Программа вебинара

- На мировом рынке DLP набирает обороты тенденция People Centric Security (PCS) или «человек в центре внимания». Потому что причиной любой угрозы является, в конечном счёте, человек.
- Но как контролировать множество людей, тем или иным образом входящих в сферу интересов любого бизнеса? Для контроля всех и вся не хватит никаких ресурсов. Каким образом в Solar Dozor удалось разрешить это противоречие?

- На вебинаре на конкретных примерах мы рассмотрим некоторые практические аспекты профилирования и проведения расследований:
  - - что такое группы риска и какие они бывают;
  - - как их своевременно выявлять;
  - - особенности мониторинга групп риска;
  - - как группы риска помогают прогнозировать нарушения (работа на опережение);
  - - как группы риска помогают выявлять признаки экономического мошенничества.

Ведущие вебинара:

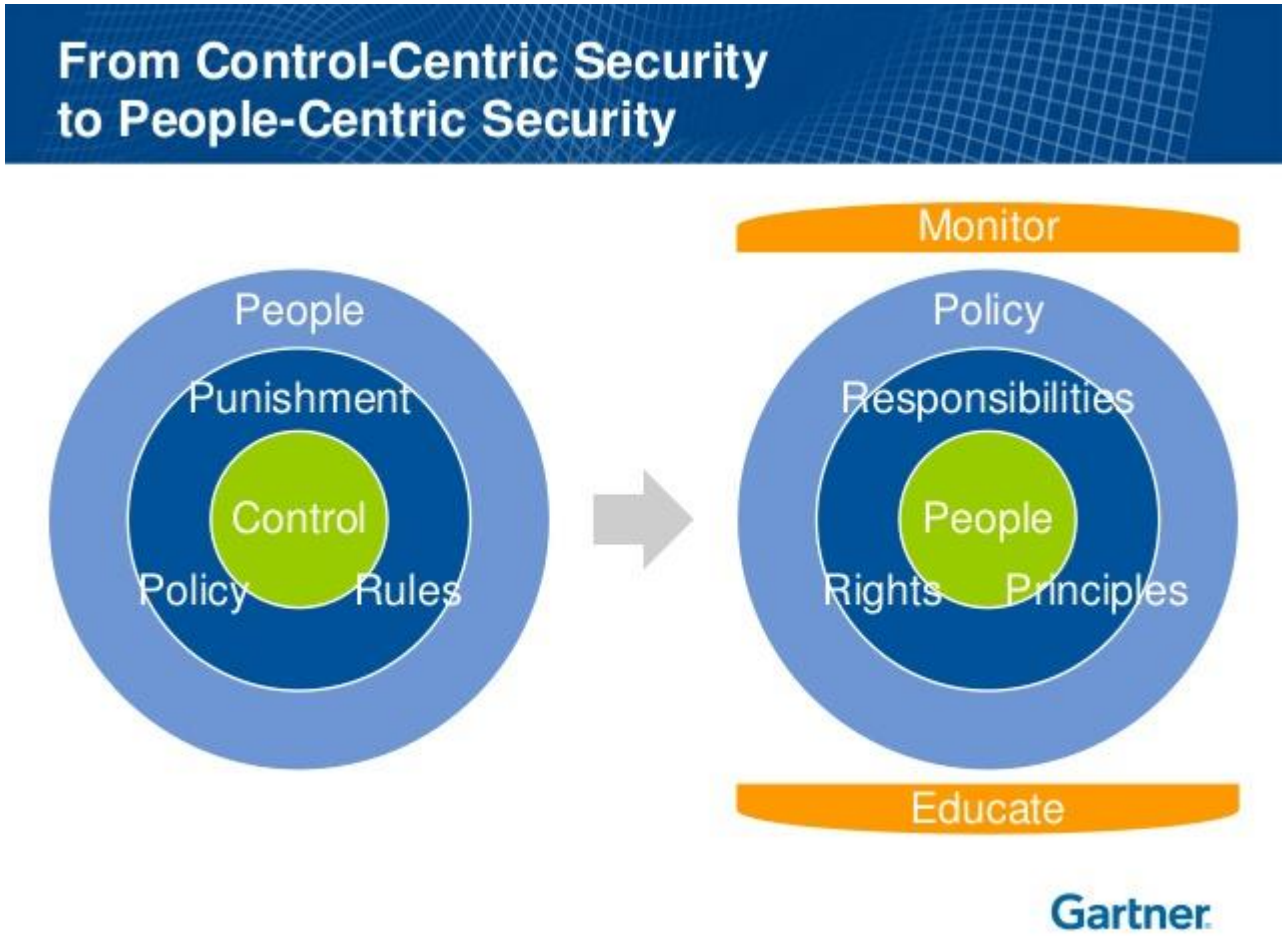
Смирнов Эликс,
кейс-аналитик компании Solar Security

Гавриш Злата,
аналитик внедрения компании Solar Security

«People centric security» в DLP – маркетинговая фича или объективная необходимость?

8 ноября 2017 г.

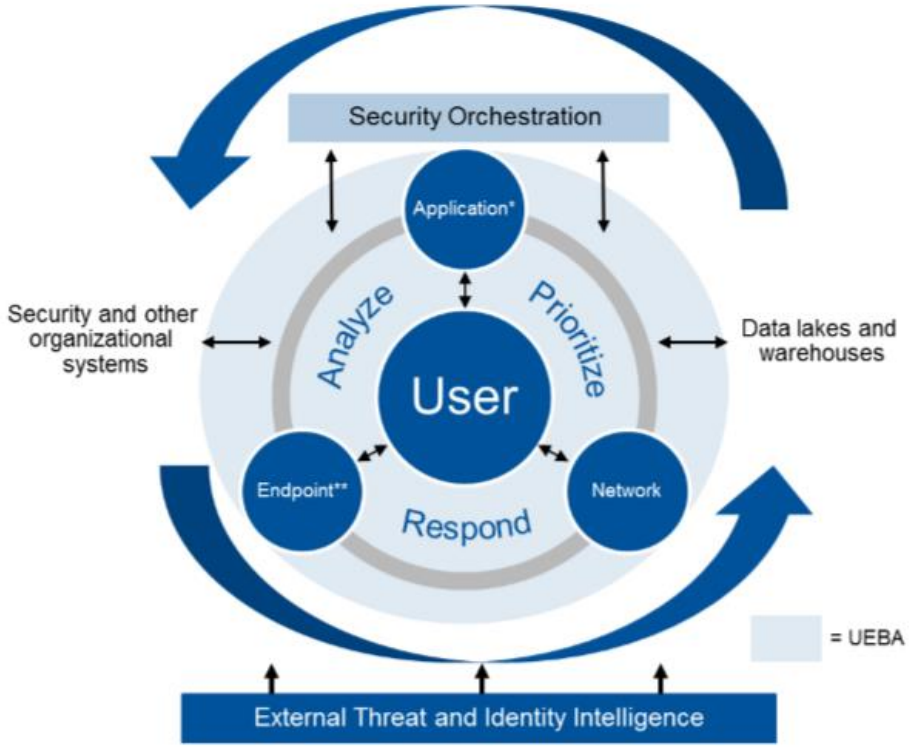
Модель People-Centric Security



Принципы PCS

- ✓Общность
- ✓Автономность
- ✓Подотчетность
- ✓Ответственность
- ✓Незамедлительность
- ✓Пропорциональность
- ✓Прозрачность

Значение мониторинга и аналитики



- ✓ Мониторинг пользователей как ключевой элемент People-Centric Security
- ✓ Аналитика поведения пользователей и сущностей (UEBA) становится ключевой функцией безопасности
- ✓ Потенциальный источник ценной информации для цифровых гуманитарных инициатив

Solar JSOC Security flash report (первое полугодие 2017)

