

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

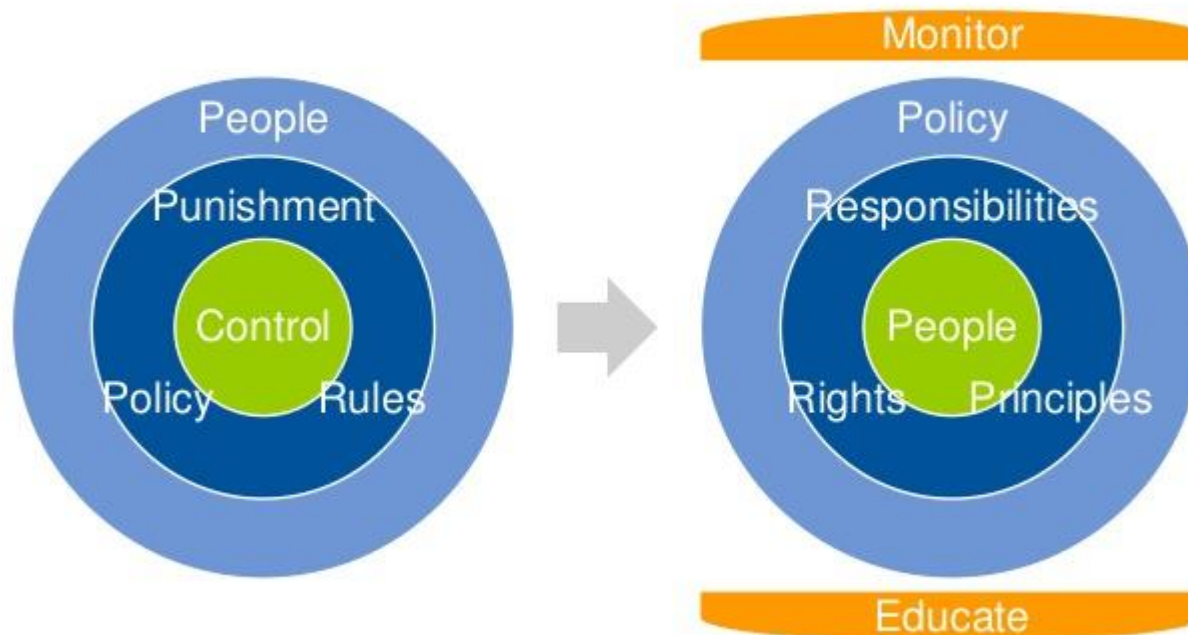


«People centric security» в DLP – маркетинговая фича или объективная необходимость?

8 ноября 2017 г.

Модель People-Centric Security

From Control-Centric Security to People-Centric Security

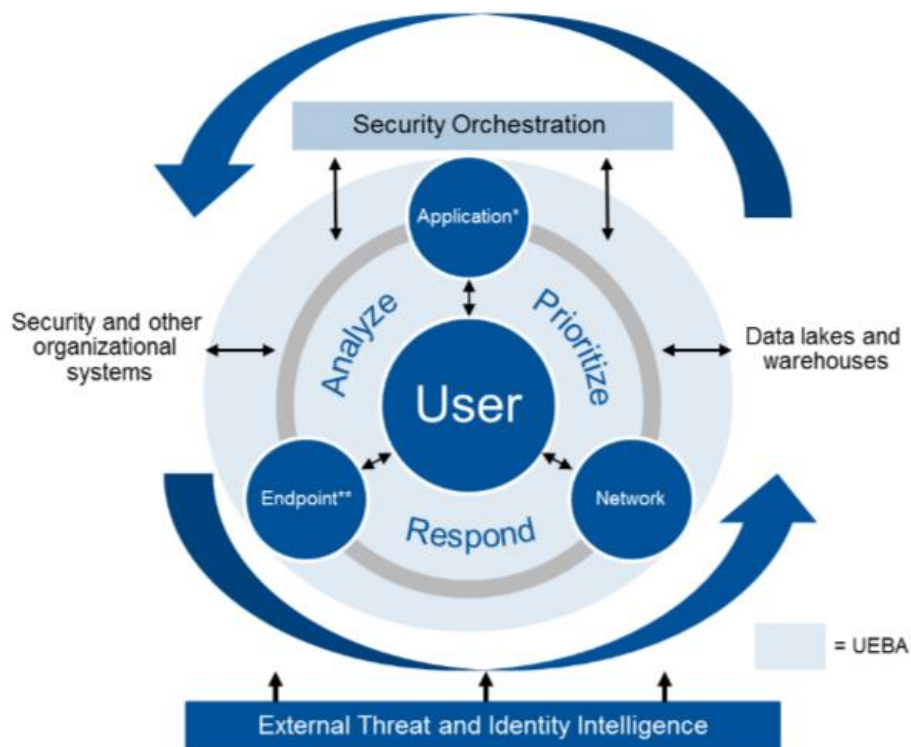


Gartner

Принципы PCS

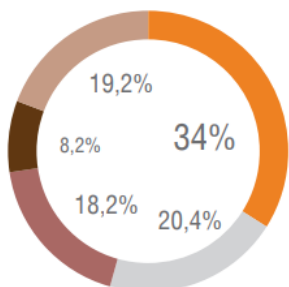
- ✓ **Общность**
- ✓ **Автономность**
- ✓ **Подотчетность**
- ✓ **Ответственность**
- ✓ **Незамедлительность**
- ✓ **Пропорциональность**
- ✓ **Прозрачность**

