

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Введение в конкурентную разведку

Примеры кейсов

Авдюнин Максим

«Перспективный мониторинг»

Наша деятельность

Мониторинг инцидентов ИБ



Тестирование на проникновение



Анализ защищённости ПО



Разработка ПО



Расследование инцидентов ИБ



Конкурентная разведка



Наша деятельность

Конкурентная разведка



Что такое конкурентная разведка?

Конкурентная разведка (далее КР) — сбор и обработка данных из открытых источников, для выработки управленческих решений с целью повышения конкурентоспособности коммерческой организации, проводимые в рамках закона и с соблюдением этических норм.

Целью КР в техническом понимании является получение максимального объёма релевантной информации об исследуемых объектах, установление взаимосвязей между ними и прочими выявленными в ходе проведения работ сущностями.

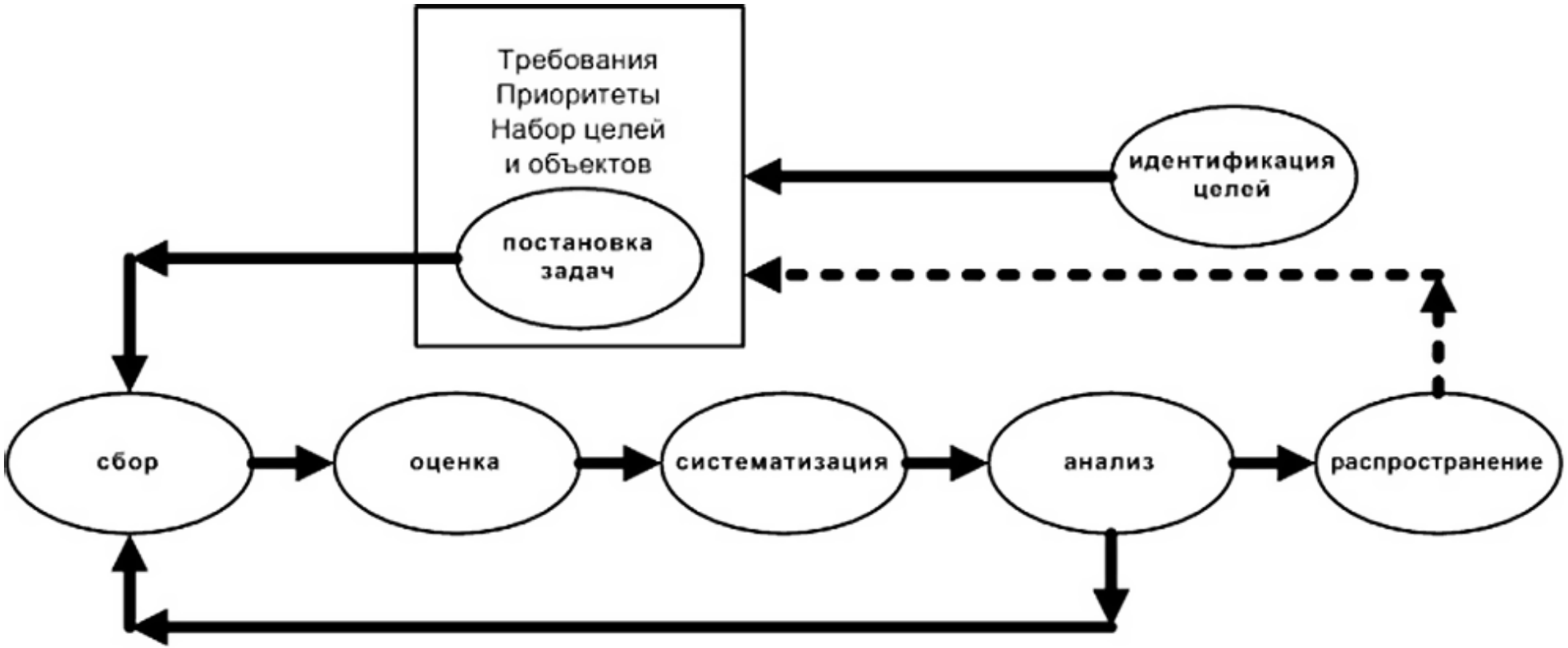
Задачи КР

Сбор данных в рамках КР служит целям заказчика и решает те или иные поставленные им задачи, в частности:

- Определение стратегии, потенциала и прочих свойств конкурентов.
- Проверка контрагентов, защита от мошеннических и других недружественных действий в отношении компании.
- Анализ рынка (ёмкости, насыщенности, динамики развития).
- Проведение маркетингового анализа и построение маркетинговой политики, создание образа бренда или продукта.
- Проведение расследований (фактов хищения, растраты, вывода денег компании за границу, утечек информации и т.д.).

Разведывательный цикл

Основные шаги при проведении конкурентной разведки:



Кейс 1
«На чистую воду»

Заказчик

Провайдер трекинговой информации о грузоперевозках

Описание инцидента

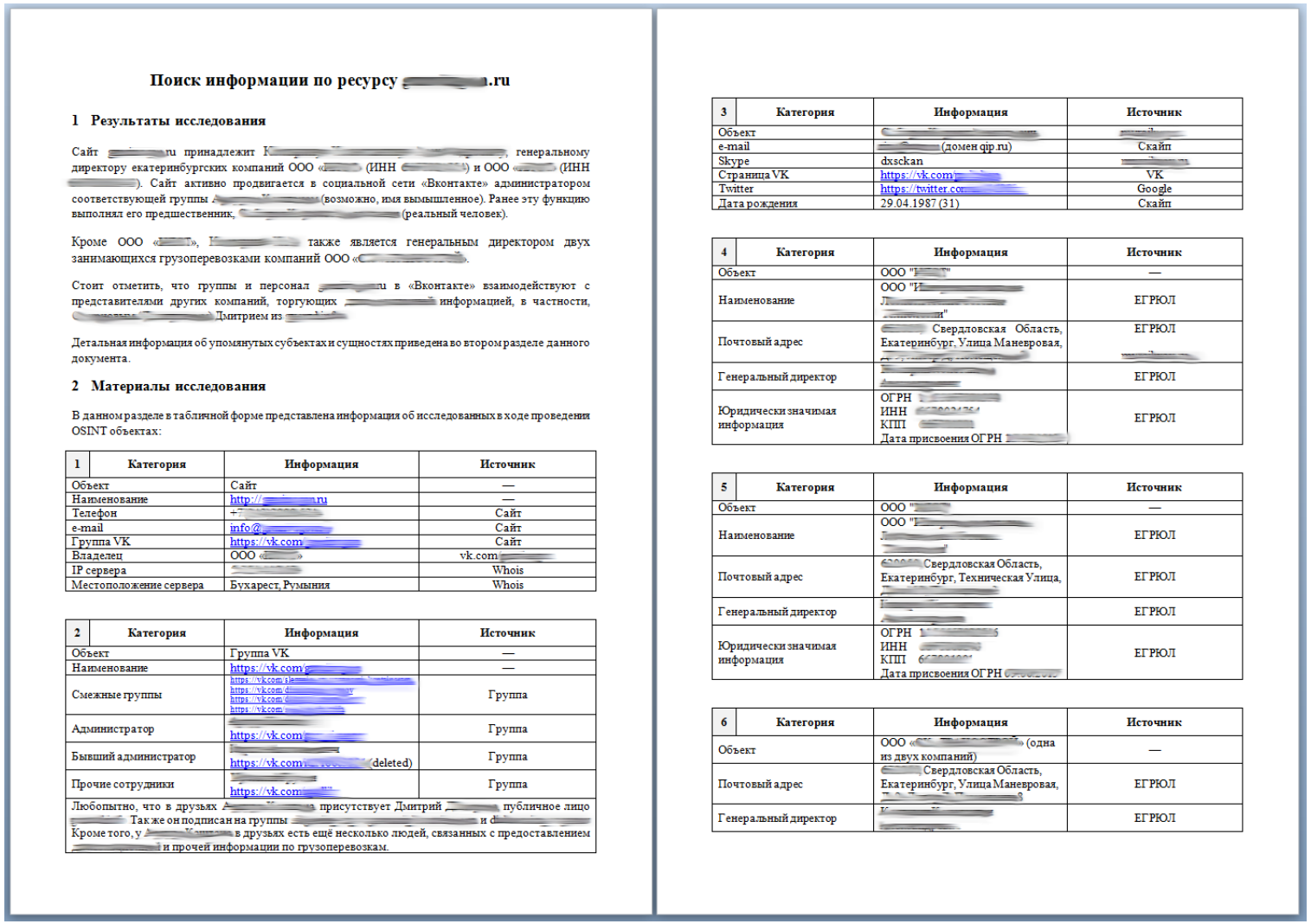
Ряд интернет-ресурсов предлагал информацию, распространяемую Заказчиком, на продажу, очевидно **получая её в обход официальных каналов**. Необходимо было установить, каким образом это происходило.

Расследование инцидента

В рамках проекта были проведены работы по конкурентной разведке и инструментальному исследованию указанных заказчиком сайтов. По их результатам были получены:

- Список аффилированных с исследуемыми сайтами лиц.
- Их персональные данные, контактная информация, социальные связи и т.д.
- Конфиденциальные сведения, в частности, юридические документы.

Сайт 1



Поиск информации по ресурсу [redacted].ru

1 Результаты исследования

Сайт [redacted].ru принадлежит К[redacted], генеральному директору екатеринбургских компаний ООО «[redacted]» (ИНН [redacted]) и ООО «[redacted]» (ИНН [redacted]). Сайт активно продвигается в социальной сети «Вконтакте» администратором соответствующей группы [redacted] (возможно, имя вымышленное). Ранее эту функцию выполнял его предшественник, [redacted] (реальный человек).

Кроме ООО «[redacted]», К[redacted] также является генеральным директором двух занимающихся грузоперевозками компаний ООО «[redacted]».

Стоит отметить, что группы и персонал [redacted].ru в «Вконтакте» взаимодействуют с представителями других компаний, торгующих [redacted] информацией, в частности, [redacted] Дмитрием из [redacted].

Детальная информация об упомянутых субъектах и сущностях приведена во втором разделе данного документа.

2 Материалы исследования

В данном разделе в табличной форме представлена информация об исследованных в ходе проведения OSINT объектах:

1	Категория	Информация	Источник
Объект		Сайт	—
Наименование		http://[redacted].ru	—
Телефон		+[redacted]	Сайт
e-mail		info@[redacted]	Сайт
Группа VK		https://vk.com/[redacted]	Сайт
Владелец		ООО «[redacted]»	vk.com/[redacted]
IP сервера		[redacted]	Whois
Местоположение сервера		Бухарест, Румыния	Whois

2	Категория	Информация	Источник
Объект		Группа VK	—
Наименование		https://vk.com/g[redacted]	—
Смежные группы		https://vk.com/[redacted] https://vk.com/[redacted] https://vk.com/[redacted] https://vk.com/[redacted]	Группа
Администратор		[redacted] https://vk.com/[redacted]	Группа
Бывший администратор		[redacted] https://vk.com/[redacted] (deleted)	Группа
Прочие сотрудники		[redacted] https://vk.com/[redacted]	Группа
Любопытно, что в друзьях [redacted] присутствует Дмитрий [redacted], публичное лицо [redacted]. Также он подписан на группы [redacted] и [redacted]. Кроме того, у [redacted] в друзьях есть ещё несколько людей, связанных с предоставлением [redacted] и прочей информации по грузоперевозкам.			

