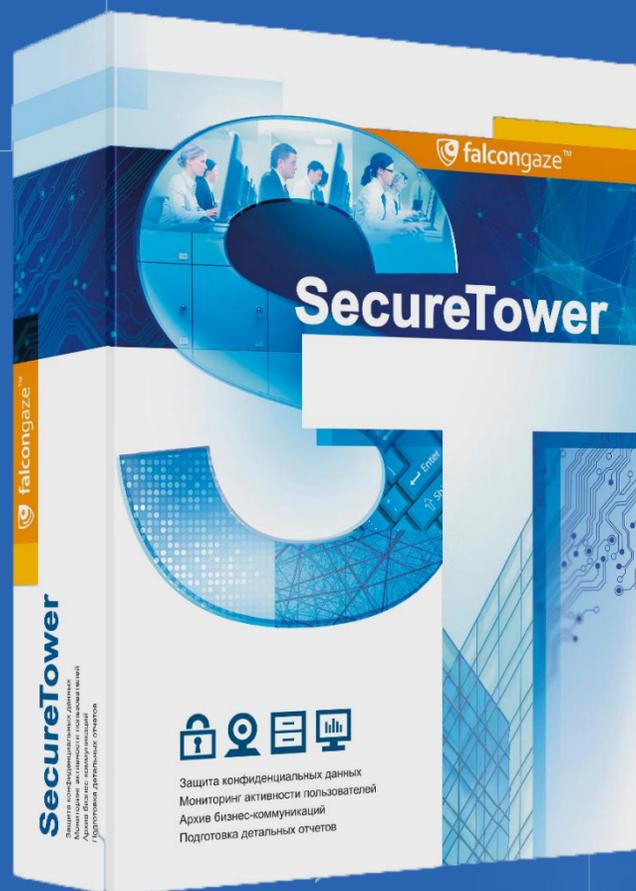
Подсветка Найдено: 0/12

Сведения по заработной плате сотрудников отдела продаж, август 2012 года.

1. Семён Васнецов - 60000
2. Игорь Новиков - 70000
3. Андрей Чёрный - 75000
4. Владимир Голубев - 70000
5. Игорь Андрущенко - 65000
6. Иван Синявко - 55000
7. Семён Серичев - 60000
8. Авдеев Василий - 75000
9. Ольга Примачек - 80000
10. Антон Демко - 70000
11. Светлана Полякова - 65000
12. Егор Шинкерев - 70000



КЕЙС #4



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

Интервал поиска

За все время

Количество результатов

5000 результатов

Доступный интервал поиска: 12.05.2019 - 16.05.2019

Группы Active Directory

Условия поиска

Поиск по цифровым отпечаткам

Банк данных:

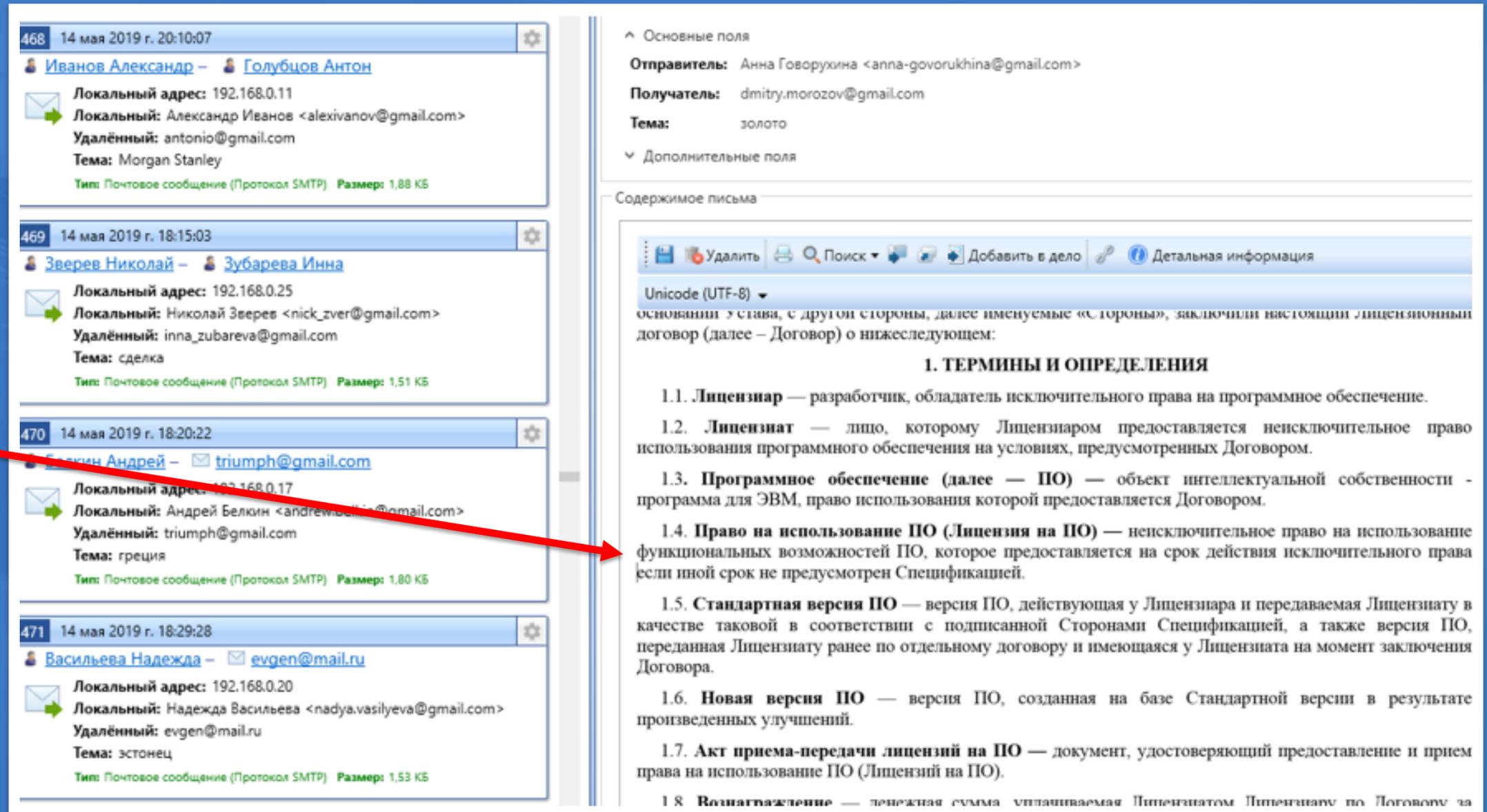
Банк цифровых отпечатков(Контракты)