Значение мониторинга и аналитики

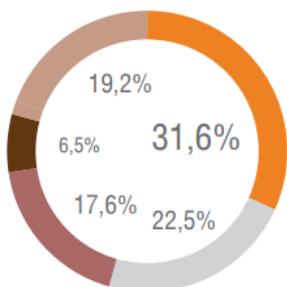


- ✓ Мониторинг пользователей как ключевой элемент People-Centric Security
- ✓ Аналитика поведения пользователей и сущностей (UEBA) становится ключевой функцией безопасности
- ✓ Потенциальный источник ценной информации для цифровых гуманитарных инициатив

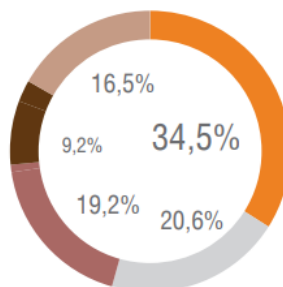
Распределение по каналам утечек



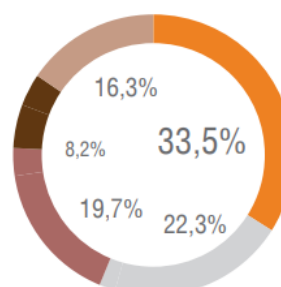
Q1 2016



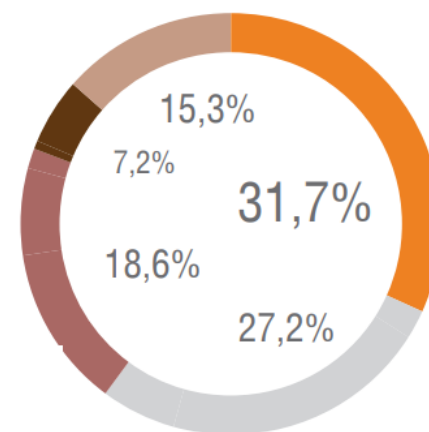
Q2 2016



Q3 2016



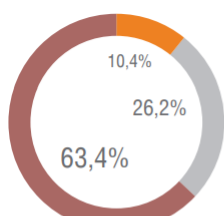
Q4 2016



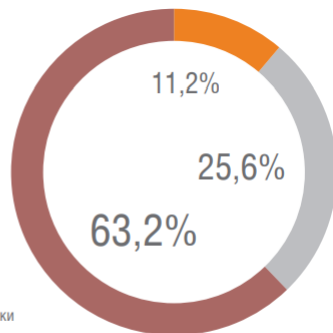
1/2 2017

- Электронная почта
- Веб-ресурсы
- Съемные носители
- Печать
- Устройства прямого доступа в интернет

Инициаторы внутренних инцидентов



Q4 2016



1/2 2017

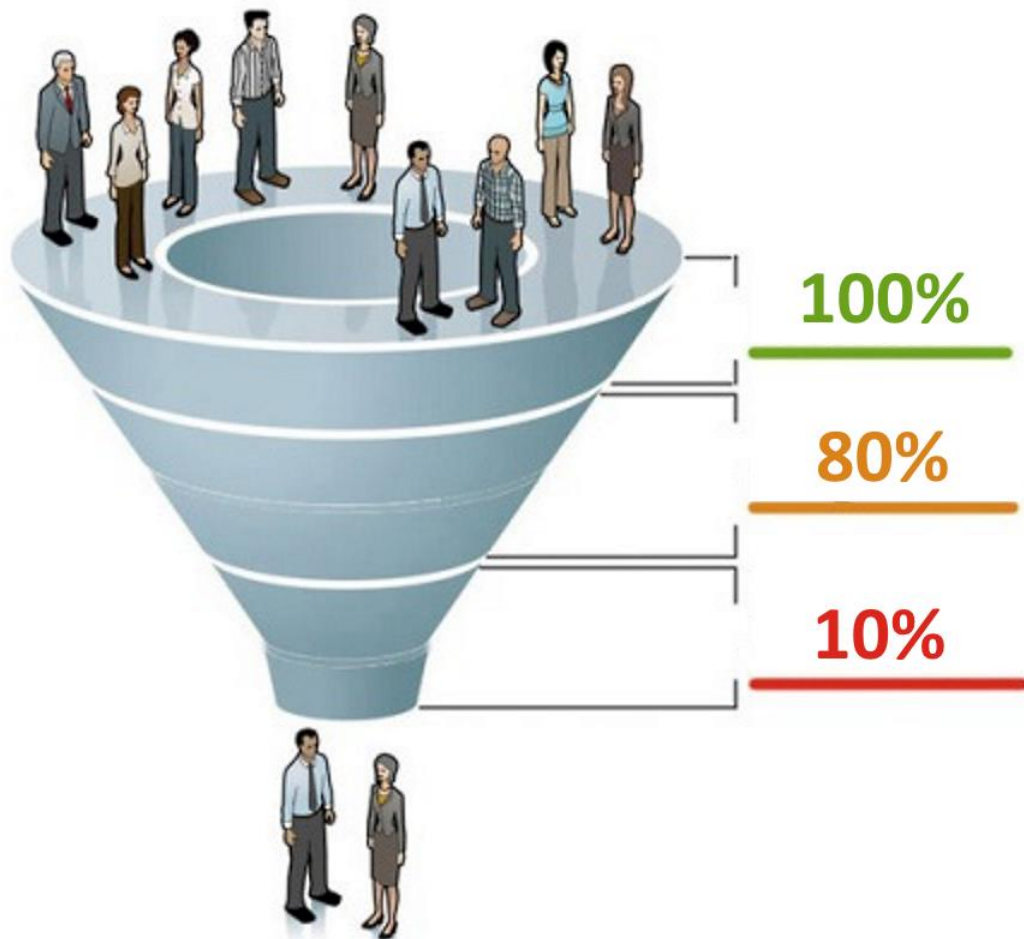
- Аутсорсеры, контрагенты, подрядчики
- Внутренние штатные администраторы
- Прочие внутренние пользователи



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





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
- ✓ ...