3	Категория	Информация	Источник
Объект		[redacted]	[redacted]
e-mail		[redacted] (домен qip.ru)	Скайп
Skype		dxsckan	[redacted]
Страница VK		https://vk.com/[redacted]	VK
Twitter		https://twitter.com/[redacted]	Google
Дата рождения		29.04.1987 (31)	Скайп

4	Категория	Информация	Источник
Объект		ООО "[redacted]"	—
Наименование		ООО "[redacted]"	ЕГРЮЛ
Почтовый адрес		[redacted] Свердловская Область, Екатеринбург, Улица Маневровая, [redacted]	ЕГРЮЛ
Генеральный директор		[redacted]	ЕГРЮЛ
Юридически значимая информация		ОГРН [redacted] ИНН [redacted] КПП [redacted] Дата присвоения ОГРН [redacted]	ЕГРЮЛ

5	Категория	Информация	Источник
Объект		ООО "[redacted]"	—
Наименование		ООО "[redacted]"	ЕГРЮЛ
Почтовый адрес		[redacted] Свердловская Область, Екатеринбург, Техническая Улица, [redacted]	ЕГРЮЛ
Генеральный директор		[redacted]	ЕГРЮЛ
Юридически значимая информация		ОГРН [redacted] ИНН [redacted] КПП [redacted] Дата присвоения ОГРН [redacted]	ЕГРЮЛ

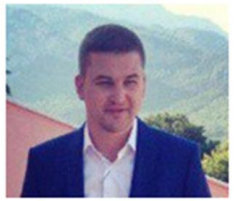
6	Категория	Информация	Источник
Объект		ООО «[redacted]» (одна из двух компаний)	—
Почтовый адрес		[redacted] Свердловская Область, Екатеринбург, Улица Маневровая, [redacted]	ЕГРЮЛ
Генеральный директор		[redacted]	ЕГРЮЛ

Сайт 1

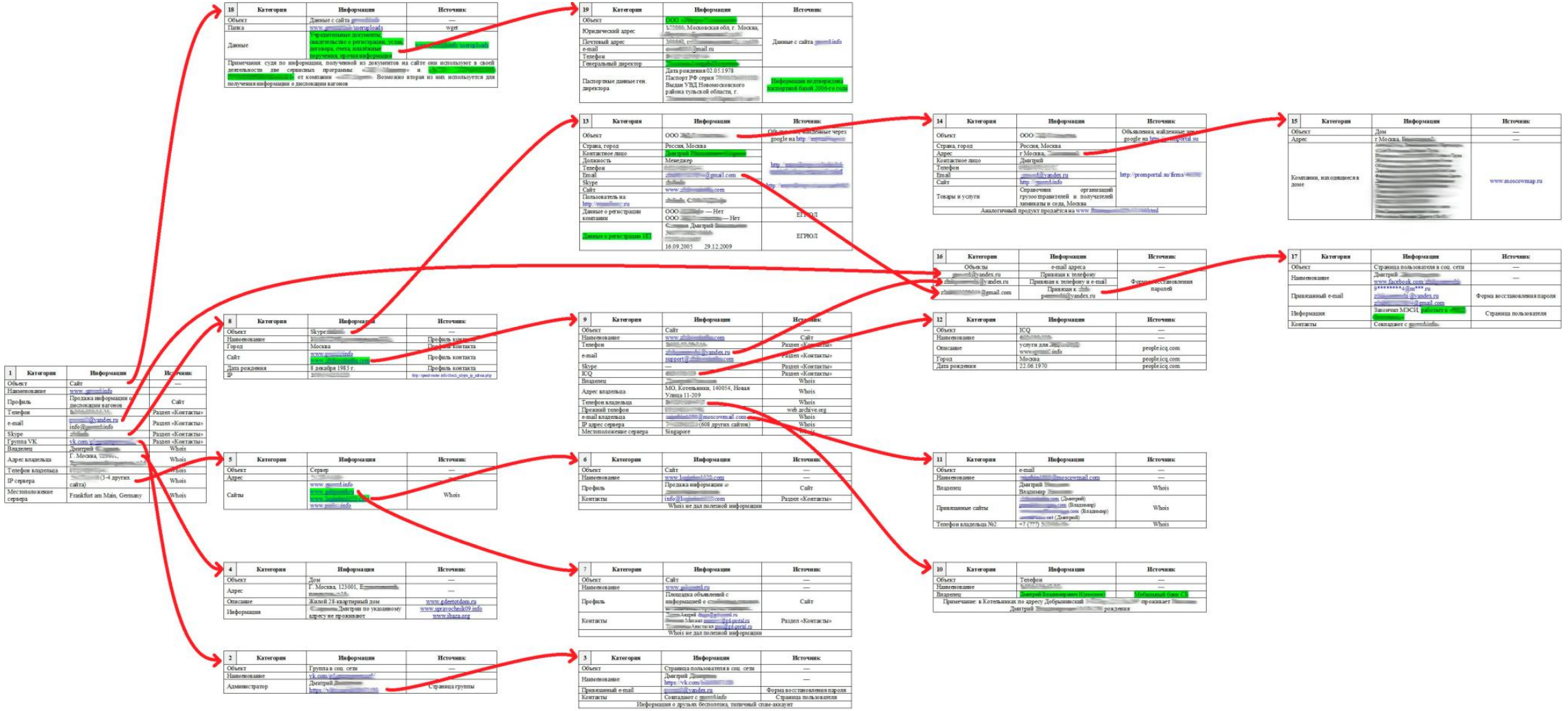
3 Команда сайта

Информация о нынешнем генеральном директоре ООО «[redacted]» найдена не была.

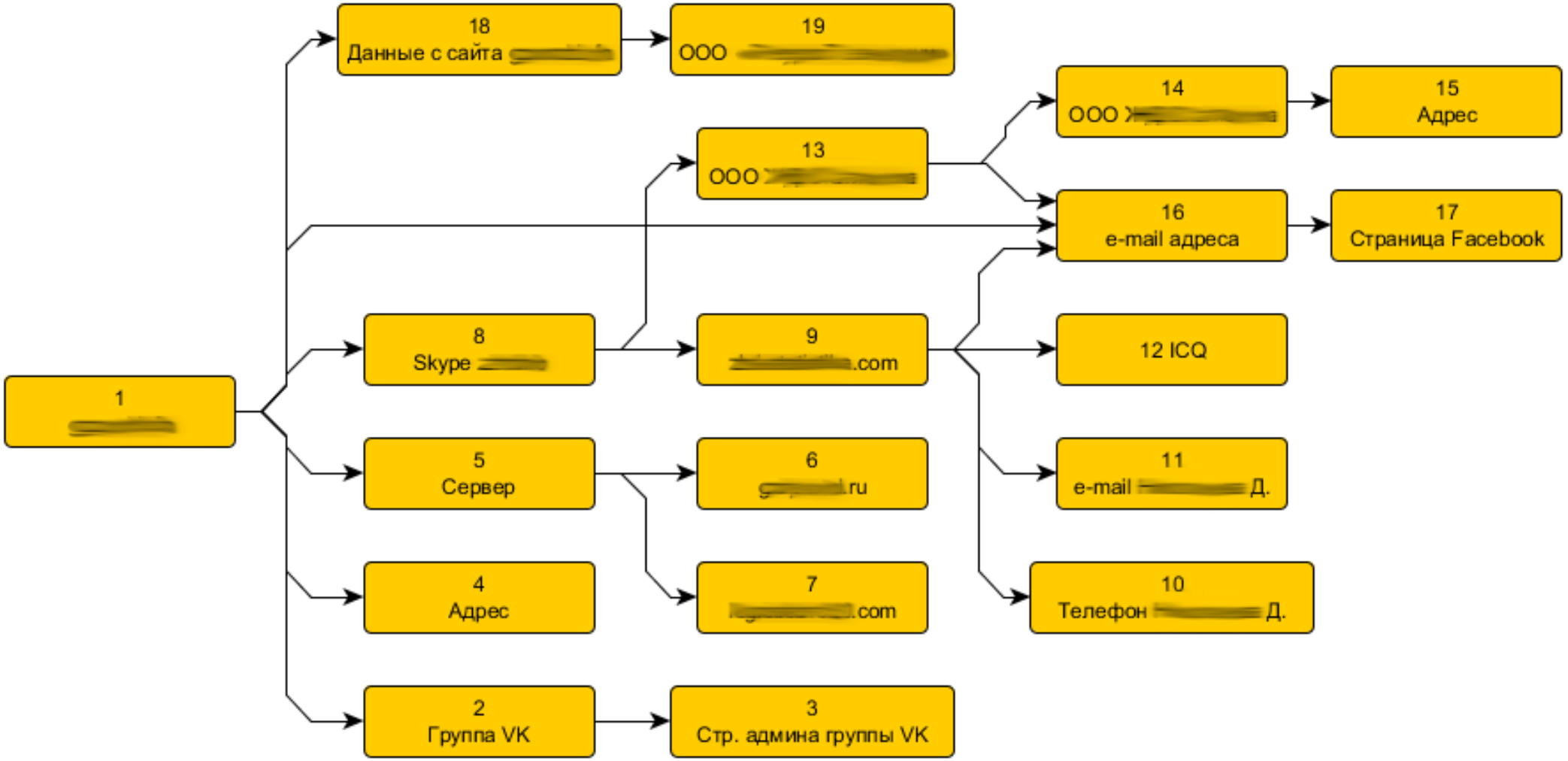
За организацию работы сайта [redacted] отвечают (или отвечали) следующие сотрудники ООО «[redacted]»:

1. [redacted] Генеральный директор (бывший)  vk.com/[redacted]	2. [redacted] Технический директор  https://vk.com/[redacted] (заморожена)	3. [redacted] Главный бухгалтер  (?)
4. [redacted] Бухгалтер  www.facebook.com/[redacted]	5 [redacted] Менеджер (по работе с клиентами)  vk.com[redacted]	6. [redacted] Менеджер  vk.com[redacted]
7. [redacted] Менеджер  vk.com/[redacted]	8. [redacted] Консультант (?)  vk.com/[redacted]	9. [redacted] Бывшая сотрудница ЗАО «[redacted]» (?)  vk.com/[redacted]

