

Защита конфиденциальной информации от интернет-угроз

МАСАЛОВИЧ
Андрей Игоревич



Киберпространство сегодня: новые угрозы и вызовы

- ❑ Массовые утечки конфиденциальной информации
 - ❑ Активное и жесткое информационное противоборство
 - ❑ Аналитические методы разведки - выявление скрытых связей и др.
-

Конкурентная разведка

- ❑ **Конкурентная разведка** ([англ. Competitive Intelligence](#), сокр. CI) — сбор и обработка данных из разных источников, для выработки управленческих решений с целью повышения конкурентоспособности коммерческой организации, проводимые в рамках закона и с соблюдением этических норм (в отличие от [промышленного шпионажа](#)); а также структурное подразделение предприятия, выполняющее эти функции.
- ❑ Конкурентная разведка – это информационное обеспечение победы над конкурентами
- ❑ «Я просто не люблю неожиданностей»

Собираем данные о персоне

Журавлев Сергей Валерианович

Родился 17 июля 1966 г. в г.Воронеж. В 1983 г. окончил среднюю школу №33.

С 1983 по 1985 год - учёба в техникуме. Специальность - регулировщик радиоаппаратуры. Диплом с отличием. В этот же период - работа в Воронежском научно-исследовательском институте приборного машиностроения.

В 1985-1987 годах - служба в рядах Советской Армии. Отдельная специализированная часть милиции.

С 1988 по 1994 год - студент Воронежского лесотехнического института. Специальность инженер-технолог.

С 1991 года - заместитель директора производственного объединения «Контакт».

С 1997 года - генеральный директор ЗАО "Финансовая компания "Аксиома".

Кандидат экономических наук.



Глазами конкурентного разведчика...

Журавлев Сергей Валерианович

Доход за год: ЗАО ФК "Аксиома", зарплата 720000 руб.

Квартиры: г. Воронеж, ул.К.Маркса, д.40а, кв.19, 242.5 кв.м

Земельные участки: Воронежская область,
Новоусманский район, пос.Безбожник, участок N28/1, дачный, 1463 кв.м

Жилые дома: г.Воронеж, Левобережное лесничество учебно-опытного лесхоза ВГЛТА, 209 кв.м.

Гаражи: г.Воронеж, ул. К. Маркса, д.40а, №26-27, 52 кв.м

Денежные средства на личных счетах на текущий момент:

ОАО "Московский Индустриальный банк", г. Воронеж, ул. Театральная, д. 20а, 40817810800393000800, 176219 руб.;

ОАО "Московский индустриальный банк", г. Воронеж, ул. Театральная, д. 20а, 40817810100394000075, 0 руб.;

ОАО "Московский индустриальный банк", г. Воронеж, ул. Театральная, д. 20а, 40817810000392000025, 207 руб.;

Центрально-Черноземный банк Сбербанка России, г. Воронеж, просп.Революции, д. 37, 42301810913000619762, 10 руб.;

Центрально-Черноземный банк Сбербанка России, г. Воронеж, ул.9 Января, д.28, 40817810513007107778, 477 руб.

Акции и иное участие в коммерческих организациях:

"Волгострой", г. Воронеж, ул.Брянская, д.71а, участие 5.88;

"Прогресс-К", г. Воронеж, просп.Патриотов, д.75, участие 52.5;

"Культурная инициатива", г. Воронеж, ул.Генерала Лизюкова, д.60, 34%;

"Альфа-строй", г. Воронеж, просп.Революции, д.37, участие 100;