Менеджер цифровых отпечатков

Порог срабатывания:

50%

**СОВПАДЕНИЕ ПО ТЕКСТУ
НА 50% И БОЛЕЕ**



The screenshot shows an email client interface with a list of four emails on the left and the content of the selected email on the right.

Left Panel (Email List):

- 468** 14 мая 2019 г. 20:10:07
Иванов Александр – Голубцов Антон
Локальный адрес: 192.168.0.11
Локальный: Александр Иванов <alexivanov@gmail.com>
Удалённый: antonio@gmail.com
Тема: Morgan Stanley
Тип: Почтовое сообщение (Протокол SMTP) Размер: 1,88 КБ
- 469** 14 мая 2019 г. 18:15:03
Зверев Николай – Зубарева Инна
Локальный адрес: 192.168.0.25
Локальный: Николай Зверев <nick_zver@gmail.com>
Удалённый: inna_zubareva@gmail.com
Тема: сделка
Тип: Почтовое сообщение (Протокол SMTP) Размер: 1,51 КБ
- 470** 14 мая 2019 г. 18:20:22
Белкин Андрей – triumph@gmail.com
Локальный адрес: 192.168.0.17
Локальный: Андрей Белкин <andrewbelkin@gmail.com>
Удалённый: triumph@gmail.com
Тема: греция
Тип: Почтовое сообщение (Протокол SMTP) Размер: 1,80 КБ
- 471** 14 мая 2019 г. 18:29:28
Васильева Надежда – evgen@mail.ru
Локальный адрес: 192.168.0.20
Локальный: Надежда Васильева <nadya.vasilyeva@gmail.com>
Удалённый: evgen@mail.ru
Тема: эстонец
Тип: Почтовое сообщение (Протокол SMTP) Размер: 1,53 КБ

Right Panel (Email Content):

Основные поля

Отправитель: Анна Говорухина <anna-govorukhina@gmail.com>
Получатель: dmitry.morozov@gmail.com
Тема: золото

Дополнительные поля

Содержимое письма

Unicode (UTF-8) ▼
основании 3-й статьи, с другой стороны, далее именуемые «Стороны», заключили настоящий лицензионный договор (далее – Договор) о нижеследующем:

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

- 1.1. Лицензиар** — разработчик, обладатель исключительного права на программное обеспечение.
- 1.2. Лицензиат** — лицо, которому Лицензиаром предоставляется неисключительное право использования программного обеспечения на условиях, предусмотренных Договором.
- 1.3. Программное обеспечение (далее — ПО)** — объект интеллектуальной собственности - программа для ЭВМ, право использования которой предоставляется Договором.
- 1.4. Право на использование ПО (Лицензия на ПО)** — неисключительное право на использование функциональных возможностей ПО, которое предоставляется на срок действия исключительного права (если иной срок не предусмотрен Спецификацией).
- 1.5. Стандартная версия ПО** — версия ПО, действующая у Лицензиара и передаваемая Лицензиату в качестве таковой в соответствии с подписанной Сторонами Спецификацией, а также версия ПО, переданная Лицензиату ранее по отдельному договору и имеющаяся у Лицензиата на момент заключения Договора.
- 1.6. Новая версия ПО** — версия ПО, созданная на базе Стандартной версии в результате произведенных улучшений.
- 1.7. Акт приема-передачи лицензий на ПО** — документ, удостоверяющий предоставление и прием права на использование ПО (Лицензий на ПО).
- 1.8. Вознаграждение** — денежная сумма, уплачиваемая Лицензиатом Лицензиару по Договору за

Быстрота
развертывания
системы

Система
«2-в-1»

Широкий спектр
контролируемых
каналов

Простота и удобство в
использовании

Системные
требования



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

#CODEIB



**ЛЮБОЕ ДОСТИЖЕНИЕ
НАЧИНАЕТСЯ С
РЕШЕНИЯ
ПОПРОБОВАТЬ**