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

Персона Пугачева Елена Филипповна

Соединить карточки Редактировать Сводный отчет по персоне Скопировать ссылку

Фото

Пугачева Елена Филипповна
 Ст. бухгалтер
 Отдел бухгалтерского учета

Группы
 Поиск работы АО "Машиностроительный з...
 Отдел Главного бухгалтера Управление бухгалтерского ...
 Отдел бухгалтерского учета


Контактная информация
 @ ef.pugachjova@mzprogress... 8-903-123-4567
 1154 IP 192.105.172.229
 <нет данных>

Руководитель
 Канаша Светлана Андрияновна

Статус
 Принят 15 Января 2014 (стаж 3 года 5 мес)

Привилегии
 smb:\\1c-7.7\tehproject\pravo\ - владелец

Изменение уровня доверия
 Текущее значение: 0 Дельта: 0



Электронные адреса	Персональные данные	Примечания
SID: S-1-5-21-793904598-20...	День рождения: 12.02.1964	ie.kalinkin 27.04.2015
Login: ef.pugachjova		Личная карточка Т-2 (Пугачева Е.Ф.).doc (186 КБ)
Почта: ef.pugachjova@mzprog...	Дополнительные свойства	
Skype: ef.pugachjova	Мобильный телефон: 8-903-123-4567	

Рабочие станции

IP адрес	192.105.172.229
Имя хоста	pc-efpugachjova.mzpro...

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)





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

Solar Dozor

Поиск в системе

+ Раздел + Группы + Персону

Начните вводить текст

Досье / Поиск работы

Персоны События Коммуникации **Правила**

Добавить персону

На особом контроле ✓

Испытательный срок

На увольнение

Под подозрением

Поиск работы

Тендерный отдел

Организационная структура

АО "Машиностроительный завод "Прогресс"

Департамент заводоуправления

Отдел Главного бухгалтера






Первый отдел


Пресс-служба

Производственный департамент

Служба внутреннего контроля

ФИО ↑ Статус агента уд

	Пугачева Елена Филипповна Ст. бухгалтер	0	5	8	12
	Семерикова Наталья Антониновна Заведующая лабораторией качества	0			4
	Сереброва Екатерина Семеновна Ст.специалист по организации тендеров	0	1	1	3
	Сунгатулин Юрий Арсениевич Ведущий конструктор	0			3
	Уваров Константин Давидович Ст.менеджер	0			2



Ямзина Владлена Мефодиев... 🔍

Менеджер по работе с клиентами
Отдел депозитных операций


серьезные события	1
сообщения	3
файлы исходящие	3
файлы входящие	0

Группы на особом контроле


<p>На увольнение</p> <div style="display: flex; align-items: center; justify-content: center;"> +5 <div style="border: 2px solid orange; border-radius: 50%; width: 40px; height: 40px; display: flex; align-items: center; justify-content: center;"> 5 </div> </div>	<p>Испытательный срок</p> <div style="display: flex; align-items: center; justify-content: center;"> <div style="border: 2px solid teal; border-radius: 50%; width: 40px; height: 40px; display: flex; align-items: center; justify-content: center;"> 2 </div> 0 </div>
<p>Расходование материальных средств</p> <div style="display: flex; align-items: center; justify-content: center;"> <div style="border: 2px solid teal; border-radius: 50%; width: 40px; height: 40px; display: flex; align-items: center; justify-content: center;"> 4 </div> 0 </div>	<p>Под подозрением</p> <div style="display: flex; align-items: center; justify-content: center;"> <div style="border: 2px solid teal; border-radius: 50%; width: 40px; height: 40px; display: flex; align-items: center; justify-content: center;"> 1 </div> 0 </div>