Сайт 2


1 Категория Информация Источник
Объект Сайт —
Наименование www.[redacted].info
Профиль Продажа информации о дислокации вагонов Сайт
Телефон [redacted] Раздел «Контакты»
e-mail [redacted]@yandex.ru Раздел «Контакты»
info@[redacted].info
Skype [redacted] Раздел «Контакты»
Группа VK vk.com/[redacted] Раздел «Контакты»
Владелец Дмитрий [redacted] Whois
Адрес владельца Г. Москва, [redacted] Whois
Телефон владельца [redacted] Whois
IP сервера [redacted] (3-4 других сайта) Whois
Местоположение сервера Frankfurt am Main, Germany Whois
18 Категория Информация Источник
Объект Данные с сайта [redacted].info —
Папка www.[redacted].info/upload/ wget
Данные Учредительные документы, свидетельство о регистрации, устав, договора, счета, платежные поручения, прочая информация www.[redacted].info/upload/
Примечание: судя по информации, полученной из документов на сайте они используют в своей деятельности две сервисных программы: «[redacted]» и «[redacted]» от компании [redacted]. Возможно вторая из них используется для получения информации о дислокации вагонов
19 Категория Информация Источник
Объект ООО [redacted] Данные с сайта [redacted].info
Юридический адрес [redacted], Московская обл, г. Москва, [redacted]
Почтовый адрес [redacted]
e-mail [redacted]@mail.ru
Телефон [redacted]
Генеральный директор [redacted]
Паспортные данные ген. директора Дата рождения 02.05.1978
Паспорт РФ серия [redacted]
Выдан УВД Новомосковского района тульской области, г. [redacted]
Информация подтверждена паспортной базой 2006-го года
13 Категория Информация Источник
Объект ООО [redacted] Объявления, найденные через google на http://[redacted]
Страна, город Россия, Москва
Контактное лицо Дмитрий [redacted]
Должность Менеджер http://[redacted]
Телефон [redacted]
Email [redacted]@gmail.com
Skype [redacted]
Сайт www.[redacted].com http://[redacted]
Пользователь на http://[redacted].ru [redacted]
Данные о регистрации компании ООО [redacted] — Нет
ООО [redacted] — Нет ЕГРЮЛ
Данные о регистрации ИП [redacted] Дмитрий [redacted] ЕГРЮЛ
16.09.2005 29.12.2009
14 Категория Информация Источник
Объект ООО [redacted] Объявления, найденные через google на http://promportal.su
Страна, город Россия, Москва
Адрес г Москва, [redacted]
Контактное лицо Дмитрий
Телефон [redacted]
Email [redacted]@yandex.ru http://promportal.su/firms/[redacted]
Сайт http://[redacted].info
Товары и услуги Справочник организаций грузоотправителей и получателей химикаты и сода, Москва
Аналогичный продукт продается на www.[redacted].html
15 Категория Информация Источник
Объект Дом —
Адрес г Москва, [redacted] —
Компании, находящиеся в доме [redacted] www.moscowmap.ru
16 Категория Информация Источник
Объекты e-mail адреса —
[redacted]@yandex.ru Привязан к телефону
[redacted]@yandex.ru Привязан к телефону и e-mail Форма восстановления паролей
[redacted]@gmail.com Привязан к [redacted] pennmobil@yandex.ru
17 Категория Информация Источник
Объект Страница пользователя в соц. сети —
Наименование Дмитрий [redacted] www.facebook.com/[redacted] —
Привязанный e-mail [redacted]@yandex.ru
[redacted]@gmail.com Форма восстановления пароля
Информация Закончил МЭСИ, работает в [redacted] Страница пользователя
Контакты Совпадают с [redacted].info
8 Категория Информация Источник
Объект Skype: [redacted] —
Наименование [redacted] Профиль контакта
Город Москва Профиль контакта
Сайт www.[redacted].info
www.[redacted].com Профиль контакта
Дата рождения 8 декабря 1983 г. Профиль контакта
IP [redacted] http://geoiptool.com/ru/?IP=[redacted]
9 Категория Информация Источник
Объект Сайт —
Наименование www.[redacted].com Сайт
Телефон [redacted] Раздел «Контакты»
e-mail [redacted]@yandex.ru
support@[redacted].com Раздел «Контакты»
Skype — Раздел «Контакты»
ICQ [redacted] Раздел «Контакты»
Владелец [redacted] Whois
Адрес владельца МО, Котельники, 140054, Новая Улица 11-209 Whois
Телефон владельца [redacted] Whois
Прежний телефон [redacted] web.archive.org
e-mail владельца [redacted]@moscowmail.com Whois
IP адрес сервера [redacted] (608 других сайтов) Whois
Местоположение сервера Singapore Whois
12 Категория Информация Источник
Объект ICQ —
Наименование [redacted] —
Описание услуги для [redacted] www.[redacted].info people.icq.com
Город Москва people.icq.com
Дата рождения 22.06.1970 people.icq.com
5 Категория Информация Источник
Объект Сервер —
Адрес [redacted] —
Сайты www.[redacted].info
www.[redacted].com
www.[redacted].info Whois
6 Категория Информация Источник
Объект Сайт —
Наименование www.[redacted].com —
Профиль Продажа информации о [redacted] Сайт
Контакты info@[redacted].com Раздел «Контакты»
Whois не дал полезной информации
11 Категория Информация Источник
Объект e-mail —
Наименование [redacted]@moscowmail.com —
Владелец Дмитрий [redacted]
Владимир [redacted] Whois
Привязанные сайты [redacted].com (Дмитрий)
[redacted].com (Владимир)
[redacted].com (Владимир)
[redacted].net (Дмитрий) Whois
Телефон владельца №2 +7 (777) [redacted] Whois
4 Категория Информация Источник
Объект Дом —
Адрес Г. Москва, 123001, [redacted] —
Описание Жилой 28-квартирный дом www.gdetotdom.ru
Информация [redacted] Дмитрии по указанному адресу не проживают www.spravochnik09.info
www.ibaza.org
7 Категория Информация Источник
Объект Сайт —
Наименование www.[redacted].ru —
Профиль Площадка объявлений с информацией о [redacted] Сайт
Контакты [redacted] Раздел «Контакты»
Whois не дал полезной информации
10 Категория Информация Источник
Объект Телефон —
Наименование [redacted] —
Владелец Дмитрий Владимирович Новиков Мобильный банк СБ
Примечание: в Котельниках по адресу Добрынинский [redacted] проживает Дмитрий [redacted] рождения
2 Категория Информация Источник
Объект Группа в соц. сети —
Наименование vk.com/[redacted] —
Администратор Дмитрий [redacted] Страница группы
https://vk.com/[redacted]
3 Категория Информация Источник
Объект Страница пользователя в соц. сети —
Наименование Дмитрий [redacted] https://vk.com/[redacted] —
Привязанный e-mail [redacted]@yandex.ru Форма восстановления пароля
Контакты Совпадают с [redacted].info Страница пользователя
Информация о друзьях бесполезна, типичный спам-аккаунт

Сайт 2


18
Данные с сайта
19
ООО
14
ООО
15
Адрес
13
ООО
16
e-mail адреса
17
Страница Facebook
1
8
Skype
9
.com
12 ICQ
5
Сервер
6
.ru
11
e-mail
Д.
4
Адрес
7
.com
10
Телефон
Д.
2
Группа VK
3
Стр. админа группы VK

Кейс 2
«Некачественная доставка»

Заказчик

Крупная логистическая компания

Описание инцидента

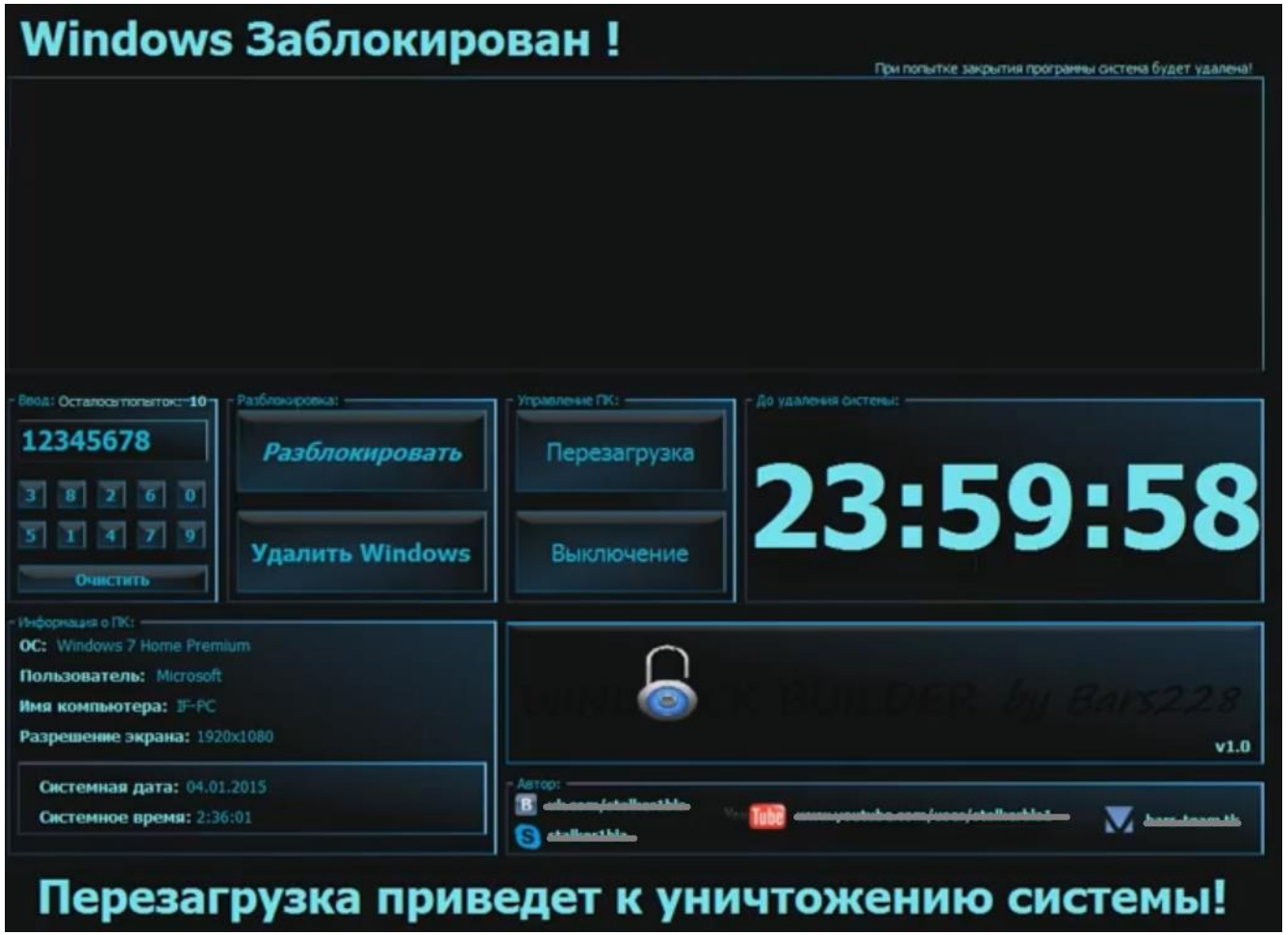
Сотрудникам компании были направлены поддельные **письма со ссылкой на фишинговый ресурс**, копирующий официальный сайт компании. В тексте письма предлагалось скачать с данного ресурса некий исполняемый файл и документ «Инструкция.docx».

Грамотные действия службы информационной безопасности заказчика позволили обнаружить подозрительную активность и привлечь к её расследованию специалистов ЗАО «ПМ».

Расследование инцидента

Несмотря на недоступность на момент исследования фишингового сайта был найден и проанализирован рассылаемый **файл**.

Его проверка на сайте virustotal.com показала, что по оценке 39 из 57 антивирусов он содержит троянскую программу **Trojan.Win32.Diztakun** — ransomware-вирус, предлагавший пользователю перевести деньги на указанный адрес под угрозой уничтожения операционной системы в ином случае.



Ссылка с сайта на документ «Инструкция.docx» в свою очередь вела на сервис **Dropbox** и документ удалось успешно скачать. Его содержимое представляло собой повторяющуюся последовательность бессмысленных символов, а сам документ не представлял угрозы.

Однако, в свойствах документа был указан **никнейм** его автора.

Поиск по нему выдал ряд сайтов, на которых был зарегистрирован соответствующий пользователь. Среди них оказалось множество **ресурсов хакерской и мошеннической направленности** (например, forum.benderbay.com, fuckav.ru), а так же социальная сеть **«В контакте»** и несколько **личных сайтов** злоумышленника.

Их анализ позволил собрать достаточное количество информации для деанонимизации устроившего атаку хакера.

Кейс 3
«Как всё устроено»

Заказчик

Крупная страховая компания

Постановка задачи

Провести поиск по открытым источникам **потенциально ценной для нарушителя информации** и данных, которые он сможет в дальнейшем использовать для **претекстинга** (социоинженерной атаки, предполагающей имперсонификацию нарушителем сотрудников компании или контрагентов с целью получения конфиденциальной информации или нарушения работы компании с помощью полученных ранее знаний о её деятельности и структуре).

Работы

В рамках выполнения задачи по отношении к компании Заказчика была проведена конкурентная разведка и инструментальный анализ его сайта.

Источники информации

- Сайты компании
- Поисковики
- Сайты с отзывами сотрудников о компании (antijob.net и т.п.)
- Архив вакансий компании (*“на позицию PPP в отдел BBB управления DDD требуется …”*)
- Пресс-релизы и новости компании (*“начальник департамента DDD NNN заявил, что…”*)
- СМИ

Результаты

Частично восстановлена структура компании:



Результаты

Частично восстановлена структура компании:



Собрана информация о сотрудниках:

ФИО	Должность	Департамент	Управление	Отдел	Телефон	Электронная почта
[illegible]	Генеральный директор, председатель Правления	—	—	—		
[illegible]	Первый заместитель Генерального директора по развитию и продажам	—	—	—		
[illegible]	Первый заместитель Генерального директора, финансовый директор	—	—	—		
[illegible]	Заместитель Генерального директора, директор Д.а	Д. анализа рисков	—	—		
[illegible]	Заместитель Генерального директора, директор Д.а	Д. клиентского сопровождения	—	—		
		Д. по работе с персоналом				[illegible]
[illegible]	Заместитель Генерального директора, директор Д.а	Д. розничных продаж	—	—		
[illegible]	Заместитель Генерального директора – директор Д.а страхования корпоративных рисков	Д. страхования корпоративных рисков	—	—		
[illegible]	Начальник отдела	Д. страхования корпоративных рисков	У. страхования непромышленных рисков	О. личного страхования	[illegible]	[illegible]
[illegible]	Начальник управления	Д. страхования корпоративных рисков	У. страхования непромышленных рисков	—	[illegible]	[illegible]
[illegible]	Начальник отдела	Д. страхования корпоративных рисков	У. страхования непромышленных рисков	О. страхования имущества и ответственности	[illegible]	[illegible]
[illegible]	Заместитель начальника отдела	Д. страхования корпоративных рисков	У. страхования непромышленных рисков	О. страхования корпоративного автотранспорта	[illegible]	[illegible]
[illegible]	Управляющий директор по страхованию строительных рисков управления	Д. страхования корпоративных рисков	У. страхования непромышленных рисков	—	[illegible]	[illegible]
[illegible]	Управляющий директор отдела	Д. страхования корпоративных рисков	У. страхования непромышленных рисков	О. страхования имущества и ответственности	[illegible]	[illegible]
[illegible]	Руководитель направления отдела	Д. страхования корпоративных рисков	У. страхования непромышленных рисков	О. страхования имущества и ответственности	[illegible]	[illegible]
[illegible]	Директор Д.а страховых и информационных технологий	Д. страховых и информационных технологий	—	—		
[illegible]	Начальник управления		Операционное У.	—		
[illegible]	Начальник управления		У. внешних коммуникаций	—	[illegible]	[illegible]
[illegible]	Начальник управления		У. перестрахования	—	[illegible]	[illegible]
[illegible]	Начальник отдела		У. перестрахования	О. облигаторного перестрахования	[illegible]	[illegible]
[illegible]	Руководитель направления отдела		У. перестрахования	О. облигаторного перестрахования	[illegible]	[illegible]
[illegible]	Руководитель направления отдела		У. перестрахования	О. облигаторного перестрахования	[illegible]	[illegible]
[illegible]	Главный специалист отдела		У. перестрахования	О. факультативного перестрахования	[illegible]	[illegible]
[illegible]	Главный специалист отдела		У. перестрахования	О. факультативного перестрахования	[illegible]	[illegible]
[illegible]	Начальник отдела		У. перестрахования	О. факультативного перестрахования	[illegible]	[illegible]
[illegible]	Начальник управления		У. страхования предприятий среднего бизнеса	—	[illegible]	[illegible]
[illegible]	Руководитель направления управления		У. страхования предприятий среднего бизнеса	—	[illegible]	[illegible]
[illegible]	Руководитель направления управления		У. страхования предприятий среднего бизнеса	—	[illegible]	[illegible]
[illegible]	Управляющий директор управления страхования промышленных рисков		У. страхования промышленных рисков	—	[illegible]	[illegible]
[illegible]	Зам. начальника управления		У. страхования промышленных рисков	—	[illegible]	[illegible]
[illegible]	Управляющий директор управления		У. страхования промышленных рисков		[illegible]	[illegible]
[illegible]	Заместитель начальника управления страхования специальных рисков		У. страхования специальных рисков	—	[illegible]	[illegible]
[illegible]	Руководитель направления управления		У. страхования специальных рисков	—	[illegible]	[illegible]
[illegible]	Начальник отдела			О. закупок	[illegible]	[illegible]
[illegible]	Главный бухгалтер					

Кейс 4
«Шекспировские страсти»

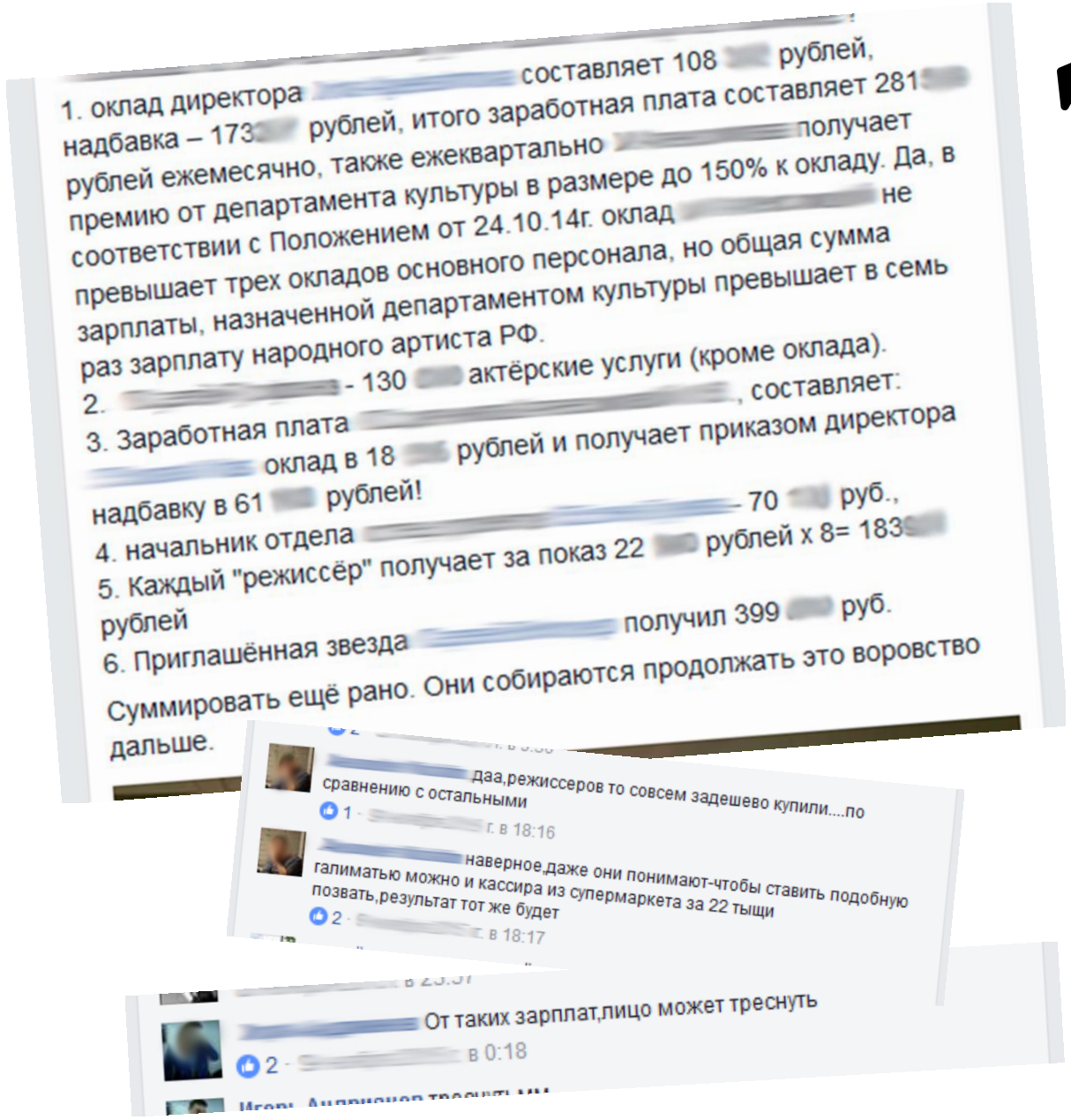
Заказчик

Организация из мира шоу-бизнеса

Описание инцидента

Злоумышленник из числа сотрудников передал третьим лицам информацию о заработной плате руководства, публикация которой привела к росту напряжённости в коллективе и негативной прессе.

Целью работ стало выяснение источника утечки и, в идеале, установление виновного.



Расследование инцидента

На первом этапе работ были **проанализированы опубликованные материалы** и составлен список потенциальных подозреваемых.

После чего был проведён ряд классических мероприятий по **форензике**. Созданы дисковых копии АРМ подозреваемых, произведён рекурсивный поиск исходной информации, сделаны предположения по возможным каналам утечки.

Кроме того, анализ открытых источников показал, что часть выложенной информации на самом деле не конфиденциальна, но **была опубликована ранее** в соответствии с законом о гос. закупках.

По результатам работ **были установлены источники информации, составившие утечку**, сформирован список подозреваемых, предложены описания возможных каналов утечки и выработаны рекомендации по их ликвидации.

Кейс 5
«Плохие новости»

Заказчик

Государственный подрядчик

Постановка задачи

Провести тестирование на проникновение в режиме «чёрного ящика»

Работы

Классическое тестирование на проникновение не дало результатов, поэтому в рамках проекта была проведена **фишинг-атака** на компанию заказчика, в ходе которой сотрудникам было отправлено 2 “новостных” письма, содержащих ссылки на скрипт, перехватывающий аутентификационные данные пользователей соответствующих машин.

Результаты

- Более половины сотрудников прошло хотя бы по одной ссылке
- Никто из них не сообщил об инциденте в службу ИБ заказчика
- Исследователями был получен полный доступ к IT-инфраструктуре заказчика
- Действия службы ИБ заказчика протоколировались, протокол был включён в состав отчёта

Кейс 6
«Опасная утечка»

Заказчик

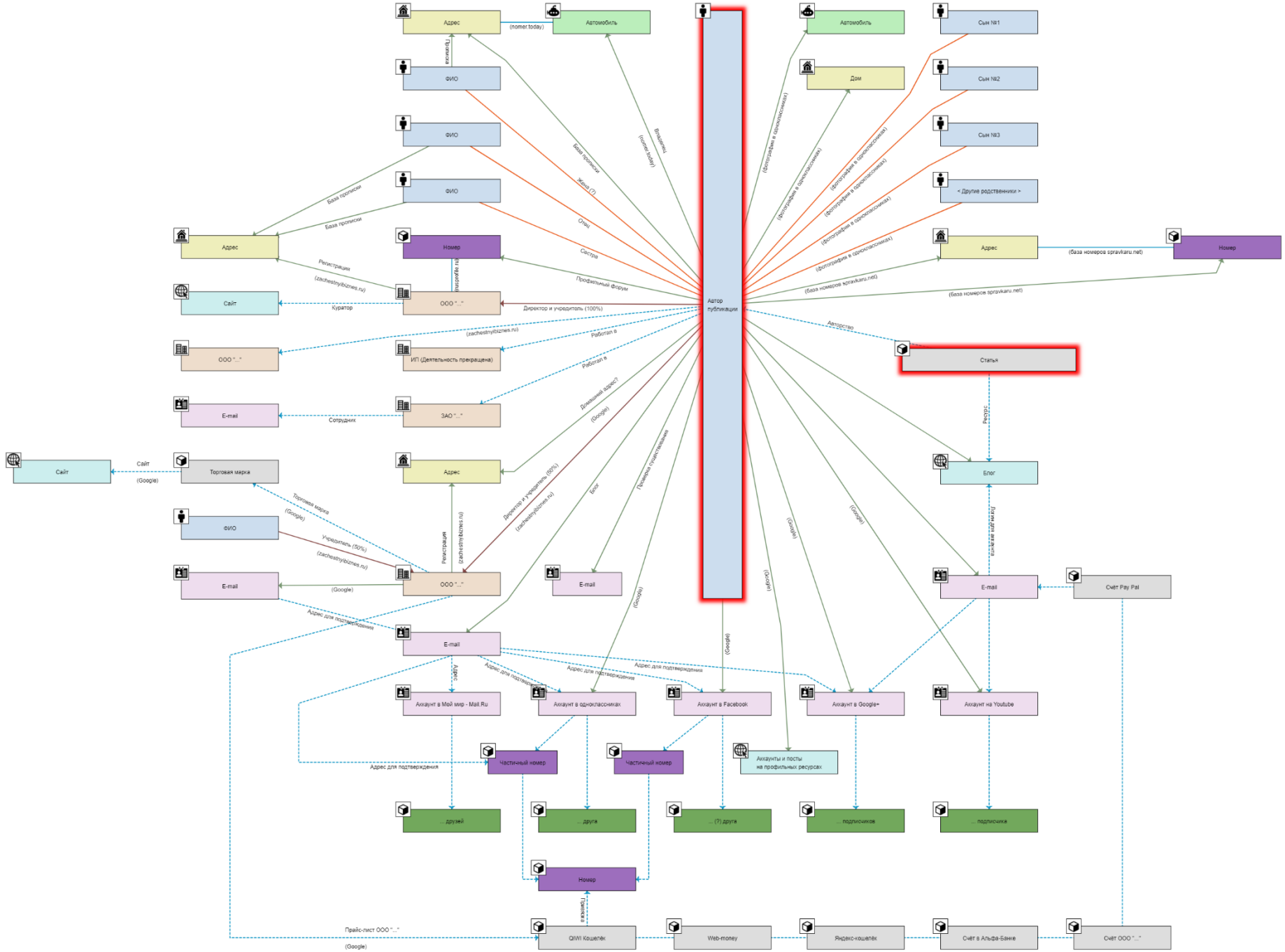
Крупная промышленная компания

Постановка задачи

В крупной промышленной компании произошла **утечка финансовой информации**, в частности, списка клиентов и сумм контрактов. Информация была опубликована в крайне негативном ключе в профильном блоге и растиражирована СМИ.