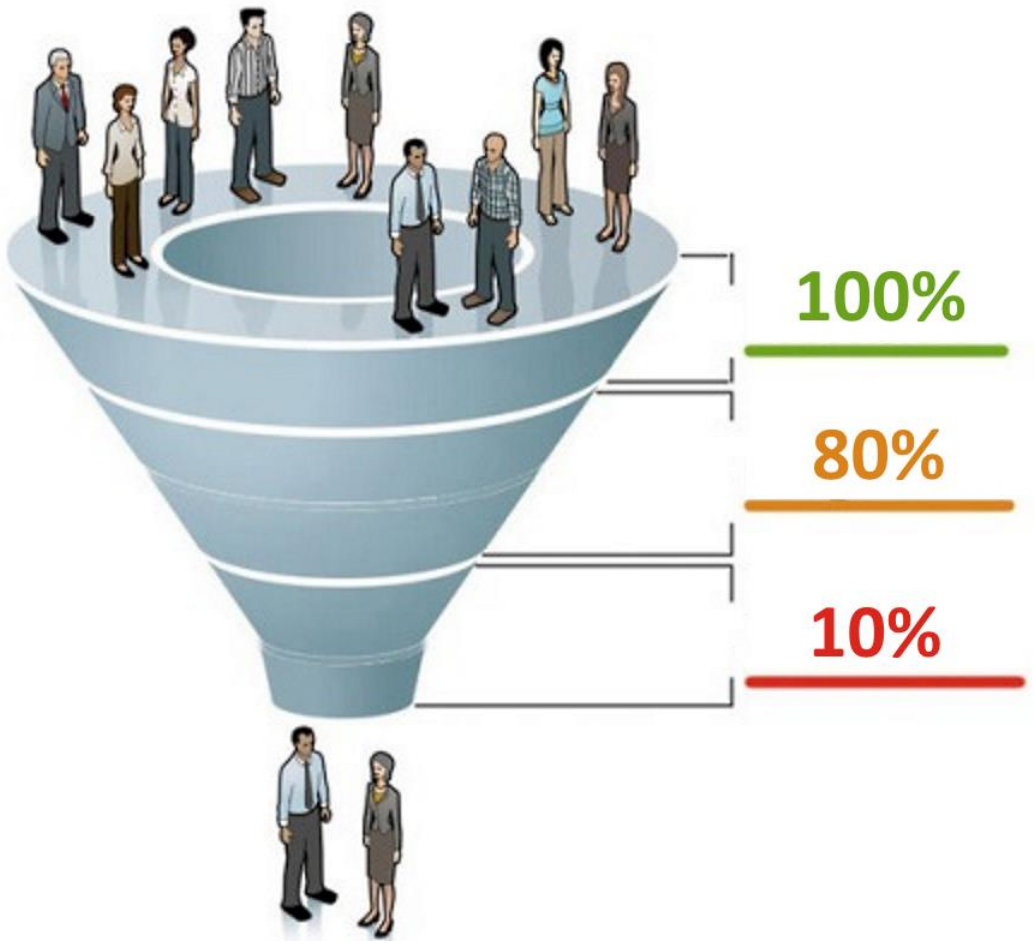
Распределение по каналам утечек

Инициаторы внутренних инцидентов

Нужно ли обучение?

Причина **80% утечек** из корпоративной компьютерной сети **- ошибки и халатность персонала**

«Воронка» профилактики



10% не нарушают никогда

80% нарушают в зависимости от обстоятельств

10% нарушают всегда

Цели профилактики

- выявление причин систематических нарушений
- своевременное выявление групп риска
- контроль изменения значимых обстоятельств

Рейтинг рисковых подразделений

Профиль мошенничества служб персонала

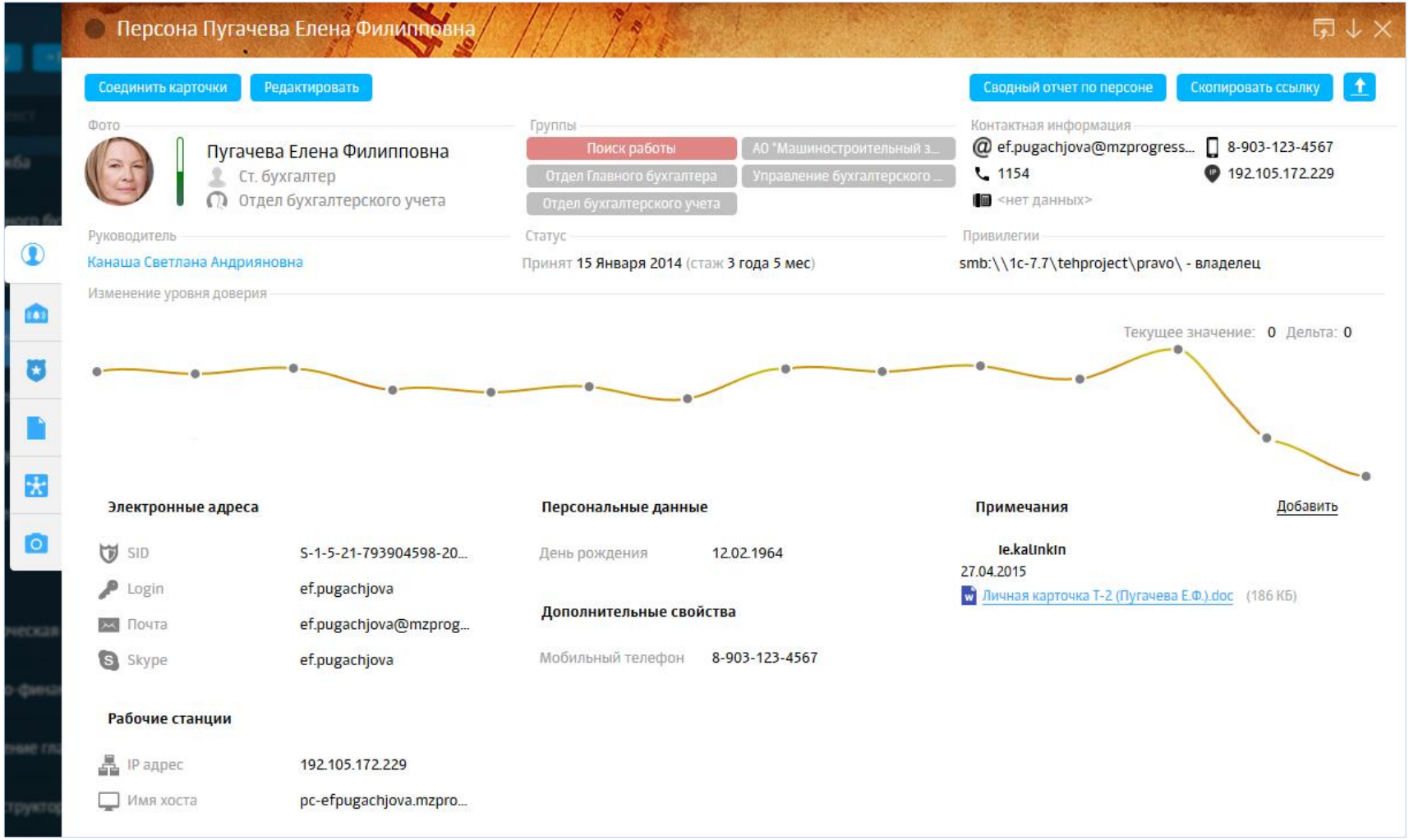
- ✓ Аффилированные (взаимозависимые) рекрутинговые агентства, СМИ, сайты
- ✓ «Продажа» персонала (ПДн сотрудников)
  - Для оформления фиктивных кредитов
  - Конкурентам
  - Хендхантерам
- ✓ Закупка тестов (методик тестирования, профилирования), обучения и методик обучения, курсов
- ✓ Закупка оборудования для собеседований
- ✓ Незаконные платные услуги
- ✓ «Мертвые души»
- ✓ Лоббирование "своих" специалистов и управленцев
- ✓ …

Поведенческие «красные» флажки

Некоторые группы риска

- **«Экстремисты»**
- **Деструктивные религии**
- **Несоответствие доходов и расходов**
- **Должники**
- **Игроманы, картежники**
- **Поиск работы (на увольнение)**
- **Аффилированность, конфликт интересов**
- **Хобби**
- **и т.д.**

Уровень доверия – инструмент выявления аномального поведения персоны



Что можно узнать из карточки персоны?