Аномальное поведение

Персоны. Снижение уровня доверия




Бубнов Вячеслав Самуилович
Заместитель начальника отдела




Ершова Евгения Александровна
Главный бухгалтер

Автоматически созданные персоны



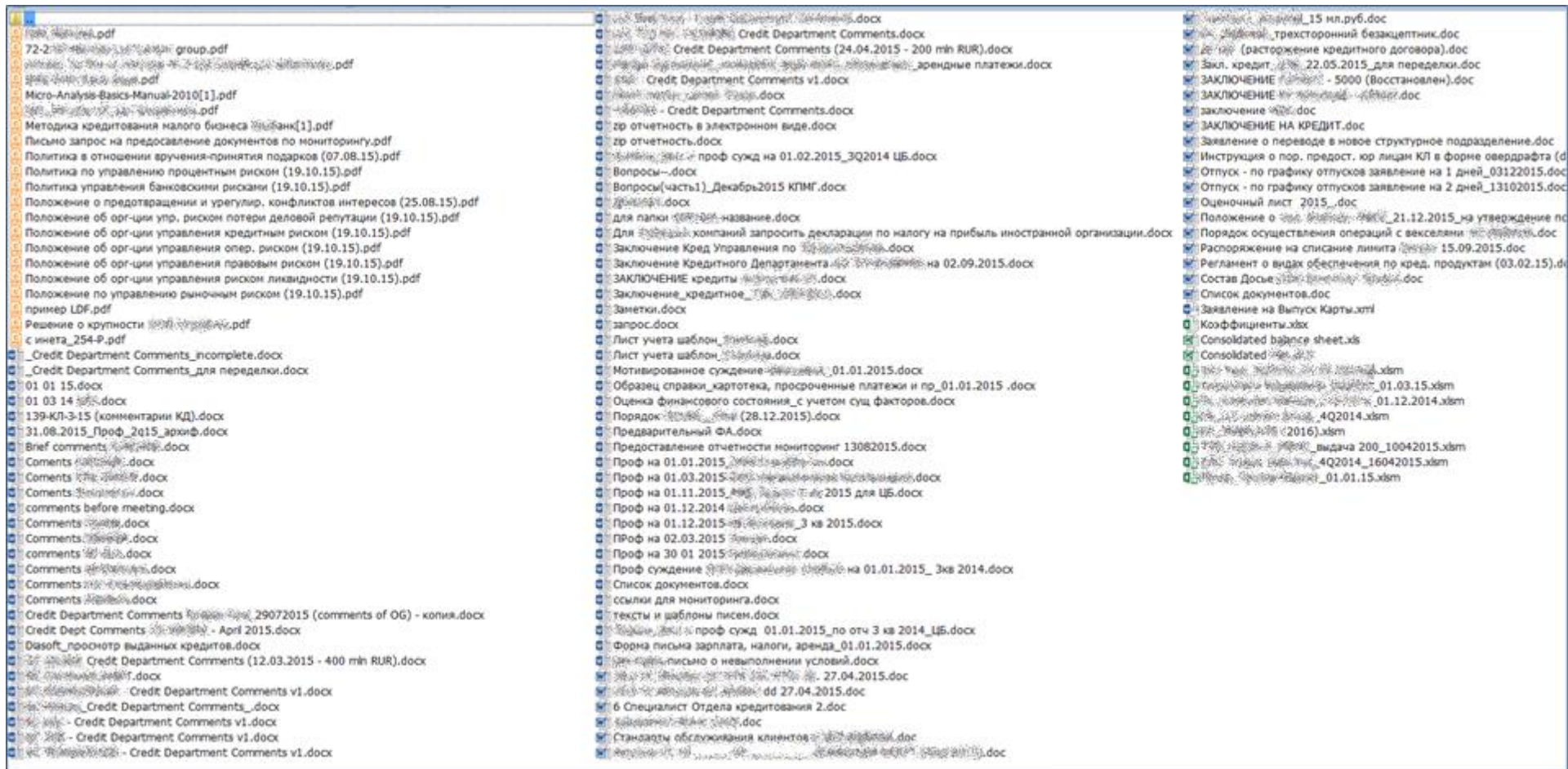
amadeus@gmail.com



floyd.george49@mailRu



Массовая пересылка увольняющимся конфиденциальных документов

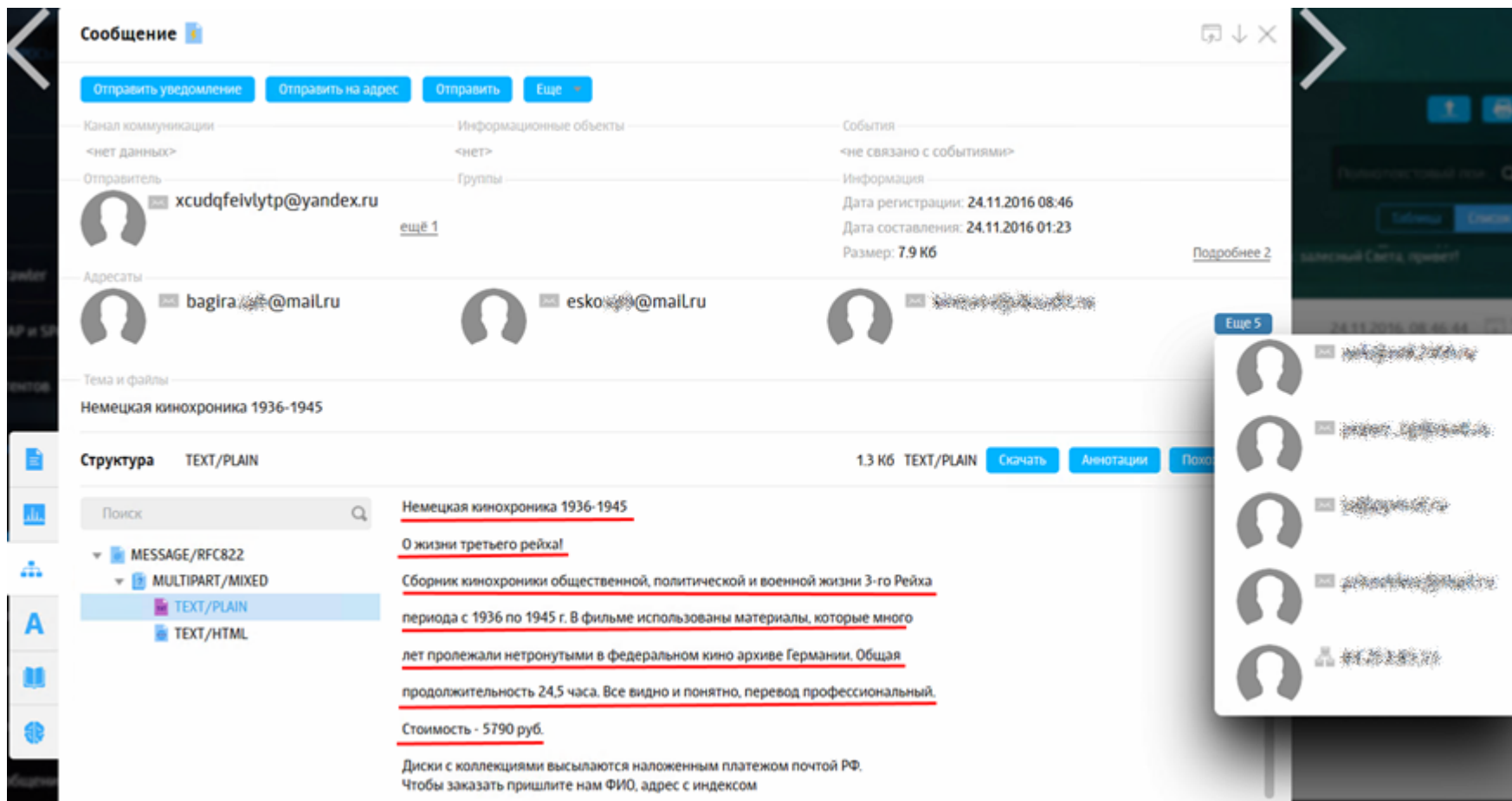


Переслано на личный ящик – 318 файлов, из них 127 - служебных документов

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)

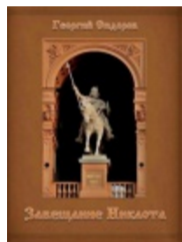
Анализ «мусора» помог в выявлении группы риска «Экстремизм»



СПАМ-сообщение с предложением о покупке нацистской кинохроники

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 венецкой, прибалтийской Руси. Там где некогда стояли великие столичные города западных славян: Торнов, Ретра, Волин, Венета, Дубин и другие.