Работы

Был проведён поиск информации об авторе публикации, содержащей конфиденциальные сведения заказчика, проверено наличие у него связей с сотрудниками компании, собраны сведения личного характера.


Адрес
(nomer.today)
Автомобиль
Автомобиль
Сын №1
Сын №2
Сын №3
Дом
< Другие родственники >
ФИО
ФИО
ФИО
Проживал
База прописки
База прописки
Жена (?)
Отец
Сестра
Владелец
(nomer.today)
(фотография в одноклассниках)
(фотография в одноклассниках)
(фотография в одноклассниках)
(фотография в одноклассниках)
(фотография в одноклассниках)
Автор публикации
Адрес
Номер
(база номеров spravkaru.net)
Номер
Адрес
Регистрация
(zachestnyibiznes.ru)
Профильный форум
(база номеров spravkaru.net)
(база номеров spravkaru.net)
Сайт
Куратор
ООО "..."
Директор и учредитель (100%)
(zachestnyibiznes.ru)
Авторство
ООО "..."
ИП (Деятельность прекращена)
Работал в
Работал в
Статья
E-mail
Сотрудник
ЗАО "..."
Домашний адрес?
(Google)
Ресурс
Сайт
Сайт
(Google)
Торговая марка
Адрес
Блог
Торговая марка
(Google)
ФИО
Учредитель (50%)
(zachestnyibiznes.ru)
Регистрация
(zachestnyibiznes.ru)
Директор и учредитель (50%)
(zachestnyibiznes.ru)
Блог
Привязка существования
Для активации
E-mail
(Google)
ООО "..."
E-mail
E-mail
Счёт Pay Pal
(Google)
(Google)
(Google)
(Google)
Адрес для подтверждения
E-mail
Адрес для подтверждения
Адрес для подтверждения
Адрес для подтверждения
Адрес для подтверждения
Аккаунт в Мой мир - Mail.Ru
Аккаунт в одноклассниках
Аккаунт в Facebook
Аккаунт в Google+
Аккаунт на Youtube
Частичный номер
Частичный номер
Аккаунты и посты на профильных ресурсах
Адрес для подтверждения
... друзей
... друга
... (?) друга
... подписчиков
... подписчика
Номер
Привязка
Прайс-лист ООО "..."
(Google)
QIWI Кошелёк
Web-money
Яндекс-кошелёк
Счёт в Альфа-Банке
Счёт ООО "..."

Кейс 7
«В особо крупном размере»

Заказчик

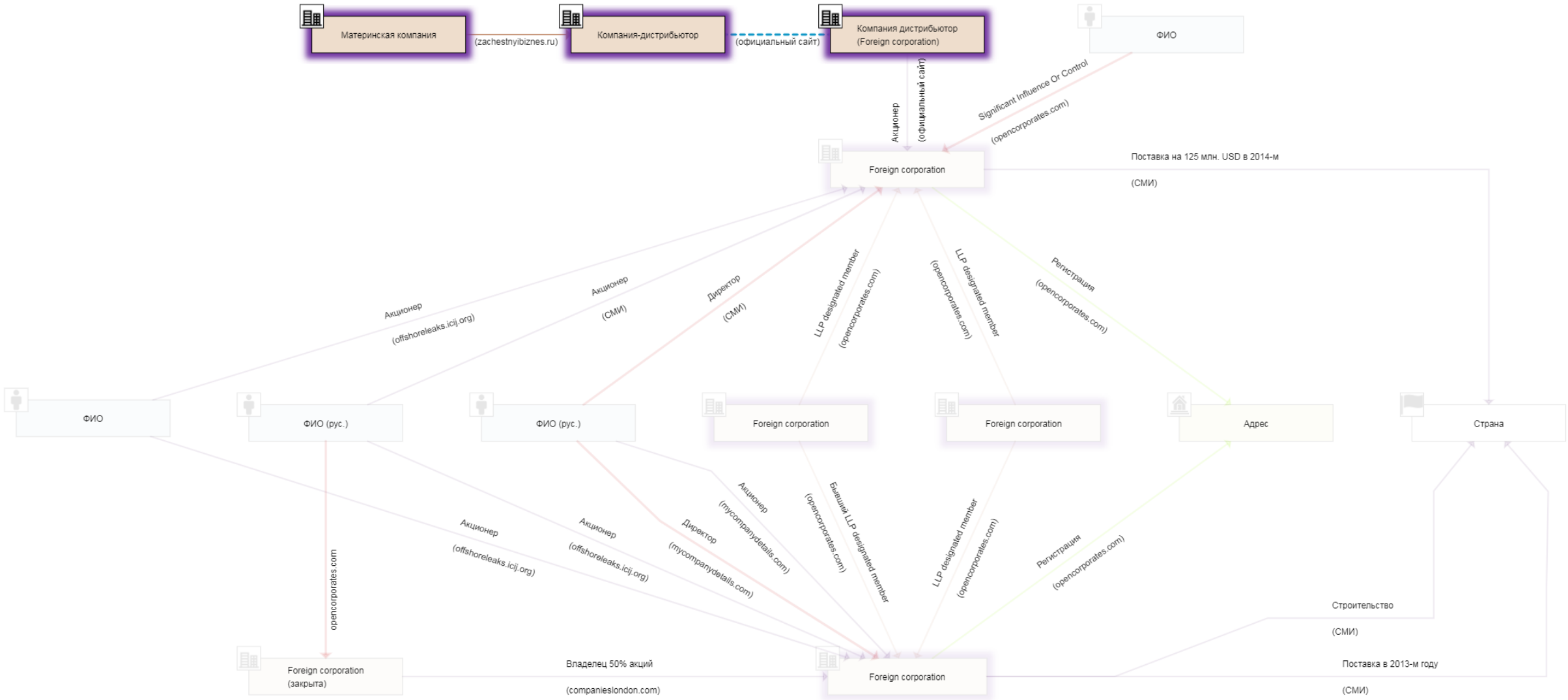
Крупная промышленная компания

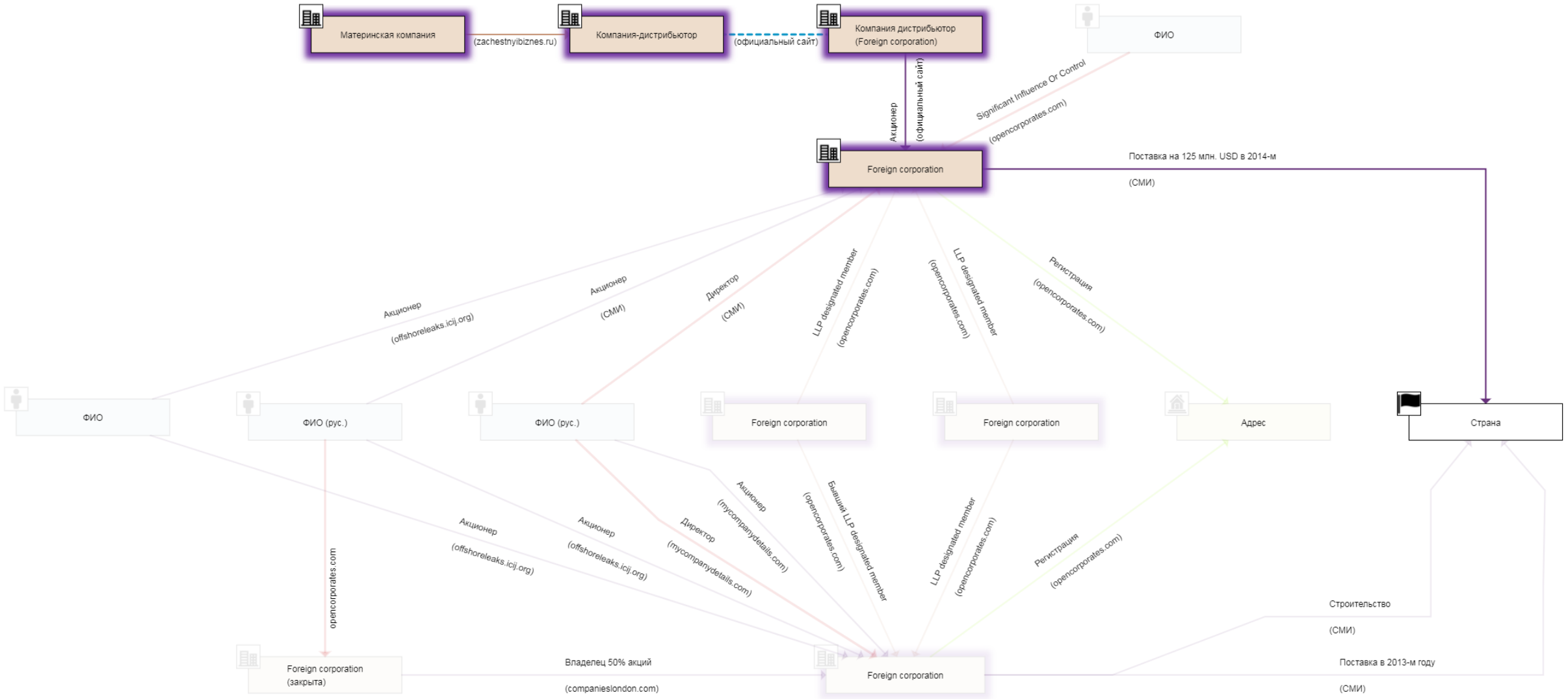
Постановка задачи

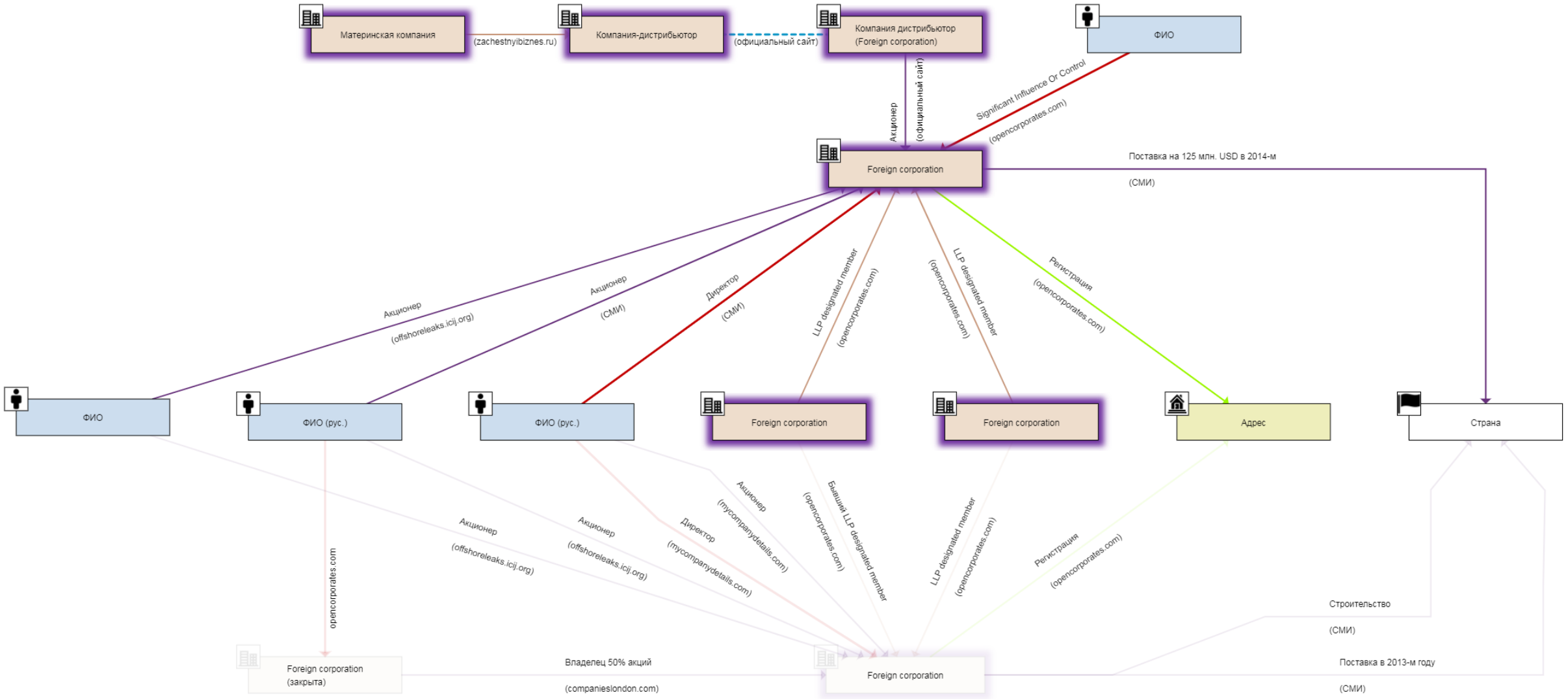
У руководства крупной промышленной компании возник **ряд вопросов относительно прозрачности бизнеса** своего дочернего предприятия, компании-дистрибьютора, отвечающей за реализацию продукции в одной из стран СНГ.