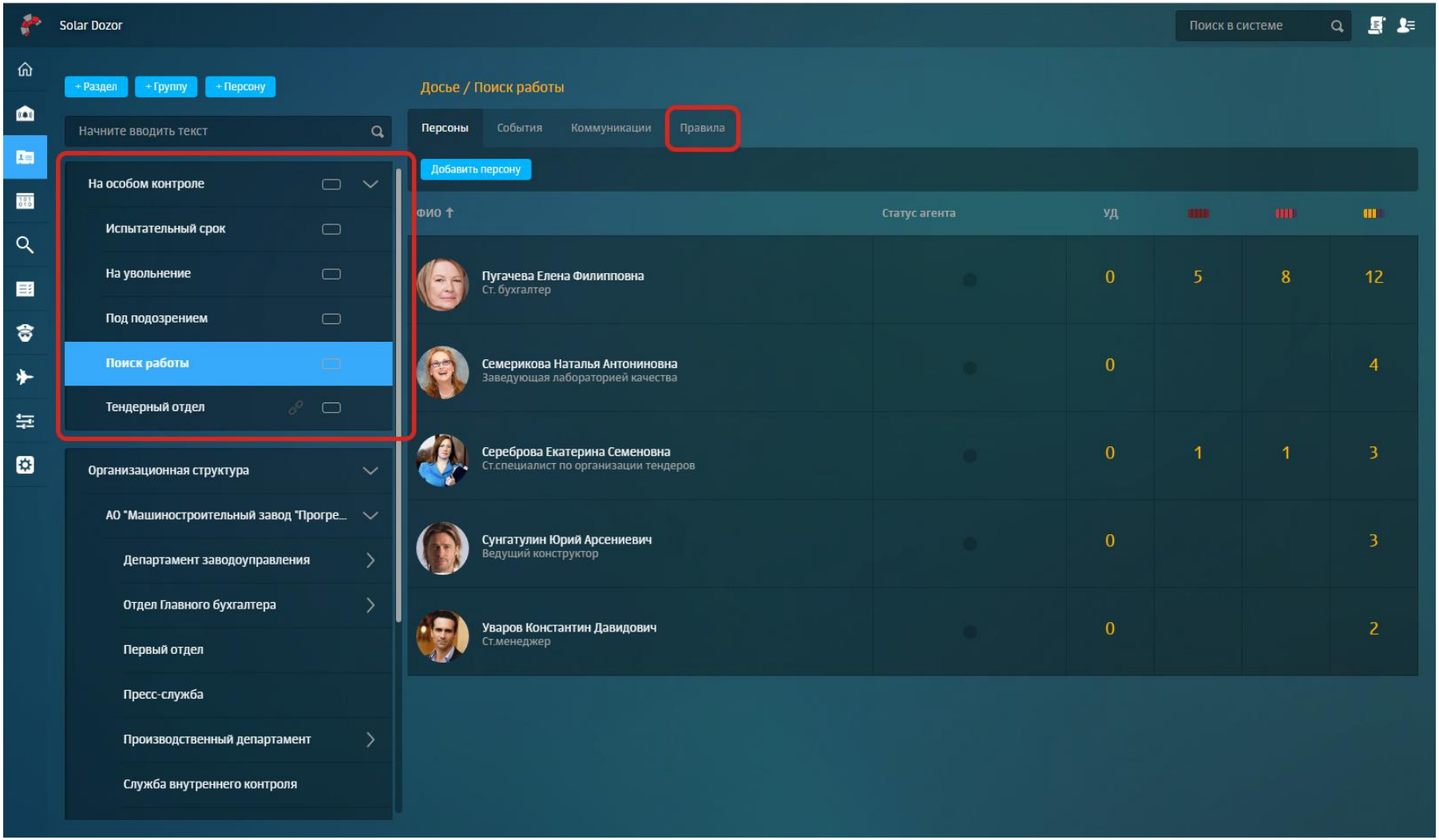
- ✓ Должности особого риска (топ-менеджмент, закупки, продажи, кадры, бухгалтерия, секретари и т.п.)
- ✓ Возраст сотрудников (профиль действий)
- ✓ Стаж работы (профиль действий)
- ✓ **Дни рождения**
- ✓ Возможные связи (родственные, этнические)

Мониторинг событий на PCA

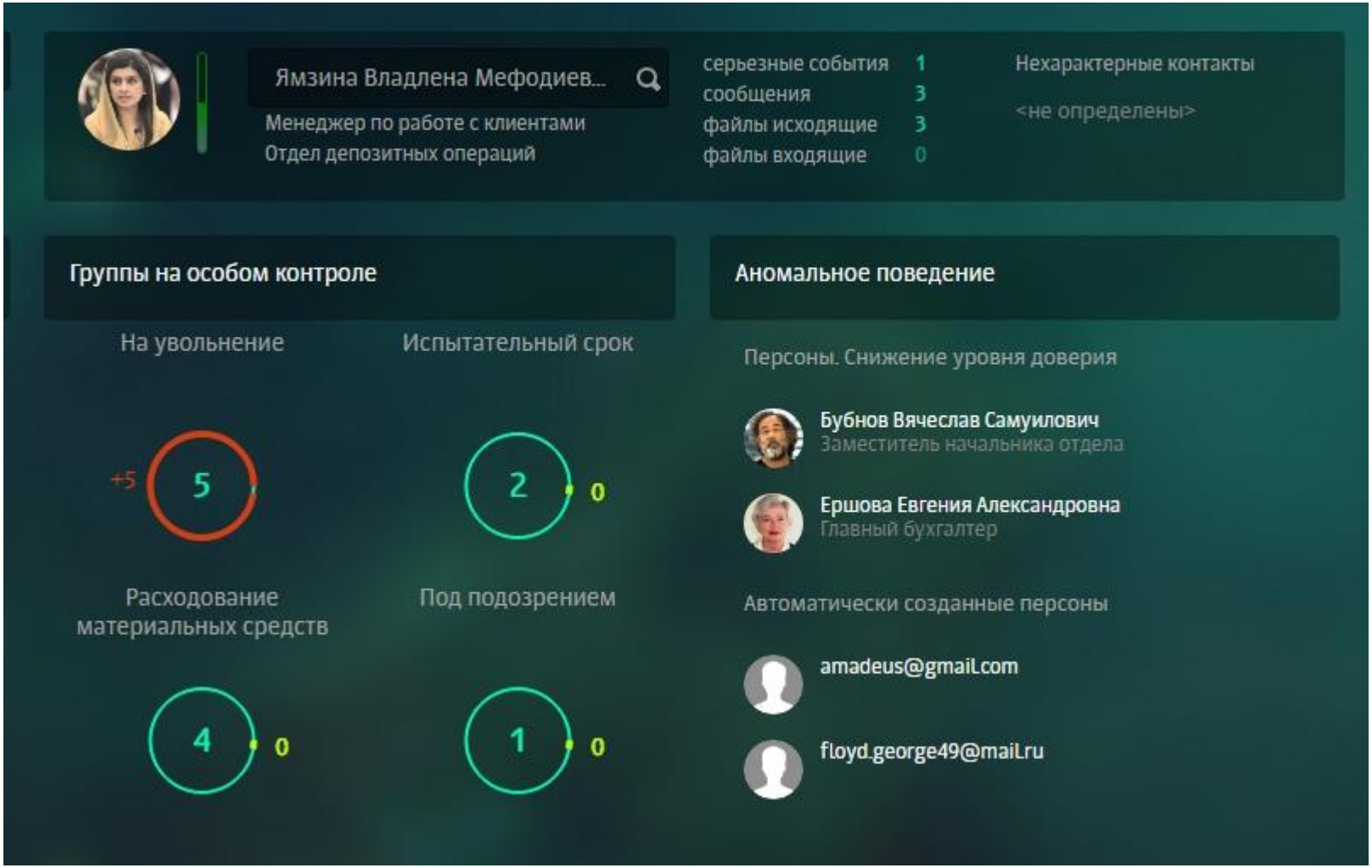
Алгоритм автоматической обработки действий персоны (при поиске работы)