В книге ярко показана роль вождя венецков, 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.

Сообщение 📄 ↓ ✕

Отправить уведомление Отправить на адрес Отправить Еще ▾

Канал коммуникации	Информационные объекты	События
🗣️ Публикация в Интернет	📄 Σ — Книги	<не связано с событиями>
Отправитель	Группы	Информация
👤 site@mexalib.com	ещё 1	Дата регистрации: 21.11.2016 03:09 Размер: 475.1 Кб Тип: network Подробнее 1
Адресаты		
👤 185.74.252.19		
Тема и файлы		
File download detected!		
🔗 Святогорец Паисий Алфавит духовный старца Паисия Святогорца (2011).fb2 (349.5 Кб)		
Структура	Svyatogorets_Alfavit_duhovnyiy_startsa_Paisiya_Svyatogortsa.298946.fb2	861.2 Кб TEXT/XML Скачать Аннотации Похожие
Поиск	Москва 2011 978-5-902315-17-9	
<ul style="list-style-type: none"> MESSAGE/RFC822 <ul style="list-style-type: none"> MULTIPART/MIXED <ul style="list-style-type: none"> TEXT/PLAIN <ul style="list-style-type: none"> Святогорец Паисий Алфавит ду <ul style="list-style-type: none"> Svyatogorets_Alfavit_duhov 	АЛФАВИТ ДУХОВНЫЙ СТАРЦА ПАИСИЯ СВЯТОГОРЦА Избранные советы и наставления ББК 86.372 П 129 П 129 Алфавит духовный старца Паисия Святогорца. Избранные советы и наставления. — М.: Издательский Дом «Святая Гора», 2011. — 448 с.	

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

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»

Сообщение

Отправить уведомление | Отправить на адрес | Отправить | Еще

Канал коммуникации: Исходящая почта

Отправитель: mfu@ (создано по...)

Адресаты:

Тема и файлы: MFU: skan.pdf (2.2 Мб)

Структура: 1.jpg(1.png) 323 Кб IMAGE/JPEG

Поиск

- MESSAGE/RFC822
 - MULTIPART/MIXED
 - TEXT/PLAIN
 - skan.pdf
 - 1.jpg(1.png)
 - 2.jpg(1.png)
 - 3.jpg(1.png)
 - 4.jpg(1.png)
 - 5.jpg(1.png)

Кому: [адрес] 4011
Куда: Татарстан Респ
420

Уважаемая [адрес] на!

За нарушение Вами обязательств по кредитному соглашению № [адрес] заключенному с [адрес] Банк (далее – «Соглашение») от 26.10.2012 г., на основании ст. 14 Федерального закона от 21.12.2013 № 353-ФЗ «О потребительском кредите (займе)» и условий Соглашения Вам предьявляется Требование о полном досрочном погашении задолженности по Соглашению в размере 53 259,76 руб.

Требуем вернуть задолженность 53 259,76 руб. в течение 30 календарных дней с момента направления настоящего требования! (дату направления требования см. на почтовом конверте)

Структура просроченной задолженности

Комиссии	116,00
Проценты за пользование Кредитом	2 400,56
Основной долг (непогашенная сумма Кредита)	28 689,56
Сумма штрафов	22 053,65
Убытки Банка	0,00

Если по окончании указанного срока денежные средства в размере 53 259,76 руб. не будут оплачены, Вы будете обязаны оплатить также

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						Бухгалтер		
К выплате:								
ИНН 50/0118651								
Осуществленный доход		242 068,37		на детей		на детей		
Применено вычетов по НДФЛ:		на себя		на детей		имущественных		
Вид	Период	Отработано Дни Часы	Оплачено Дни 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 начисленный 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					16 332,00			
3. Доходы в натуральной форме				4. Выплачено				
					Перечислено в б/ш:	1-31 Мар 17	67 436,00	
					Перечислено в б/ш (под вклад)	1-31 Мар 17	17 280,86	
					Перечислено в б/ш (под вклад)	1-31 Мар 17	24 579,42	
Всего натуральных доходов				Всего выплат				
Долг за работником на начало месяца				Долг за работником на конец месяца				
в том числе: излишне удержанного НДФЛ на начало периода				излишне удержанного НДФЛ на конец периода				
				109 296,28				





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

Сообщение
🔍 ⏴ ✕

Отправить уведомление
Отправить на адрес
Отправить
Еще ▾

Канал коммуникации Публикация в Интернет	Информационные объекты <нет>	События <не связано с событиями>
Отправитель 	Группы	Информация Дата регистрации: 28.11.2016 10:41 Размер: 5 Кб Тип: network
Адресаты 		Подробнее 1
Тема и файлы http://ru.2dosug.ru/in?utm_content=77539&utm_medium=4110968&utm_source=tn&utm_campaign=2&img=http%3A%2F%2Freg.ozdau.top%2Fg179%2F179385%2F360631		