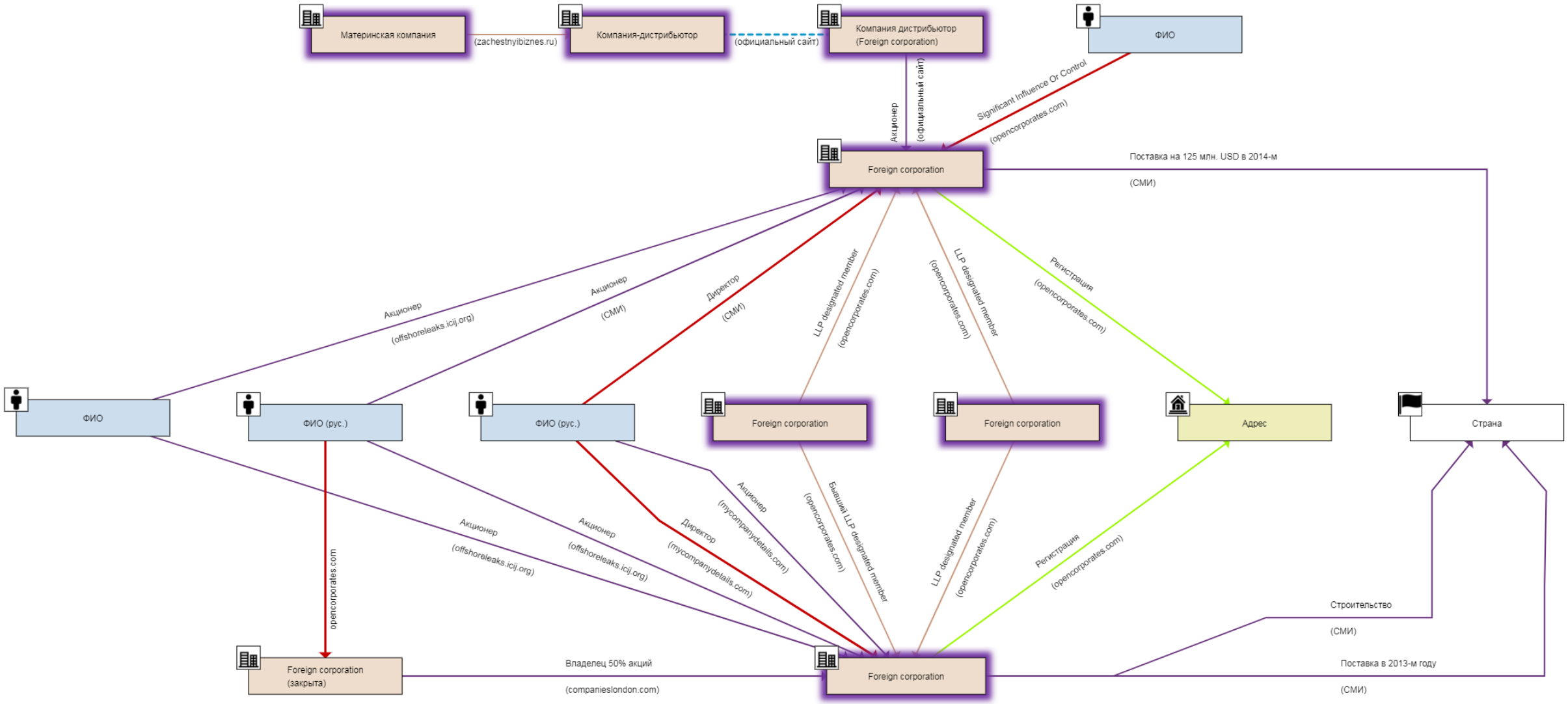
Работы

Был проведён поиск информации о деятельности искомой компании и её иностранных филиалов с целью обнаружения фактов, достаточных для инициации внутреннего расследования.

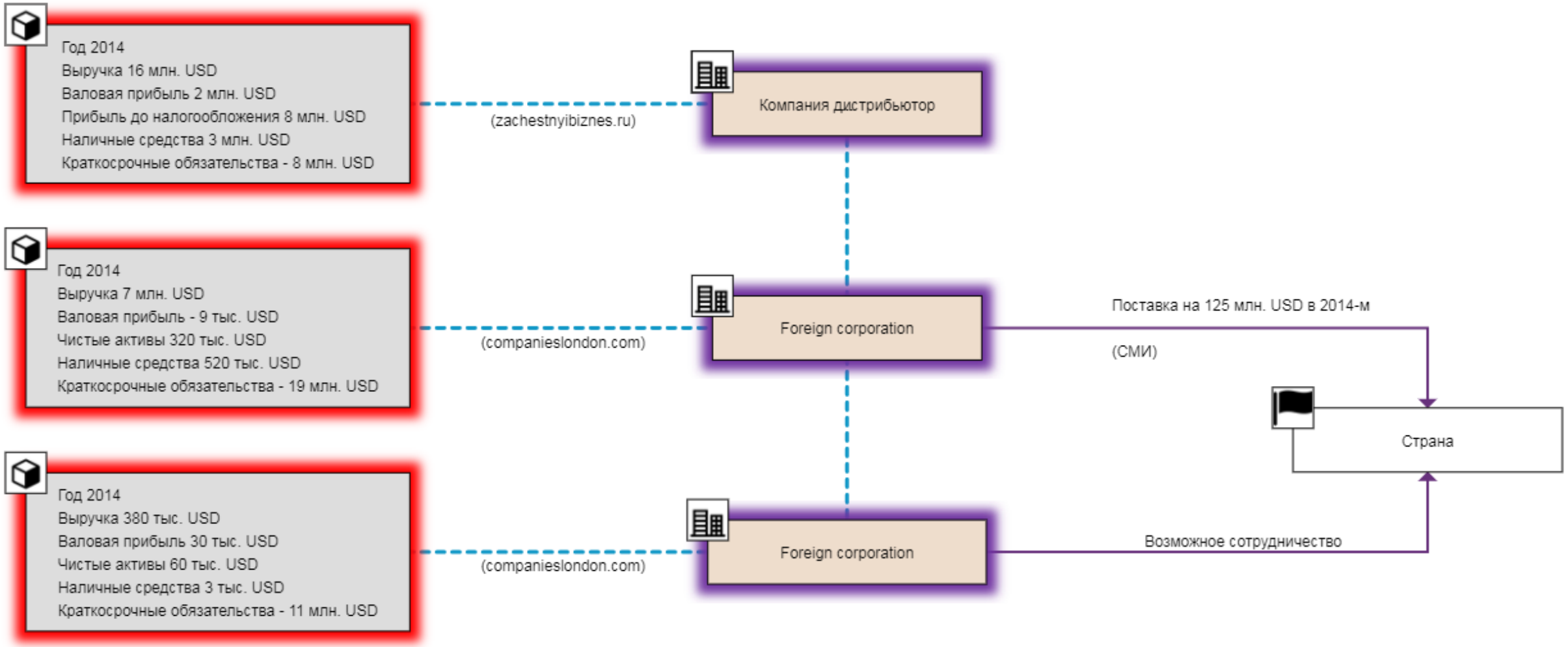

Материнская компания
(zachestnyibiznes.ru)
Компания-дистрибьютор
(официальный сайт)
Компания дистрибьютор
(Foreign corporation)
ФИО
Акционер
(официальный сайт)
Significant Influence Or Control
(opencorporates.com)
Foreign corporation
Поставка на 125 млн. USD в 2014-м
(СМИ)
Акционер
(offshoreleaks.icij.org)
Акционер
(СМИ)
Директор
(СМИ)
LLP designated member
(opencorporates.com)
LLP designated member
(opencorporates.com)
Регистрация
(opencorporates.com)
ФИО
ФИО (рус.)
ФИО (рус.)
Foreign corporation
Foreign corporation
Адрес
Страна
Акционер
(offshoreleaks.icij.org)
Акционер
(offshoreleaks.icij.org)
Директор
(mycompanydetails.com)
Акционер
(mycompanydetails.com)
Бывший LLP designated member
(opencorporates.com)
LLP designated member
(opencorporates.com)
Регистрация
(opencorporates.com)
opencorporates.com
Строительство
(СМИ)
Foreign corporation
(закрыта)
Владелец 50% акций
(companieslondon.com)
Foreign corporation
Поставка в 2013-м году
(СМИ)


Материнская компания
(zachestnyibiznes.ru)
Компания-дистрибьютор
(официальный сайт)
Компания дистрибьютор
(Foreign corporation)
ФИО
Акционер
(официальный сайт)
Significant Influence Or Control
(opencorporates.com)
Foreign corporation
Поставка на 125 млн. USD в 2014-м
(СМИ)
Акционер
(offshoreleaks.icij.org)
Акционер
(СМИ)
Директор
(СМИ)
LLP designated member
(opencorporates.com)
LLP designated member
(opencorporates.com)
Регистрация
(opencorporates.com)
ФИО
ФИО (рус.)
ФИО (рус.)
Foreign corporation
Foreign corporation
Адрес
Страна
Акционер
(offshoreleaks.icij.org)
Акционер
(offshoreleaks.icij.org)
Директор
(mycompanydetails.com)
Акционер
(mycompanydetails.com)
Бывший LLP designated member
(opencorporates.com)
LLP designated member
(opencorporates.com)
Регистрация
(opencorporates.com)
opencorporates.com
Строительство
(СМИ)
Foreign corporation
(закрыта)
Владелец 50% акций
(companieslondon.com)
Foreign corporation
Поставка в 2013-м году
(СМИ)


Материнская компания
(zachestnyibiznes.ru)
Компания-дистрибьютор
(официальный сайт)
Компания дистрибьютор
(Foreign corporation)
ФИО
Акционер
(официальный сайт)
Significant Influence Or Control
(opencorporates.com)
Foreign corporation
Поставка на 125 млн. USD в 2014-м
(СМИ)
Акционер
(offshoreleaks.icij.org)
Акционер
(СМИ)
Директор
(СМИ)
LLP designated member
(opencorporates.com)
LLP designated member
(opencorporates.com)
Регистрация
(opencorporates.com)
ФИО
ФИО (рус.)
ФИО (рус.)
Foreign corporation
Foreign corporation
Адрес
Страна
Акционер
(offshoreleaks.icij.org)
Акционер
(offshoreleaks.icij.org)
Директор
(mycompanydetails.com)
Акционер
(mycompanydetails.com)
Бывший LLP designated member
(opencorporates.com)
LLP designated member
(opencorporates.com)
Регистрация
(opencorporates.com)
opencorporates.com
Строительство
(СМИ)
Foreign corporation
(закрыта)
Владелец 50% акций
(companieslondon.com)
Foreign corporation
Поставка в 2013-м году
(СМИ)


Материнская компания
(zachestnyibiznes.ru)
Компания-дистрибьютор
(официальный сайт)
Компания дистрибьютор
(Foreign corporation)
ФИО
Акционер
(официальный сайт)
Significant Influence Or Control
(opencorporates.com)
Foreign corporation
Поставка на 125 млн. USD в 2014-м
(СМИ)
Акционер
(offshoreleaks.icij.org)
Акционер
(СМИ)
Директор
(СМИ)
LLP designated member
(opencorporates.com)
LLP designated member
(opencorporates.com)
Регистрация
(opencorporates.com)
ФИО
ФИО (рус.)
ФИО (рус.)
Foreign corporation
Foreign corporation
Адрес
Страна
Акционер
(offshoreleaks.icij.org)
Акционер
(offshoreleaks.icij.org)
Директор
(mycompanydetails.com)
Акционер
(mycompanydetails.com)
Бывший LLP designated member
(opencorporates.com)
LLP designated member
(opencorporates.com)
Регистрация
(opencorporates.com)
opencorporates.com
Строительство
(СМИ)
Foreign corporation
(закрыта)
Владелец 50% акций
(companieslondon.com)
Foreign corporation
Поставка в 2013-м году
(СМИ)

16 + 7 + 0,38 ≠ 125


Год 2014
Выручка 16 млн. USD
Валовая прибыль 2 млн. USD
Прибыль до налогообложения 8 млн. USD
Наличные средства 3 млн. USD
Краткосрочные обязательства - 8 млн. USD
(zachestnyibiznes.ru)
Компания дистрибьютор
Год 2014
Выручка 7 млн. USD
Валовая прибыль - 9 тыс. USD
Чистые активы 320 тыс. USD
Наличные средства 520 тыс. USD
Краткосрочные обязательства - 19 млн. USD
(companieslondon.com)
Foreign corporation
Поставка на 125 млн. USD в 2014-м
(СМИ)
Страна
Год 2014
Выручка 380 тыс. USD
Валовая прибыль 30 тыс. USD
Чистые активы 60 тыс. USD
Наличные средства 3 тыс. USD
Краткосрочные обязательства - 11 млн. USD
(companieslondon.com)
Foreign corporation
Возможное сотрудничество

Кейс 8
«Неконкурентные торги»

Заказчик

Федеральное государственное бюджетное научное учреждение.