- ✓ Пересылка резюме (переход в активную фазу поиска):
  - на джоб-ресурсы
  - конкурентам
  - бывшим сотрудникам
- ✓ Анализ пересылки правилами политики (пересылка ИО «Резюме»)
- ✓ Добавление в ГрОК «Поиск работы»
- ✓ Создание событий:
  - по пересылке резюме (по количеству пересылок)
  - добавления в ГрОК «Поиск работы» (по первой пересылке резюме)
- ✓ Уведомление офицера ИБ (при необходимости)
- ✓ Применение дополнительных правил к персоне, ищущей работу

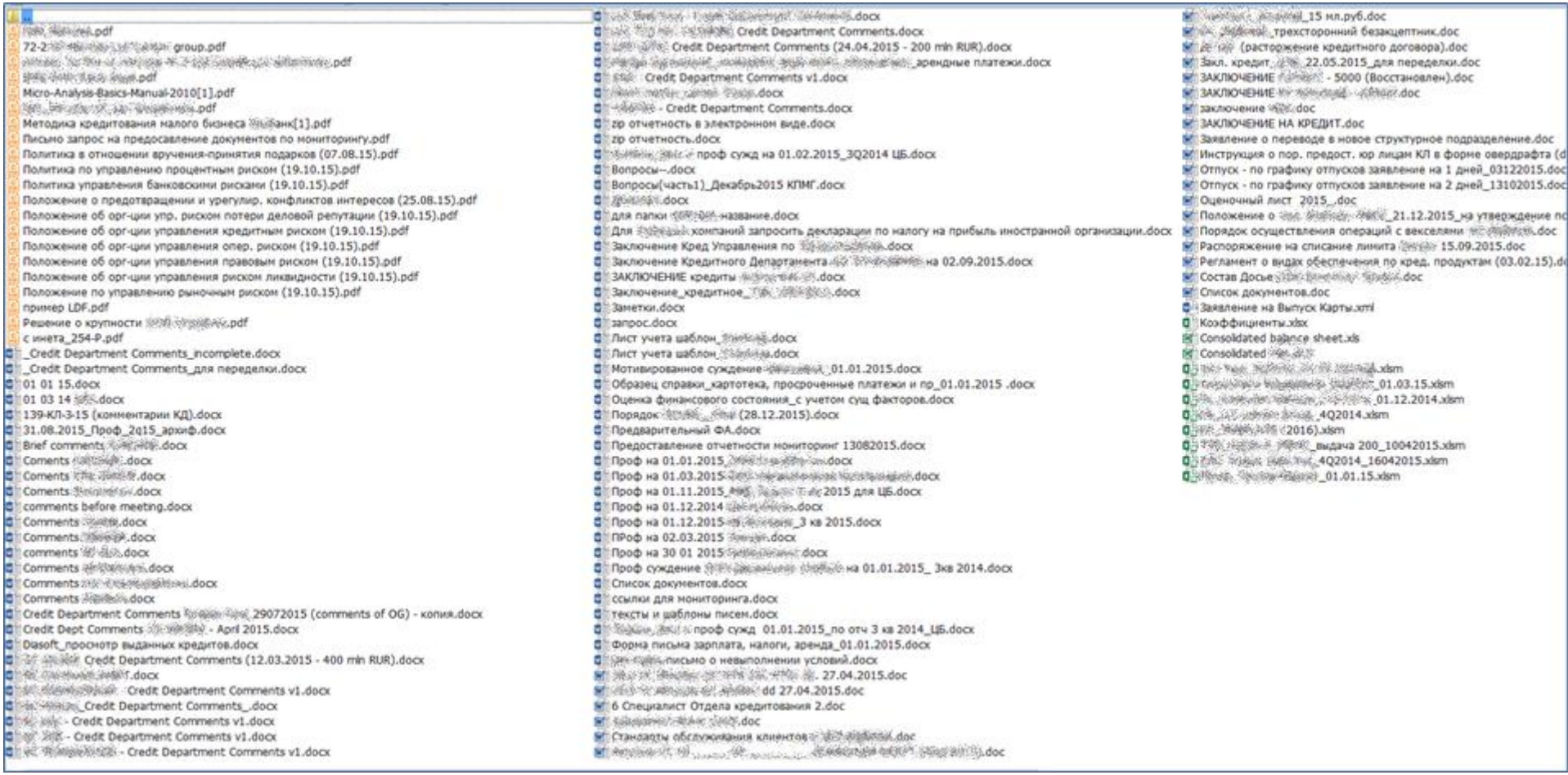
Персоны и подразделения в ГрОК



Прогнозирование утечек



Массовая пересылка увольняющимся конфиденциальных документов



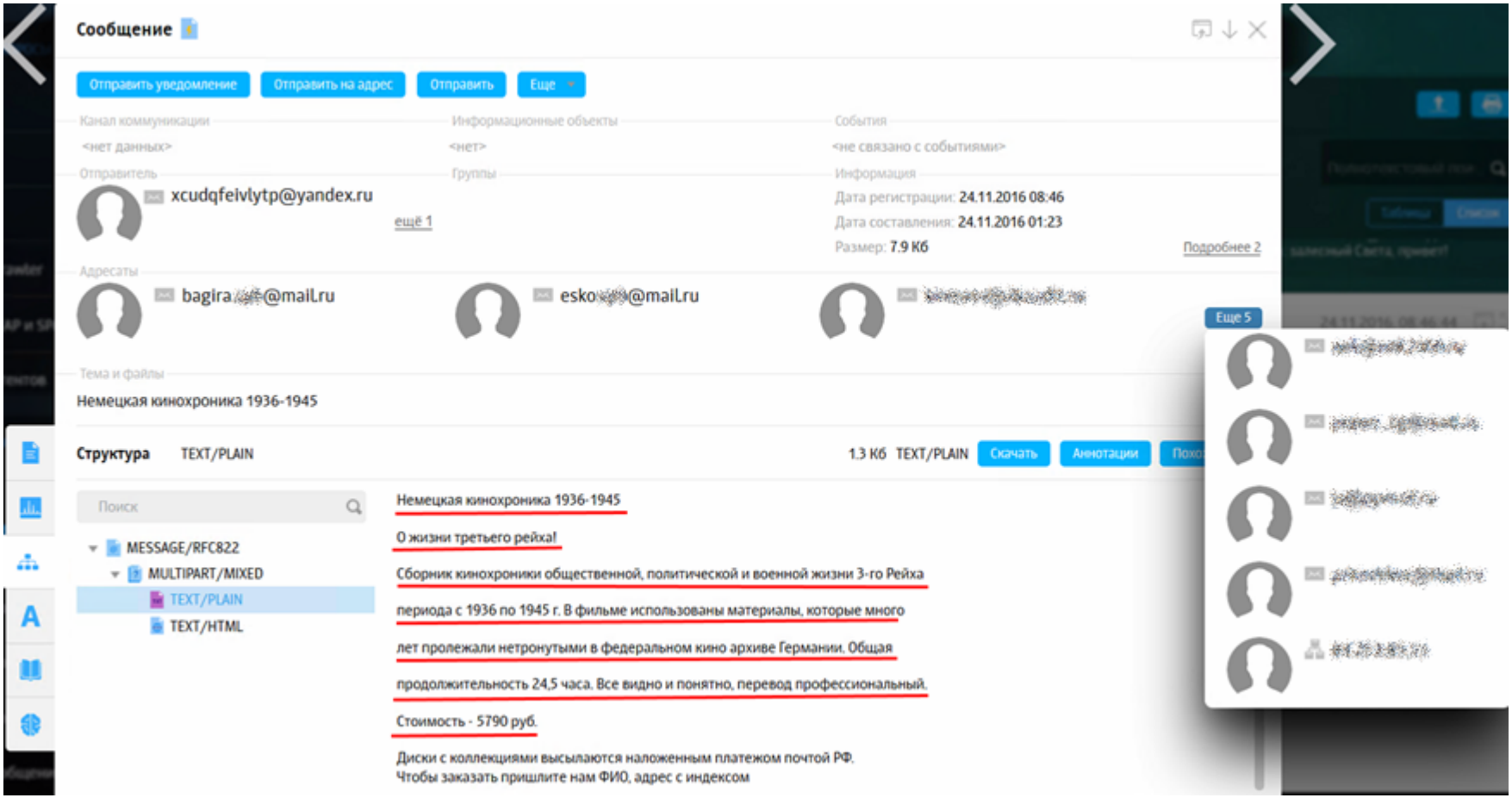
Переслано на личный ящик – 318 файлов, из них 127 - служебных документов