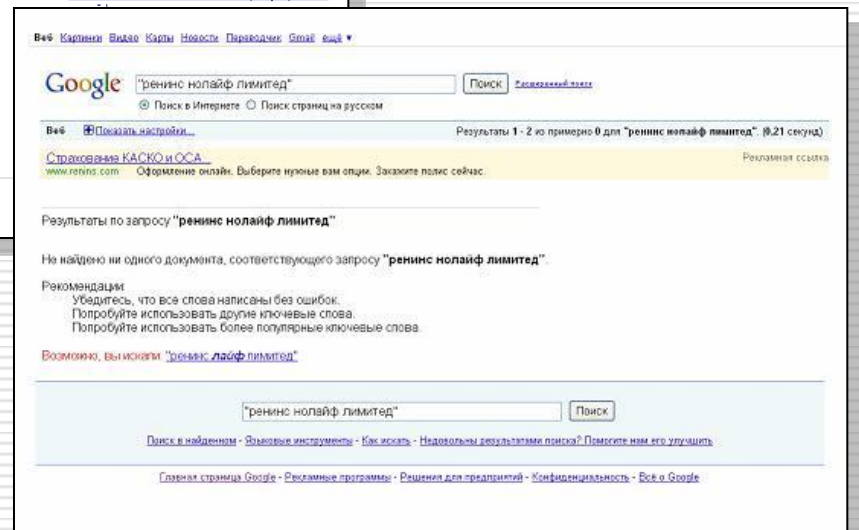
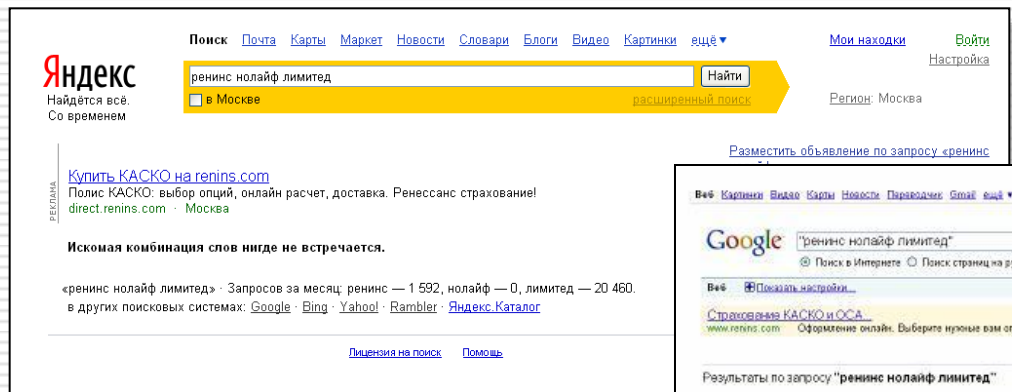
УК "Аксиома", г. Воронеж, ул.Генерала Лизюкова, д.60, участие 100;

Проектная мастерская "Аксиома", г. Воронеж, просп.Революции, д.37, 100%;

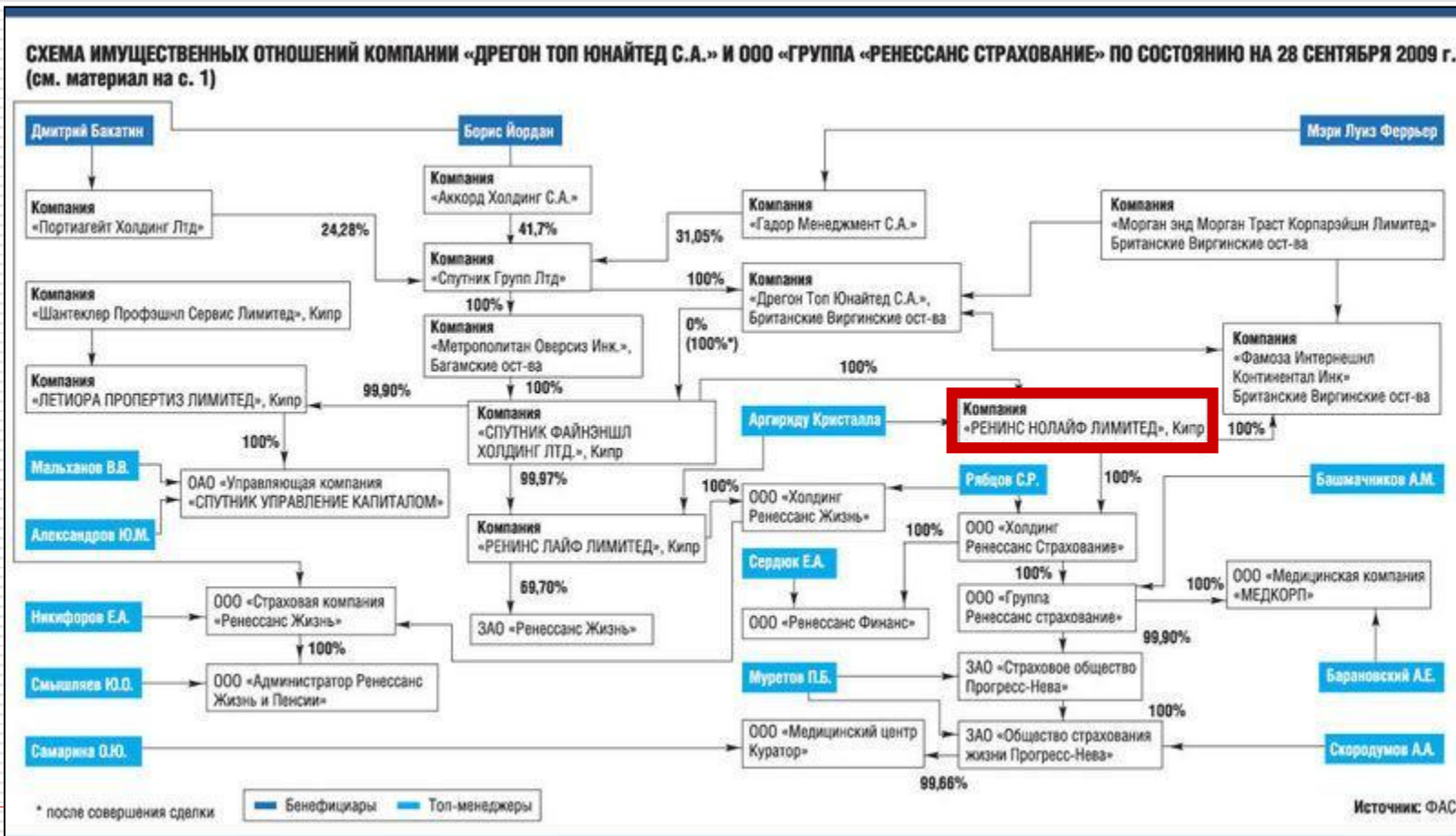
"Финансовая компания "Аксиома", г. Воронеж, пл.Ленина, д.9, участие 100