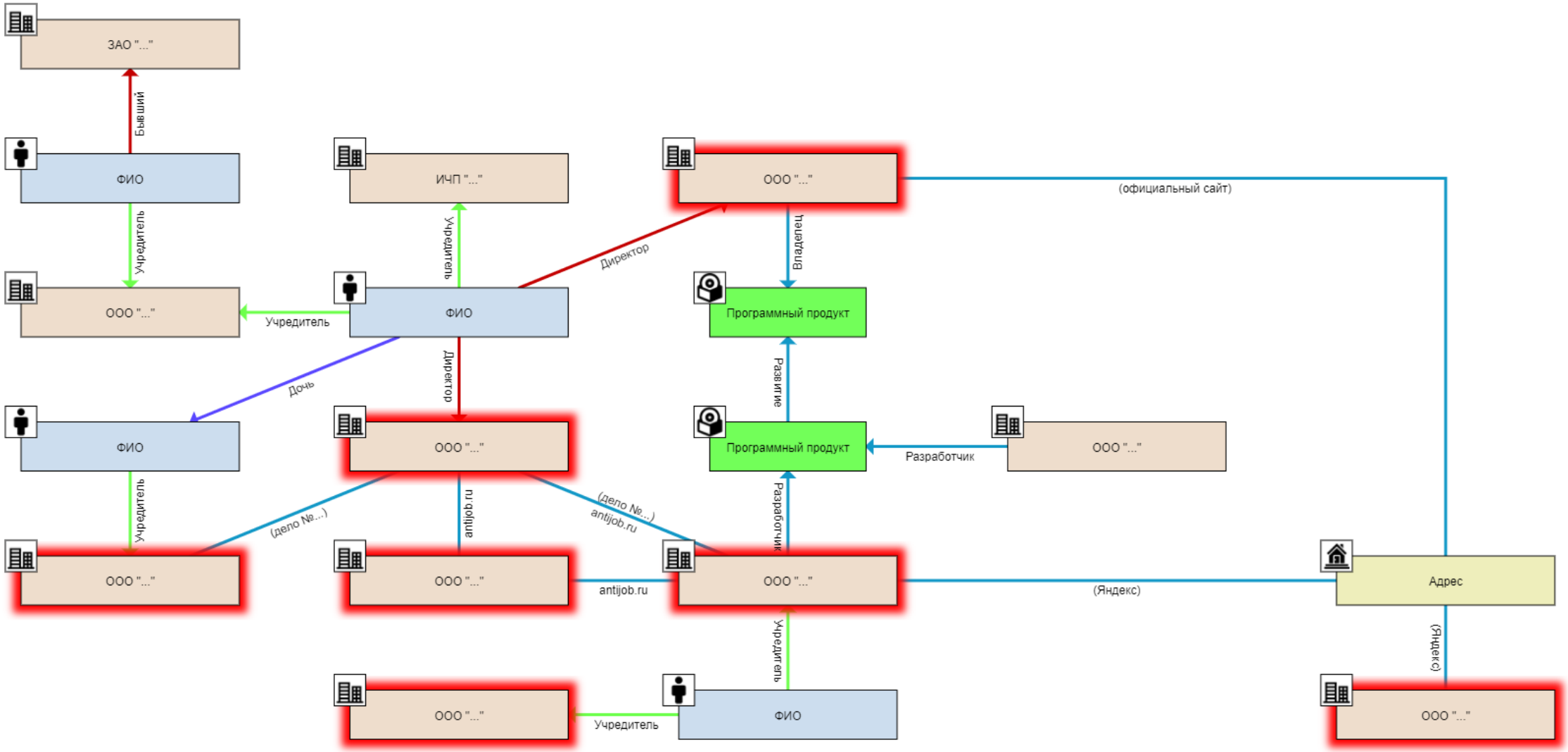
Постановка задачи

Оценить целесообразность приобретения специализированного программного обеспечения у контрагента.

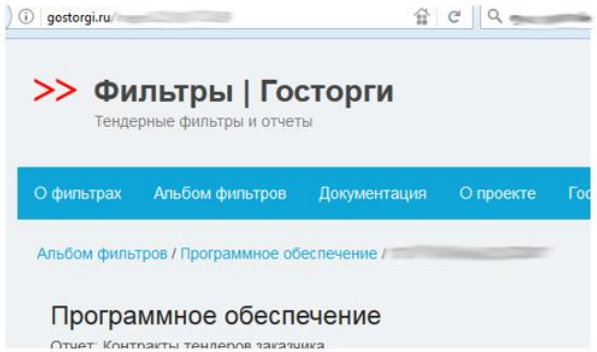
Работы

- Технический анализ ПО (функционала, используемого стека технологий, информационной безопасности и т.д.)
- Проверка контрагента (поиск аффилированных компаний, определение фактов участия в неконкурентных торгах, анализ финансовых показателей).

Схема аффилированности



Конкурсные торги



99	Обновление гипервизора терминальных серверов автоматизированной системы	Котировка	Московская обл.		ООО
100	Расходный материал для автоматизированной информационной системы.	Котировка	Московская обл.		ООО

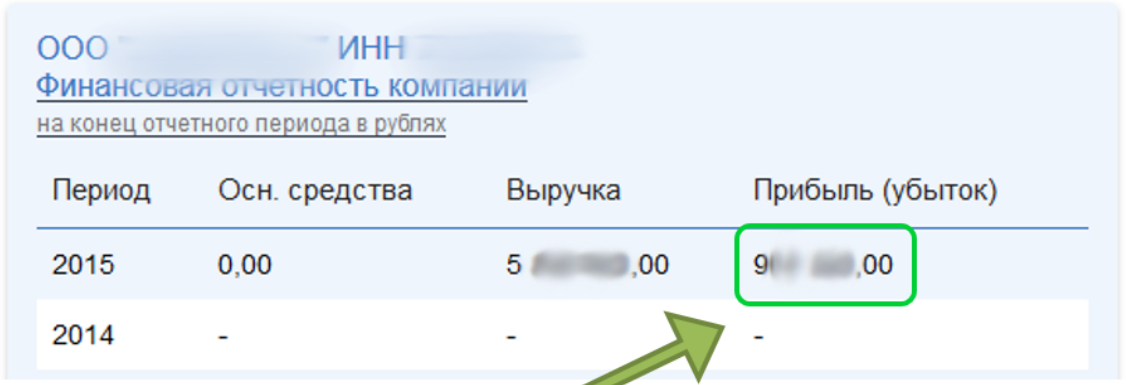
55	Расходные материалы для	Котировка	Московская обл.		ООО
56	Расходные материалы для автоматизированной информационной системы	Котировка	Московская обл.		ООО

№	Тендер	Дата	Регион	Сумма	Поставщик
1	Комплексное сопровождение ядра,		г. Москва		ООО (28)
3	Оказание услуг по комплексному сопровождению ядра,		г. Москва		ООО (28)

12	Расходные материалы для принтеров	ЭА	Московская обл.		ООО
13	Техническое обслуживание, модернизация, ремонт, замена составных частей серверной группы	ЭА	Московская обл.		ООО

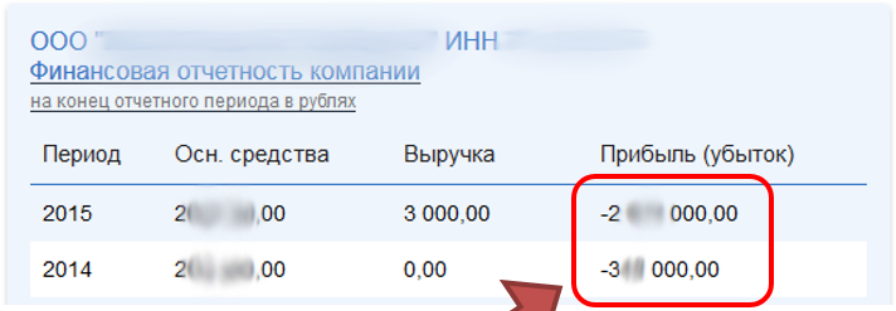
№	Тендер	Дата	Регион	Сумма	Поставщик
3	Сопровождение		г. Москва		ООО
9	Сопровождение автоматизированной информационной системы		г. Москва		ООО
17	Адаптация и внедрение автоматизированной системы		г. Москва		ООО

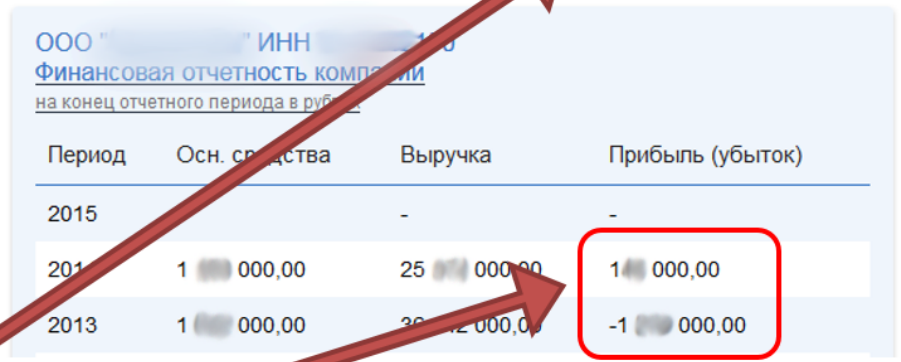
Финансовая отчётность

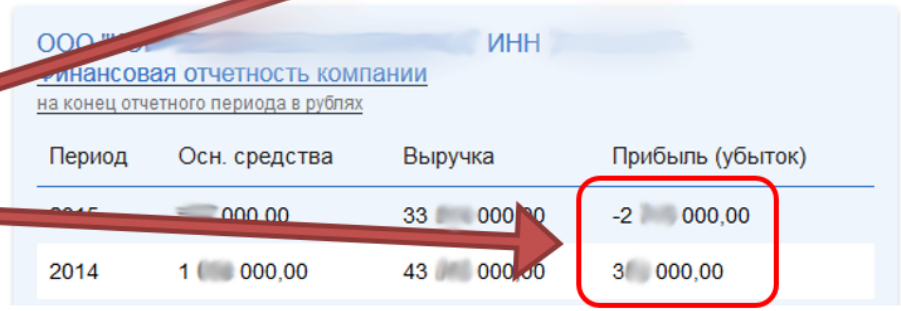


Всё в порядке?

Не факт!







Кейс 9
«Неконкурентные торги 2»

Заказчик

Государственная корпорация

Постановка задачи

В отношение крупного акционерного общества возникло подозрение, что часть закупок, которые оно осуществляет по ФЗ №223, проводится с использованием **неконкурентных механизмов**. В частности, через аффилированные компании.

Работы

Был проанализирован архив более чем 1000 закупок АО за 2017-й год по нескольким выбранным категориям на предмет пересечения участников соответствующих тендеров и связей их победителей между собой и непосредственно с самим АО.