Группа риска «Радикалы»

Примеры способов выявления:

- Лексика (характерные ключевые слова)
- Посещение сайтов и групп в социальных сетях радикальных религиозных организаций
- Загрузка файлов соответствующего содержания, (например, электронные книги, песни)

Анализ «мусора» помог в выявлении группы риска «Экстремизм»



СПАМ-сообщение с предложением о покупке нацистской кинохроники

Пример выявления персоны из группы риска «Деструктивные религии»

Поиск по сайту

Завещание Никлота. Подлинная летопись западных славян

Автор: Сидоров Г.А. | Раздел: Тайны цивилизаций

В данной книге впервые в истории литературы, в поэтической форме, представлены события, происходившие в первой половине XII столетия на территории венедской, прибалтийской Руси. Там где некогда стояли великие стольные города западных славян: Торнов, Ретра, Волин, Венета, Дубин и другие.

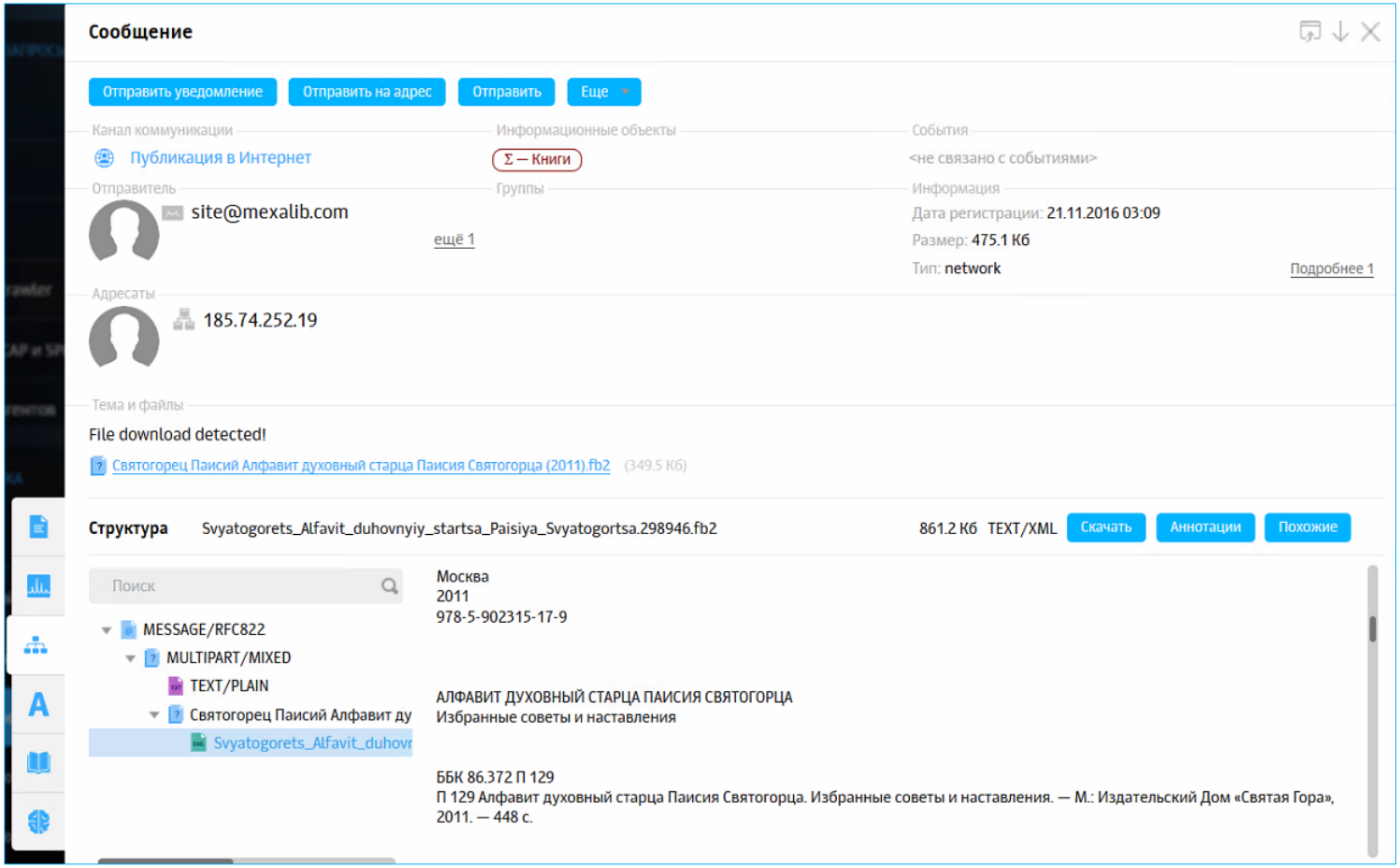
В книге ярко показана роль вождя венетов, князя ободритов — Никлота, доподлинно раскрыт его гений полководца и политика, способность князя верить в победу над силами тьмы даже тогда, когда, казалось бы, всякая надежда иссякла. Очень ярко показана в книге роль в отражении сил Запада русских волхвов, которые, смело используя свою магическую мощь, вступили в противоборство с чёрными магами — вдохновителями нашествия.

Впервые в истории литературы в данной книге в образной художественной форме показаны подлинные оккультные техники и возможности волхвов — белых магов, хранителей духовности русов, а также техники оккультной борьбы чёрных магов.

Далее »

Копирование такой книги может быть следствием увлечения Петрова А.В. оккультными «науками» и/или другими деструктивными религиями и сектами. Поэтому данная активность определена как потенциально опасная.

Выявление персоны из группы риска «Религия»