Структура
TEXT/PLAIN

2.1 Кб TEXT/PLAIN
 Скачать
Аннотации
Похожие

Поиск

Accept-Encoding: gzip, deflate
 Accept-Language: ru,en;q=0.8
 Cache-Control: max-age=0
 Connection: keep-alive
 Content-Length: 0
 Origin: http://bytde.com
 Upgrade-Insecure-Requests: 1
 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 YaBrowser/16.10.1.1114 Yowser/2.5 Safari/537.36

MESSAGE/RFC822

Accept-Encoding: gzip, deflate
 Accept-Language: ru,en;q=0.8
 Cache-Control: max-age=0
 Connection: keep-alive
 Content-Length: 0
 Origin: http://bytde.com
 Upgrade-Insecure-Requests: 1
 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 YaBrowser/16.10.1.1114 Yowser/2.5 Safari/537.36

MULTIPART/MIXED

Accept-Encoding: gzip, deflate
 Accept-Language: ru,en;q=0.8
 Cache-Control: max-age=0
 Connection: keep-alive
 Content-Length: 0
 Origin: http://bytde.com
 Upgrade-Insecure-Requests: 1
 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 YaBrowser/16.10.1.1114 Yowser/2.5 Safari/537.36

TEXT/PLAIN

Accept-Encoding: gzip, deflate
 Accept-Language: ru,en;q=0.8
 Cache-Control: max-age=0
 Connection: keep-alive
 Content-Length: 0
 Origin: http://bytde.com
 Upgrade-Insecure-Requests: 1
 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 YaBrowser/16.10.1.1114 Yowser/2.5 Safari/537.36

TEXT/PLAIN

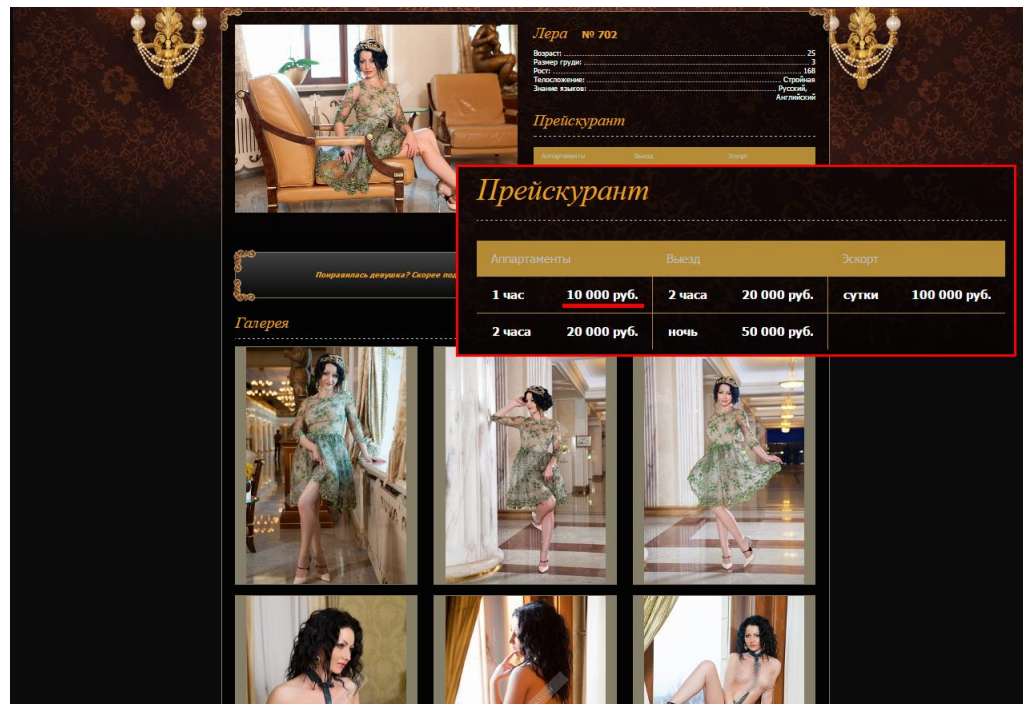
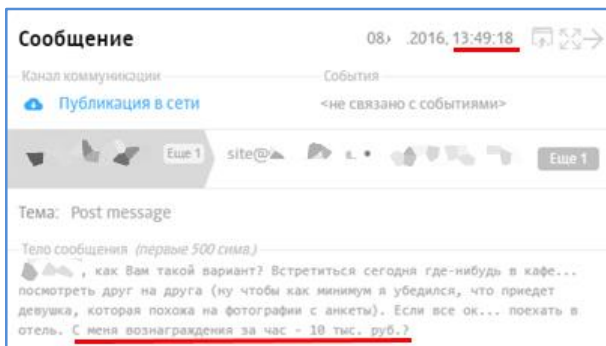
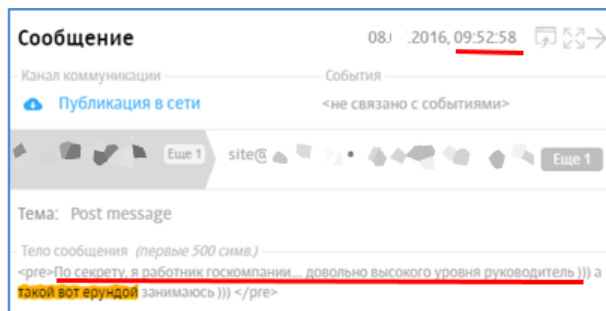
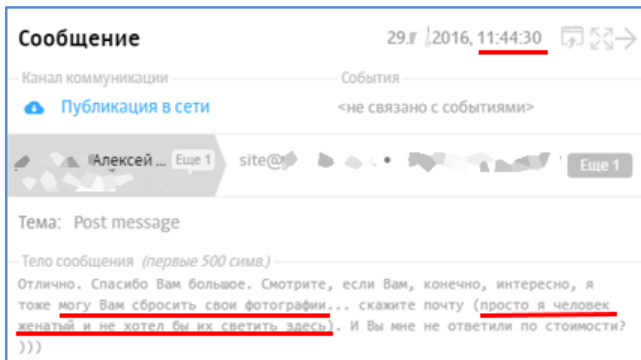
Accept-Encoding: gzip, deflate
 Accept-Language: ru,en;q=0.8
 Cache-Control: max-age=0
 Connection: keep-alive
 Content-Length: 0
 Origin: http://bytde.com
 Upgrade-Insecure-Requests: 1
 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 YaBrowser/16.10.1.1114 Yowser/2.5 Safari/537.36