Задача – узнать о компании Ренинс Нолайф Лимитед

Обычные запросы в Yandex и в Google не дают ничего:



Ренинс Нолайф Лимитед – есть такая фирма...



Интернет-разведка в действии

- ❑ http://www.ogrn.ru/info_egrul/search/5n49p166ns1
 - ❑ http://ogrn.ru/info_egrul/company/1fa661c94a5
-

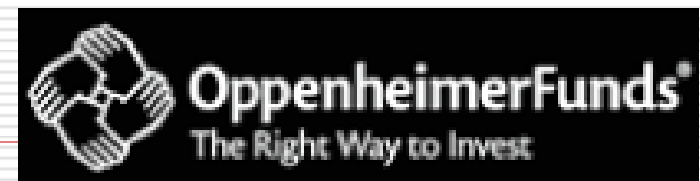
Это – безопасность

- ❑ **23 мая 2010,**
- ❑ Гонки на первенство NHRA
- ❑ Взрыв внутри автомобиля
- ❑ Пожар в двух автомобилях
- ❑ **Пилоты не пострадали**



Это – безопасность

- ❑ **11 сентября 2001 г**
- ❑ Чудовищный теракт
- ❑ От WTC остались руины
- ❑ От серверов не осталось и пыли...
- ❑ **Информационная система Фонда Оппенгеймера сохранила данные**



Это – безопасность?

- ❑ 4 декабря 2009
- ❑ **Неизвестные хакеры взломали систему безопасности сайта газеты «Московский комсомолец» и уничтожили все сетевые структуры и архивы.**
- ❑ Как рассказывают в потерпевшей редакции, уничтожению подвергся даже редакторский интерфейс **и архив за все годы существования сайта.** По словам редактора газеты Павла Гусева, хакеры атаковали в ночь на четверг.
- ❑ "Когда наши работники заметили, что происходит, они выключили всю систему, но было уже поздно. У нас, конечно, были системы безопасности, но хакерам удалось уничтожить и их."