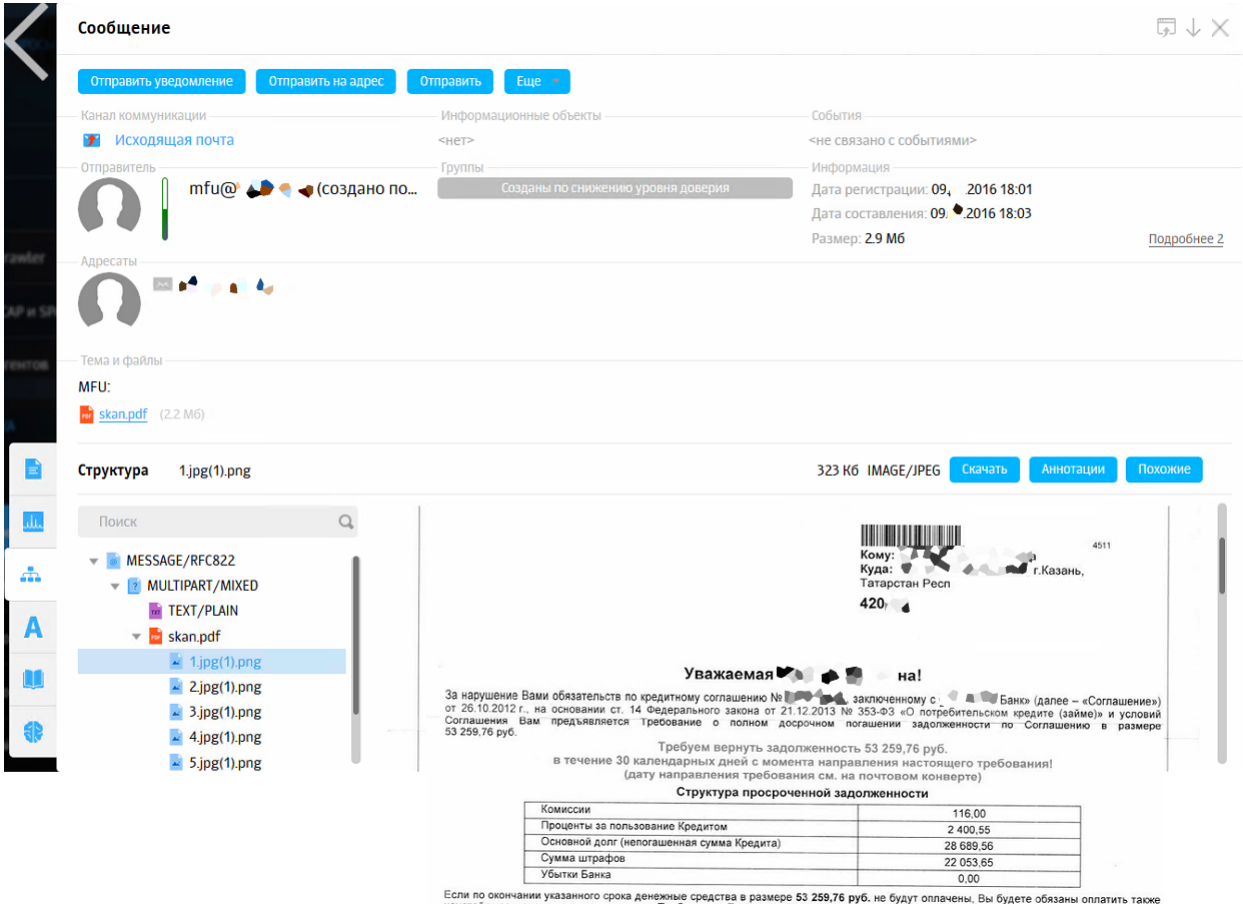
Сообщение со скачанной из интернета электронной книгой, Возможно, что это увлечение историей, но возможно и увлечение религией – для вывода данных недостаточно

Группа риска «Должники»

Способы выявления:

- Анализ лексики (просьбы о займах, требования о возврате долгов)
- Банковские требования о погашении задолженности или кредита
- Обсуждение возможности перекредитования, поиск услуг по подготовке документов
- Ипотека и последующий мониторинг тяжелых жизненных ситуаций

Группа риска «Должники»



Сканирование на служебном МФУ требования о погашении задолженности банку.

Несоответствие доходов и расходов

- ✓ Покупка квартиры в Подмосковье
- ✓ Покупка дорогостоящих туров
- ✓ Строительство дачи
- ✓ Покупка драгоценностей

Расчетный листок за Март 2017

Организация: ООО "МедКлиника" — Отдел материального учета, затрат и взаиморасчетов

Иванова Елена Петровна

К выплате: — Бухгалтер

ГКМ0013631

Общий облагаемый доход: 242 068,37

Применено вычетов по НДФЛ: на "себя" | на детей | имущественных

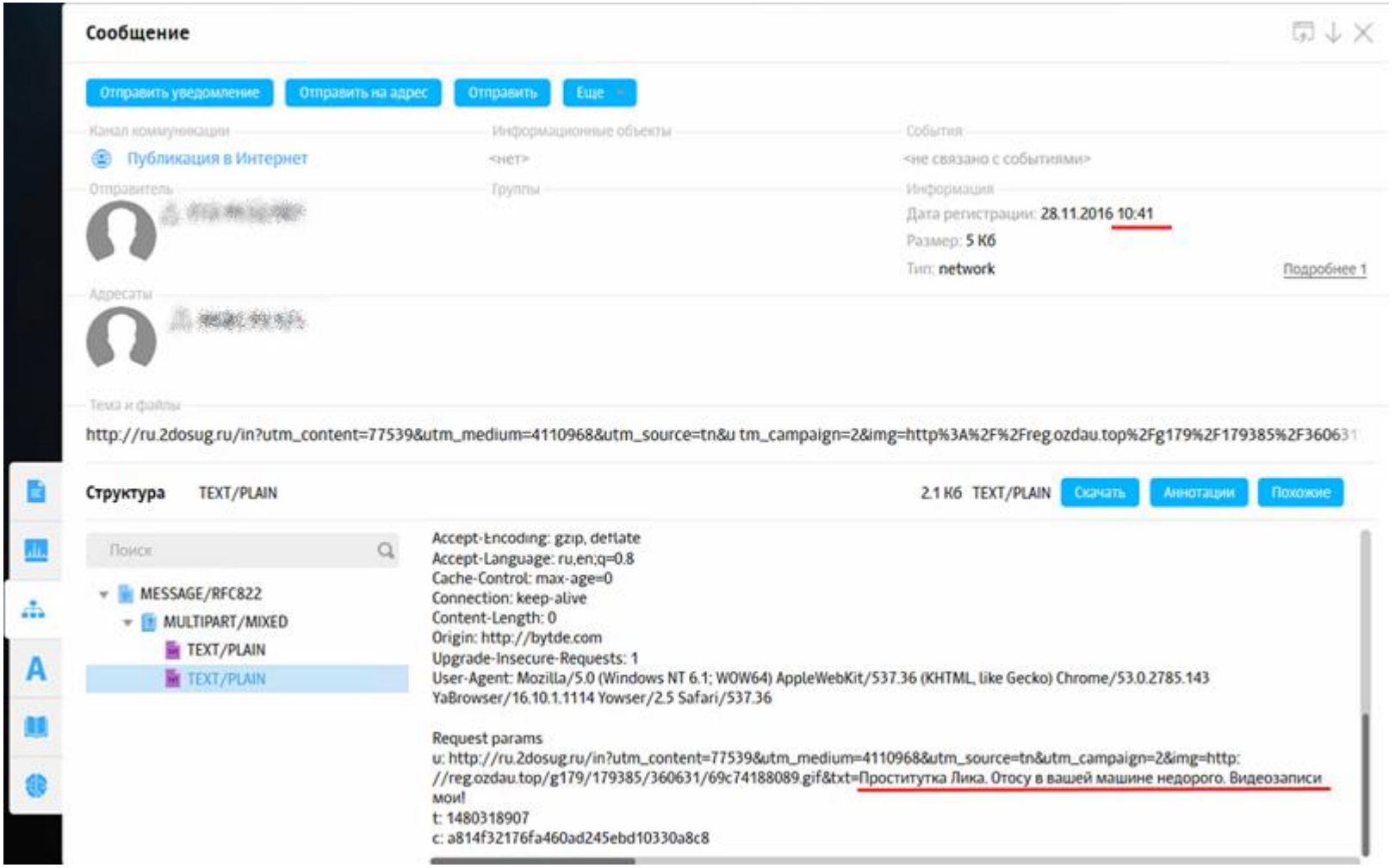
Вид	Период	Отработано Дни	Отработано Часы	Оплачено Дни	Оплачено Часы	Сумма	Вид	Период	Сумма
1.Начислено							**2. Удержано**		
Оклад по часам показатели: Тарифная ставка месячная - 44 000	1-31 Мар 17	19	151		151	37 965,71	НДФЛ исчисленный по ставке 13(30)%	1-31 Мар 17	16 332,00
оплачены периоды:	1-28 Мар 17								
Оплата отпуска по календарным дням показатели: Процент - 100	29-31 Мар 17			-3		-5 896,29			
Оплата отпуска по календарным дням показатели: Процент - 100	29-31 Мар 17			3		6 554,43			
Административная премия (процентом) показатели: Процент оплаты - xxx	1-31 Мар 17					9 491,43			
оплачены периоды:	1-28 Мар 17								
По итогам работы за год (фиксированная сумма) показатели: Сумма - 77 513	Январь 16-Декабрь 16					77 513,00			
Всего начислено						125 628,28	Всего удержано		16 332,00
3. Доходы в натуральной форме							**4. Выплачено**		
							Перечислено в банк	1-31 Мар 17	67 436,00
							Перечислено в банк (под	1-31 Мар 17	17 280,86
							Перечислено в банк (под	1-31 Мар 17	24 579,42
Всего натуральных доходов							Всего выплат		109 296,28
Долг за работником на начало месяца							Долг за работником на конец месяца		
в том числе: излишне удержанного НДФЛ на начало периода							в том числе: излишне удержанного НДФЛ на конец периода		