Request params
 u: http://ru.2dosug.ru/in?utm_content=77539&utm_medium=4110968&utm_source=tn&utm_campaign=2&img=http://reg.ozdau.top/g179/179385/360631/69c74188089.gif&txt=Проститутка Лика. Отосу в вашей машине недорого. Видеозаписи мои!
 t: 1480318907
 c: a814f32176fa460ad245ebd10330a8c8

solaresecurity.ru

+7 (499) 755-07-70

29




1. Несоответствие доходов и расходов
2. Потенциальный объект вербовки

Сводный отчет по персоне: анализ связей

Отчеты / Отчет по персоне: Кудяшов (ретро) За период: 30.01.2017 - 18.02.2017 Выполнен: 16.03.2017 21:02

[Вернуться](#) [Построить отчет](#)

Фото



Кудяшов Артем Казимирович
 Старший конструктор
 Конструкторское бюро

Руководитель
 Яндукин Аристарх Макарович

Группы

- Конструкторское бюро
- Управление главного конст...
- Департамент заводоуправ...
- АО "Машиностроительный ..."

Статус
 Принят 20 Августа 2011 (стаж 6 лет 2 мес)


Контактная информация

- @ ak.kudjashov@mzprogress.ru
- 9138
- 192.105.172.201
- <нет данных>
- <нет данных>

Привилегии
 smb:\server1\chieff\1otdel\ - чтение

[Подробнее](#)

События и инциденты



● События ● Инциденты

[Подробнее](#)

Связи	Кол-во сообщ.	Персон из орг.структ.
Связи		Персон из орг.структ.
Месседжеры		
dreladi	3	1
Веб-почта		
kudjashov-ak@mail.ru	10	1
<u>diana@escortclub.com</u>	5	4

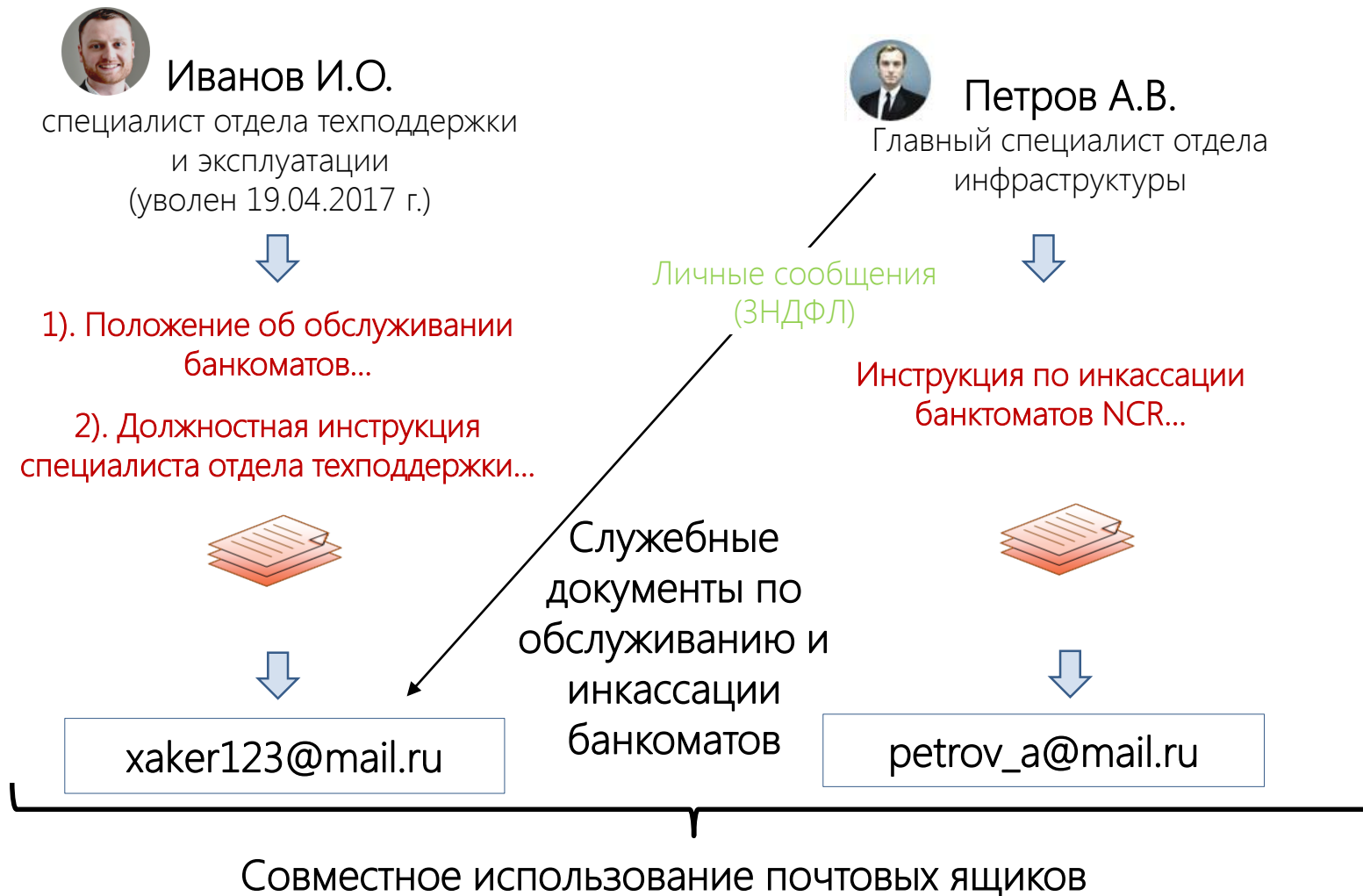
[Подробнее](#)