Гос. закупки

Закупка								Заказчик		Результат		
Номер	Название	НМЦ	Валюта	Дата публикации	Окончание приема заявок	Этап отбора	Способ отбора	Название	ИНН	Название	ИНН	Ценовое предложение
[illegible]	[illegible]	[illegible]	RUB	[illegible].2017	[illegible]	Завершена	Закупка иного способа размещения	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	RUB	[illegible].2017	[illegible]	Завершена	Закупка иного способа размещения	[illegible]	[illegible]	-	-	
[illegible]	[illegible]	[illegible]	RUB	[illegible].2017	[illegible]	Завершена	Закупка иного способа размещения	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	RUB	[illegible].2017	[illegible]	Завершена	Закупка иного способа размещения	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	RUB	[illegible].2017	[illegible]	Завершена	Закупка иного способа размещения	[illegible]	[illegible]	-	-	-
[illegible]	[illegible]	[illegible]	RUB	[illegible].2017	[illegible]	Признана несостоявшейся	Закупка иного способа размещения	[illegible]	[illegible]	-	-	-
[illegible]	[illegible]	[illegible]	RUB	[illegible].2017	[illegible]	Завершена	Закупка иного способа размещения	[illegible]	[illegible]	-	-	-
[illegible]	[illegible]	[illegible]	RUB	[illegible].2017	[illegible]	Завершена	Закупка иного способа размещения	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Подозрительные подрядчики

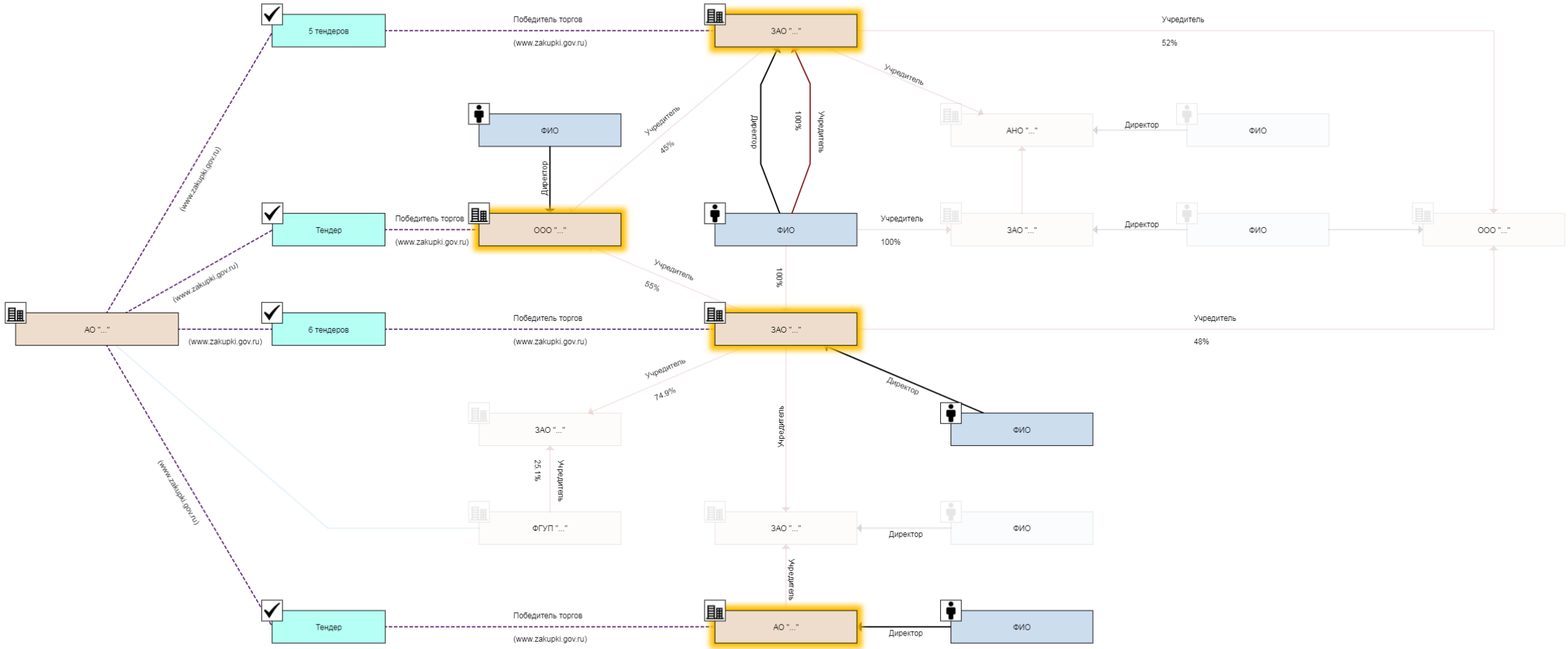
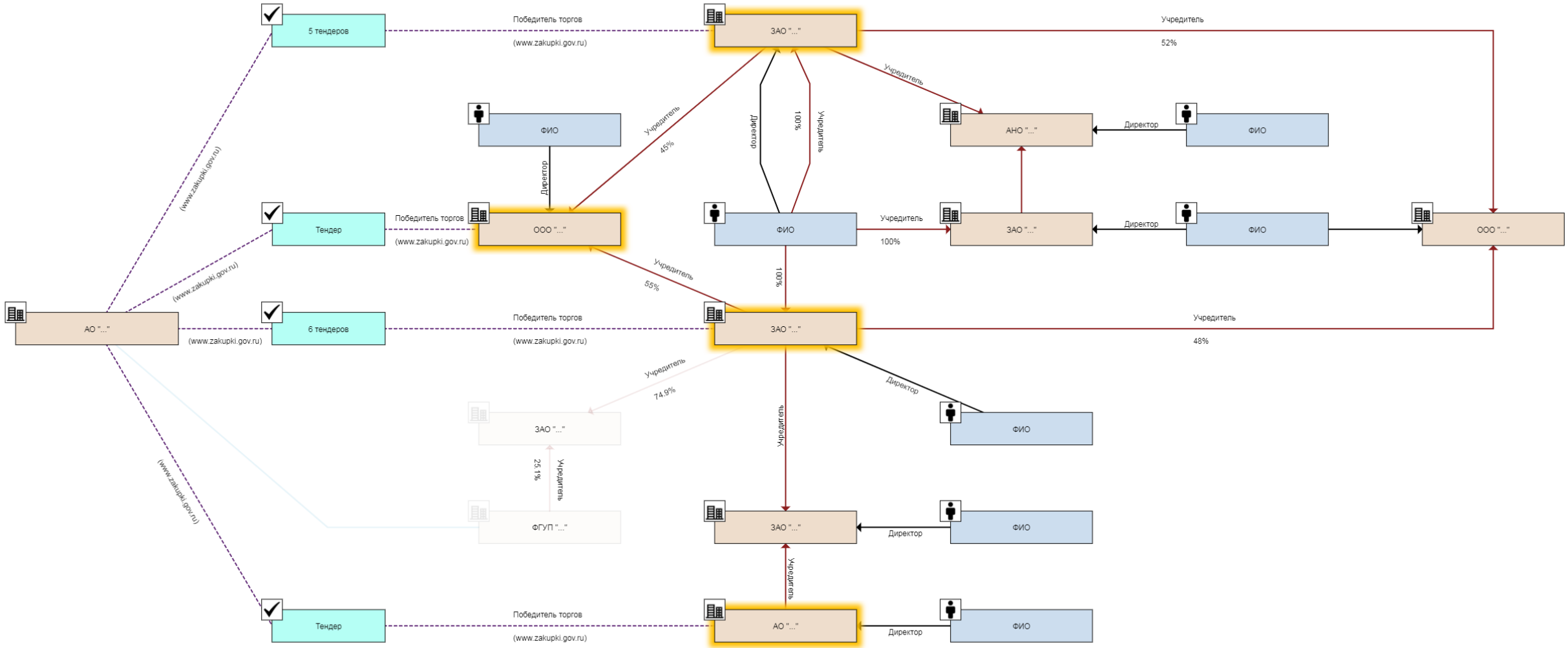
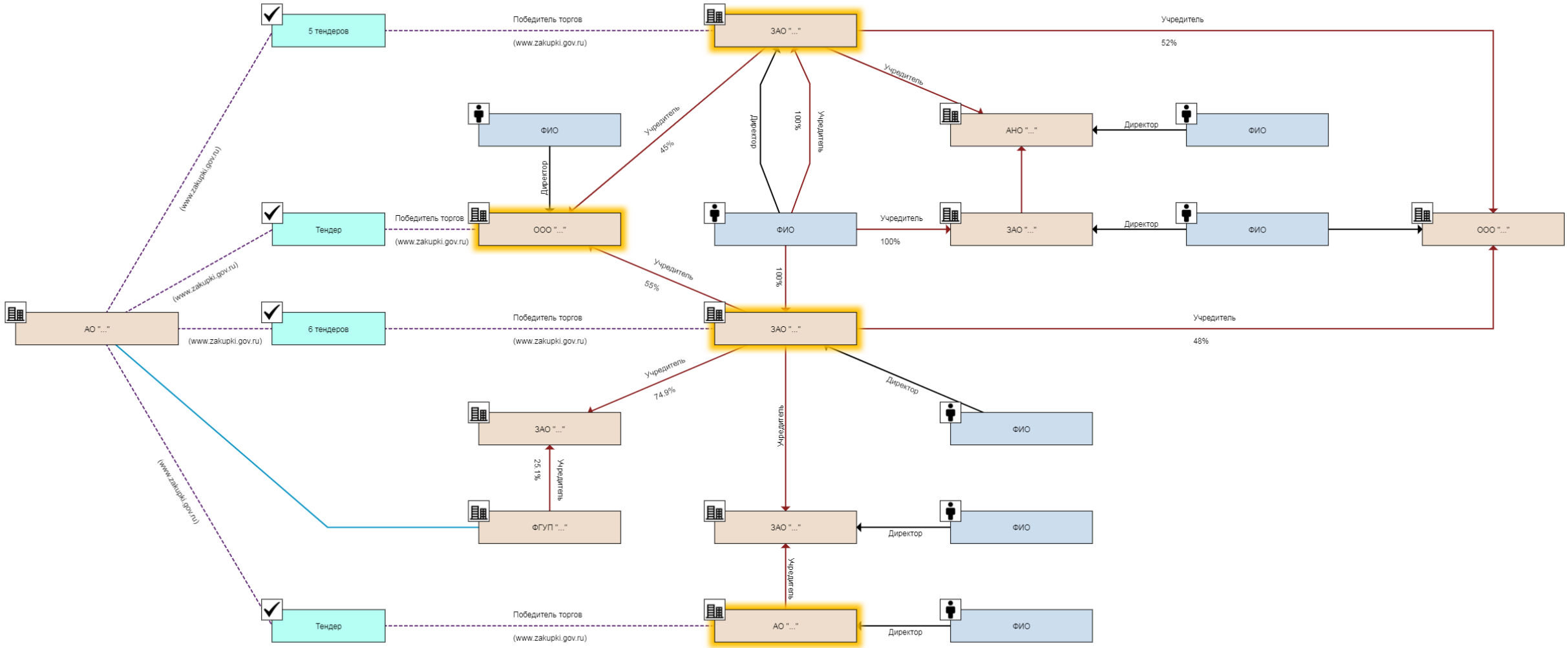
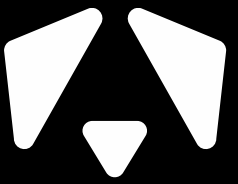


Схема аффилированности



Сговор


5 тендеров
Победитель торгов
(www.zakupki.gov.ru)
ЗАО "..."
Учредитель
52%
(www.zakupki.gov.ru)
ФИО
Учредитель
45%
Директор
100%
Учредитель
Учредитель
АНО "..."
Директор
ФИО
Тендер
Победитель торгов
(www.zakupki.gov.ru)
ООО "..."
ФИО
Учредитель
100%
ЗАО "..."
Директор
ФИО
ООО "..."
(www.zakupki.gov.ru)
Учредитель
55%
100%
АО "..."
(www.zakupki.gov.ru)
6 тендеров
Победитель торгов
(www.zakupki.gov.ru)
ЗАО "..."
Учредитель
48%
Учредитель
74,9%
Директор
ЗАО "..."
ФИО
25,1%
Учредитель
Учредитель
(www.zakupki.gov.ru)
ФГУП "..."
ЗАО "..."
Директор
ФИО
Учредитель
Тендер
Победитель торгов
(www.zakupki.gov.ru)
АО "..."
Директор
ФИО



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо за внимание!

Максим Авдюнин

Maksim.Avdyunin@amonitoring.ru