Группа риска «Несоответствие доходов и расходов»

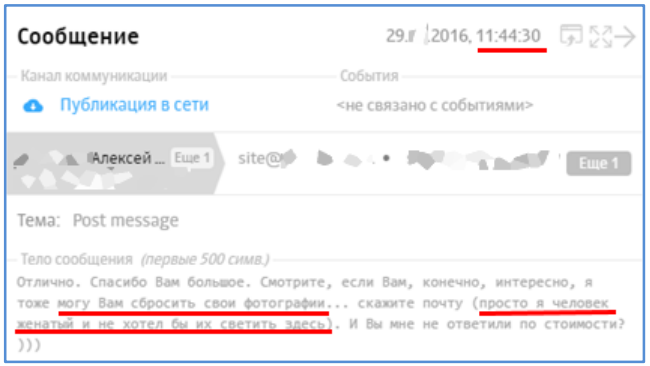
Способы выявления:

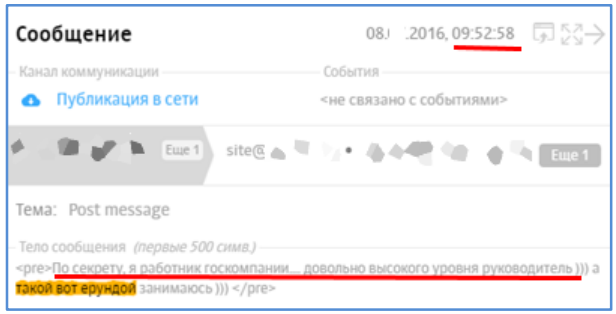
- Переписка с риэлтором о покупке недвижимости
- Печать и сканирование документов на покупку и оплату счетов
- Обсуждение покупок с родственниками и коллегами
- Посещение тематических сайтов и переписка с представительницами древнейшей профессии