Коммуникации

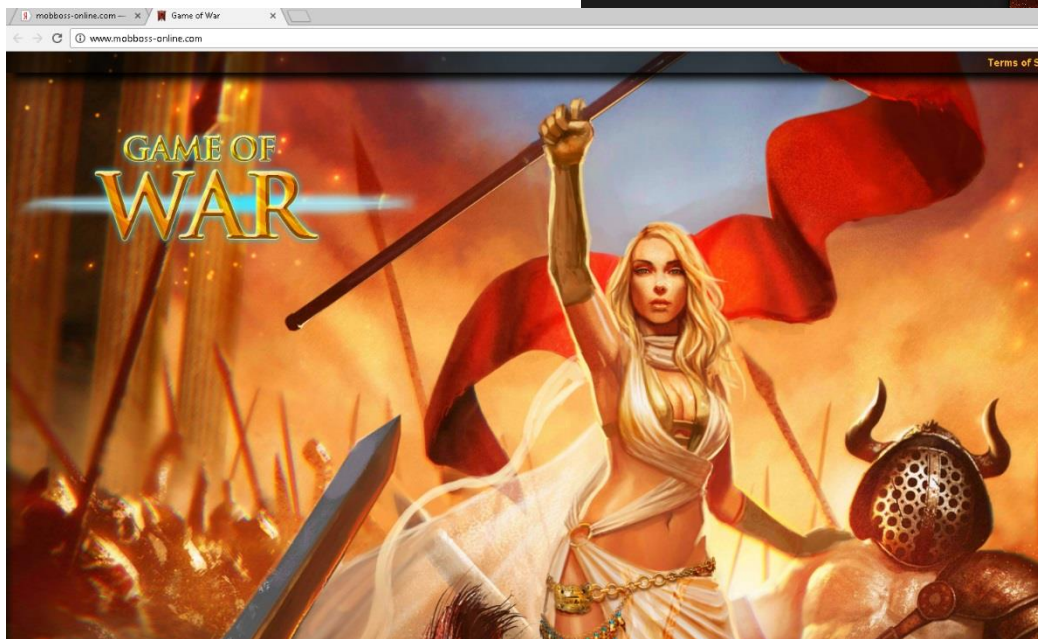
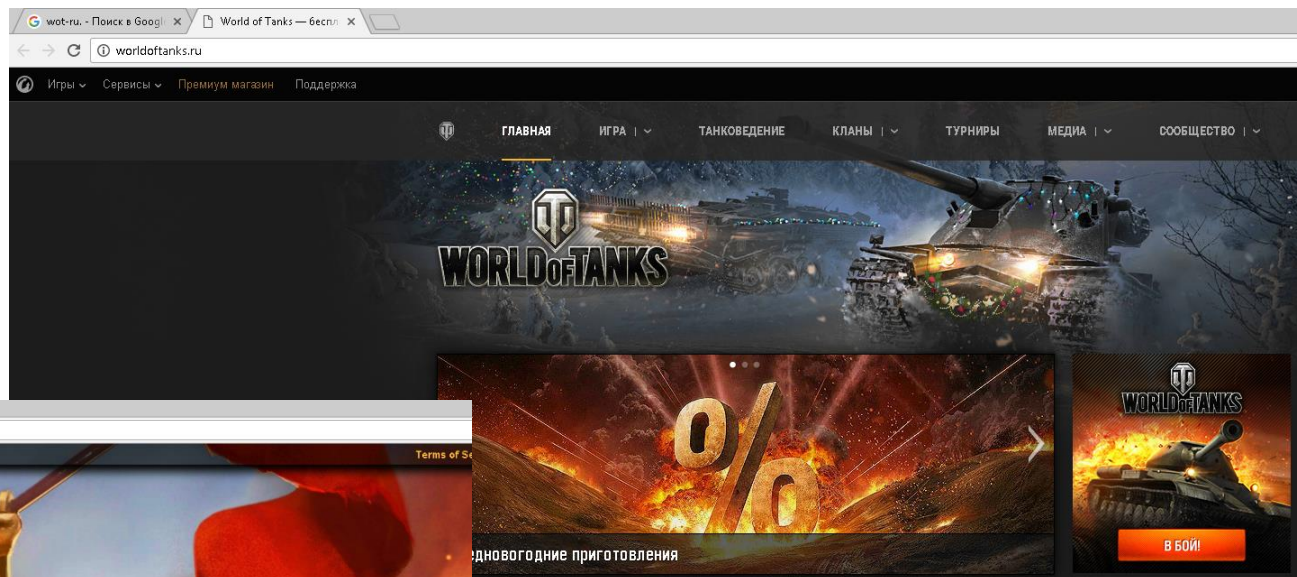
Документ	1	2	3	4	Итого	
Договор	11	6	2	4	23	
Коммерческое предложение	7	3	2	2	14	
САПР	6	1	3	1	3	14
Техническое задание	4	1	3	3	11	
Счет на оплату	3	3	1		7	

[Подробнее](#)

Пример расследования утечки



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 золота имперского весом 4,295 г? 0,005 в минус вроде вполне допустимо. И сколько будет стоить это золото? Интересует цена как одной монеты, так и небольшой партии.

4,31 г

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



**Есть вопросы?
Задавайте!**