Пример новых угроз: аппаратные снифферы



Пример упущенного контроля над ситуацией

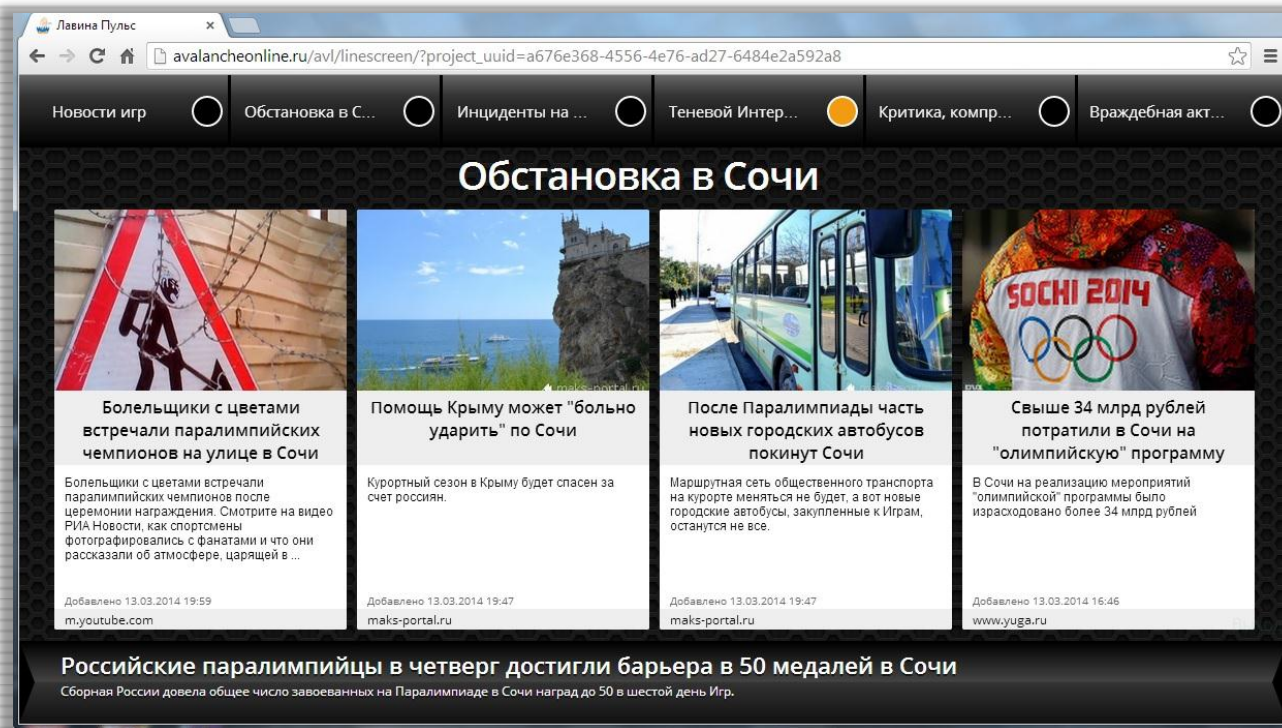
❑ Бирюлево, 10-13 октября 2013



Country	Year	Value
Algeria	2000	0.00
Algeria	2001	0.00
Algeria	2002	0.00
Algeria	2003	0.00
Algeria	2004	0.00
Algeria	2005	0.00
Algeria	2006	0.00
Algeria	2007	0.00
Algeria	2008	0.00
Algeria	2009	0.00
Algeria	2010	0.00
Algeria	2011	0.00
Algeria	2012	0.00
Algeria	2013	0.00
Algeria	2014	0.00
Algeria	2015	0.00
Algeria	2016	0.00
Algeria	2017	0.00
Algeria	2018	0.00
Algeria	2019	0.00
Algeria	2020	0.00
Algeria	2021	0.00
Algeria	2022	0.00
Algeria	2023	0.00
Algeria	2024	0.00
Algeria	2025	0.00
Algeria	2026	0.00
Algeria	2027	0.00
Algeria	2028	0.00
Algeria	2029	0.00
Algeria	2030	0.00
Algeria	2031	0.00
Algeria	2032	0.00
Algeria	2033	0.00
Algeria	2034	0.00
Algeria	2035	0.00
Algeria	2036	0.00
Algeria	2037	0.00
Algeria	2038	0.00
Algeria	2039	0.00
Algeria	2040	0.00
Algeria	2041	0.00
Algeria	2042	0.00
Algeria	2043	0.00
Algeria	2044	0.00
Algeria	2045	0.00
Algeria	2046	0.00
Algeria	2047	0.00
Algeria	2048	0.00
Algeria	2049	0.00
Algeria	2050	0.00
Algeria	2051	0.00
Algeria	2052	0.00
Algeria	2053	0.00
Algeria	2054	0.00
Algeria	2055	0.00
Algeria	2056	0.00
Algeria	2057	0.00
Algeria	2058	0.00
Algeria	2059	0.00
Algeria	2060	0.00
Algeria	2061	0.00
Algeria	2062	0.00
Algeria	2063	0.00
Algeria	2064	0.00
Algeria	2065	0.00
Algeria	2066	0.00
Algeria	2067	0.00
Algeria	2068	0.00
Algeria	2069	0.00
Algeria	2070	0.00
Algeria	2071	0.00
Algeria	2072	0.00
Algeria	2073	0.00
Algeria	2074	0.00
Algeria	2075	0.00
Algeria	2076	0.00
Algeria	2077	0.00
Algeria	2078	0.00
Algeria	2079	0.00
Algeria	2080	0.00
Algeria	2081	0.00
Algeria	2082	0.00
Algeria	2083	0.00
Algeria	2084	0.00
Algeria	2085	0.00
Algeria	2086	0.00
Algeria	2087	0.00
Algeria	2088	0.00
Algeria	2089	0.00
Algeria	2090	0.00
Algeria	2091	0.00
Algeria	2092	0.00
Algeria	2093	0.00
Algeria	2094	0.00
Algeria	2095	0.00
Algeria	2096	0.00
Algeria	2097	0.00
Algeria	2098	0.00
Algeria	2099	0.00
Algeria	2100	0.00
Algeria	2101	0.00
Algeria	2102	0.00
Algeria	2103	0.00
Algeria	2104	0.00
Algeria	2105	0.00
Algeria	2106	0.00
Algeria	2107	0.00
Algeria	2108	0.00
Algeria	2109	0.00
Algeria	2110	0.00
Algeria	2111	0.00
Algeria	2112	