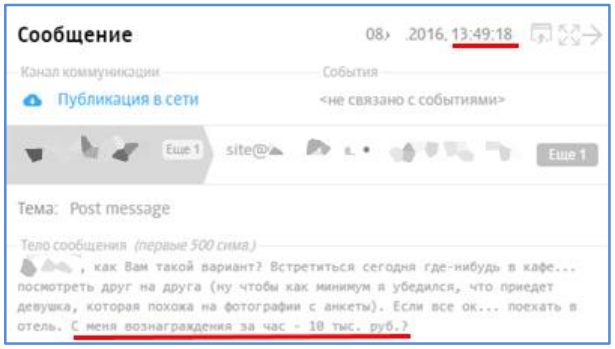
Утреннее хобби

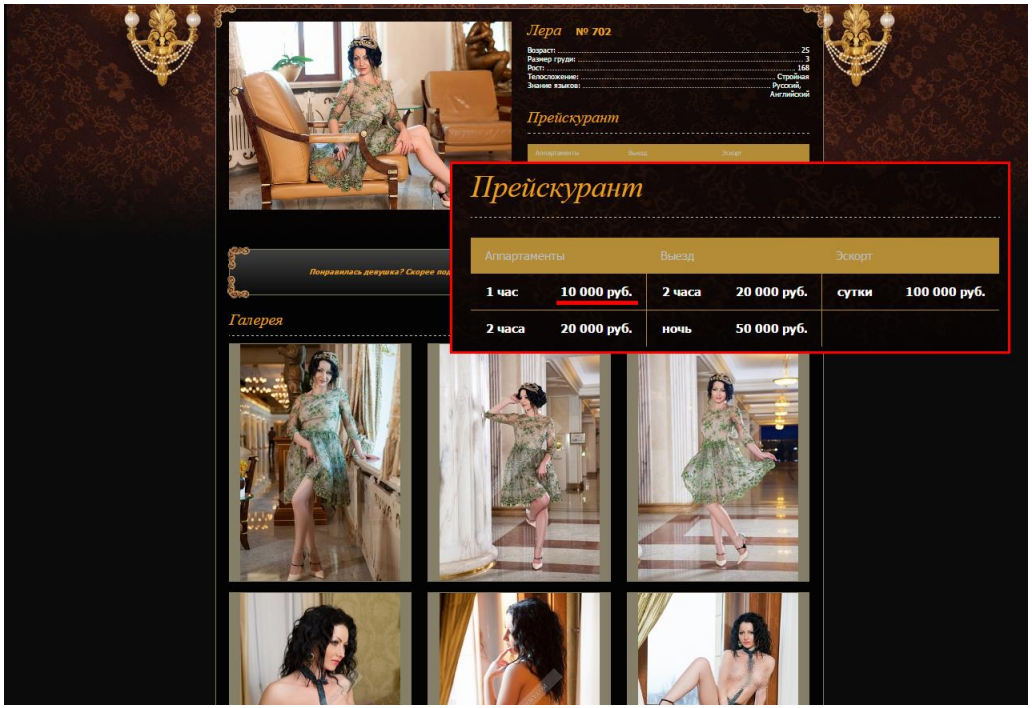


Хобби – проститутки



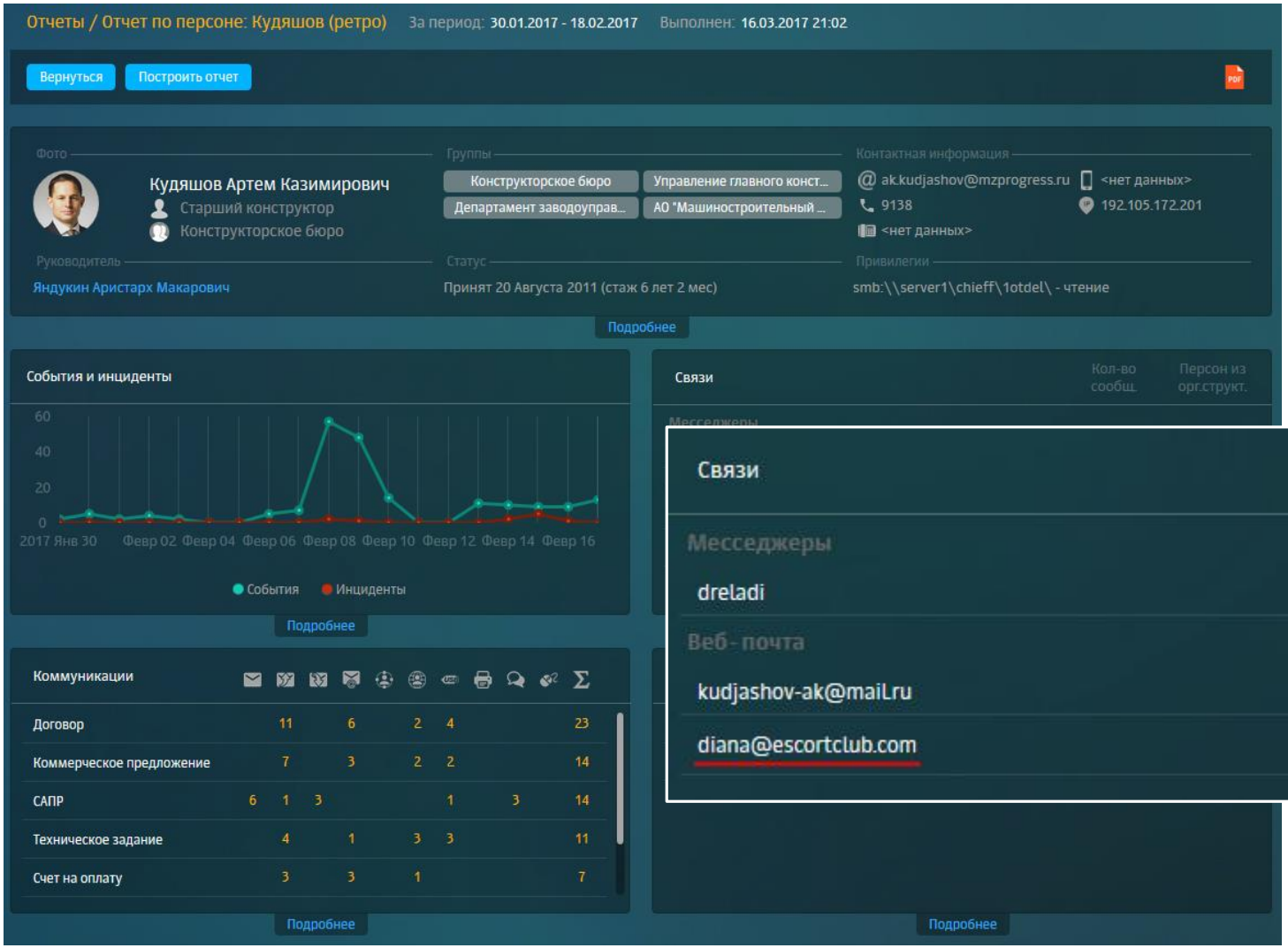






1. Несоответствие доходов и расходов
2. Потенциальный объект вербовки

Сводный отчет по персоне: анализ связей



Пример расследования утечки

Иванов И.О.
специалист отдела техподдержки
и эксплуатации
(уволен 19.04.2017 г.)

1). Положение об обслуживании банкоматов…

2). Должностная инструкция специалиста отдела техподдержки…

Петров А.В.
Главный специалист отдела
инфраструктуры

Личные сообщения
(3НДФЛ)

Инструкция по инкассации банктоматов NCR…

Служебные документы по обслуживанию и инкассации банкоматов

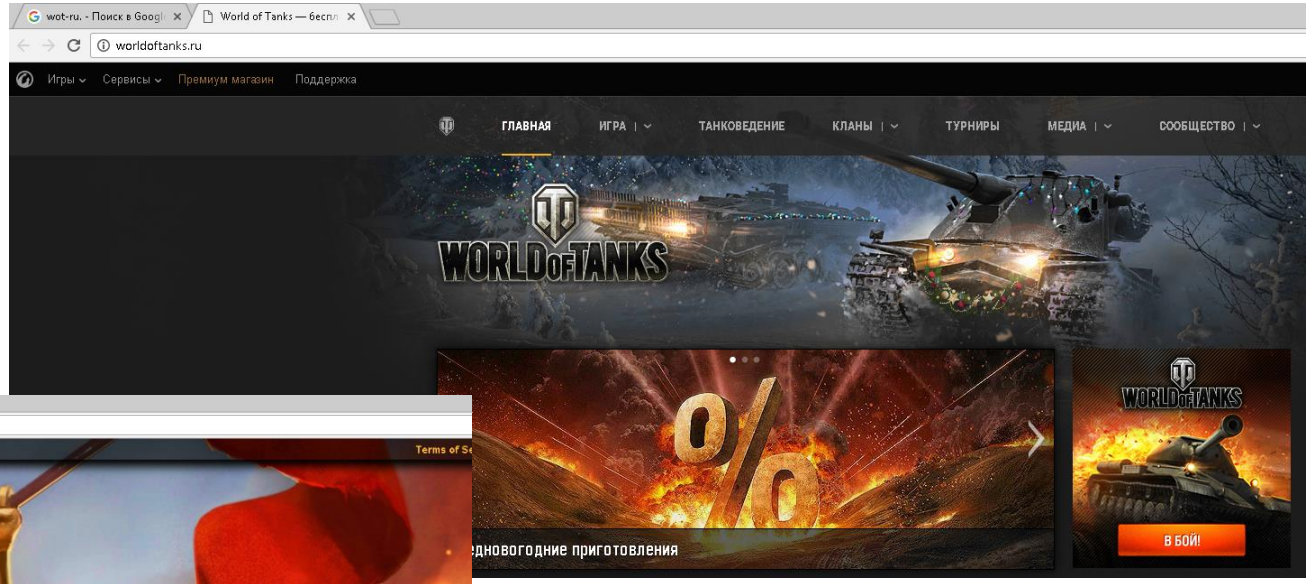
xaker123@mail.ru

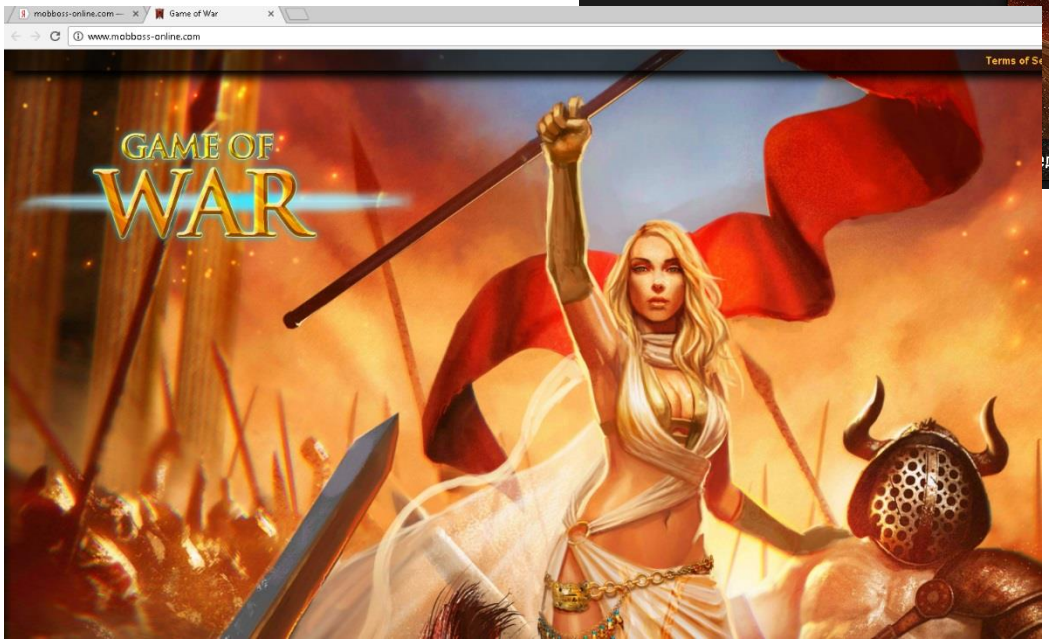
petrov_a@mail.ru

Совместное использование почтовых ящиков

Online игры

Сайт **wot-ru.loc**





Сайт **mobboss-online.com**

Группа риска «Хобби»: «безобидная» нумизматика

Сообщение

Отправить уведомление | Отправить на адрес | Отправить | Еще

Канал коммуникации: Публикация в сети

Информационные объекты: <нет>

События: <не связано с событиями>

Отправитель

ещё 1

Группы

Информация

Дата регистрации: 2016 15:35

Размер: 5.7 Кб

Протокол: http

Подробнее 4

Адресаты

Тема и файлы

Post message

Текст сообщения

А что можно сказать по подлинности этого злата имперского весом 4,295 г? 0,005 в минус вроде вполне допустимо. И сколько будет стоить это злато? Интересует цена как одной монеты, так и небольшой партии.

4,31 г

Подведем итоги

«People centric security» в DLP – маркетинговая фича или объективная необходимость?

Есть вопросы?

Задавайте!