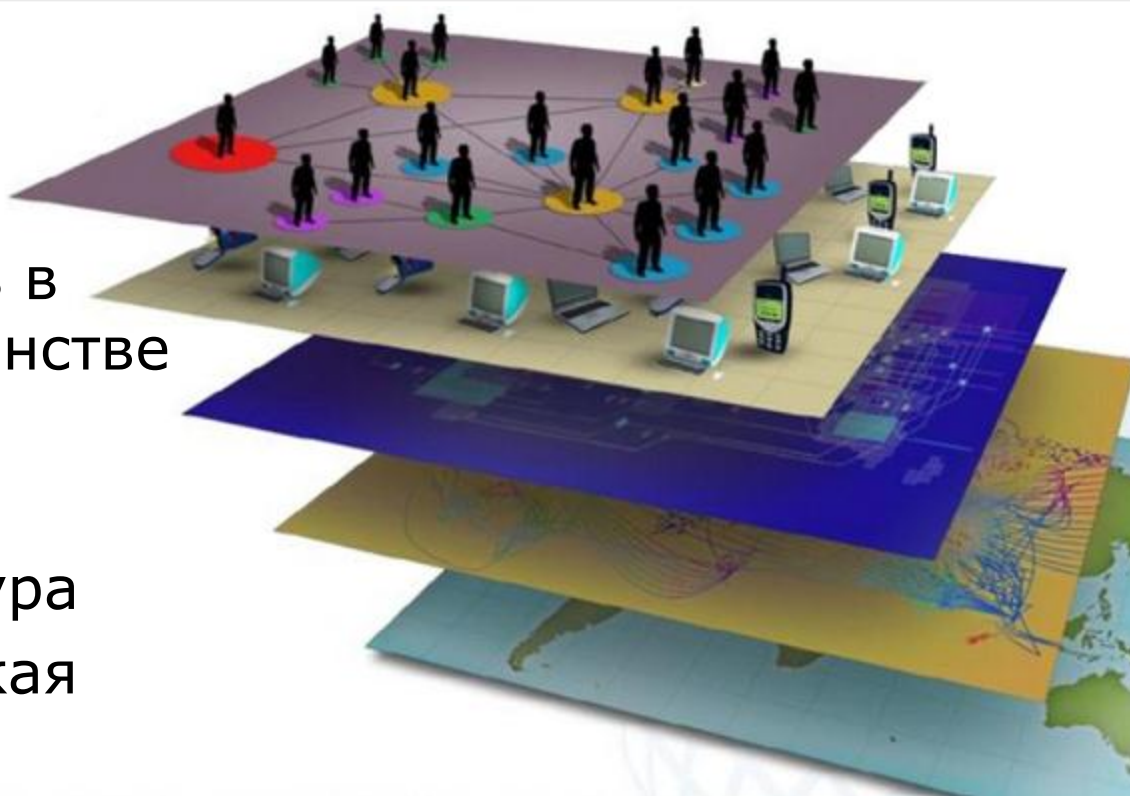
Обеспечение ситуационной осведомленности



Пространство совместных киберопераций ВС США

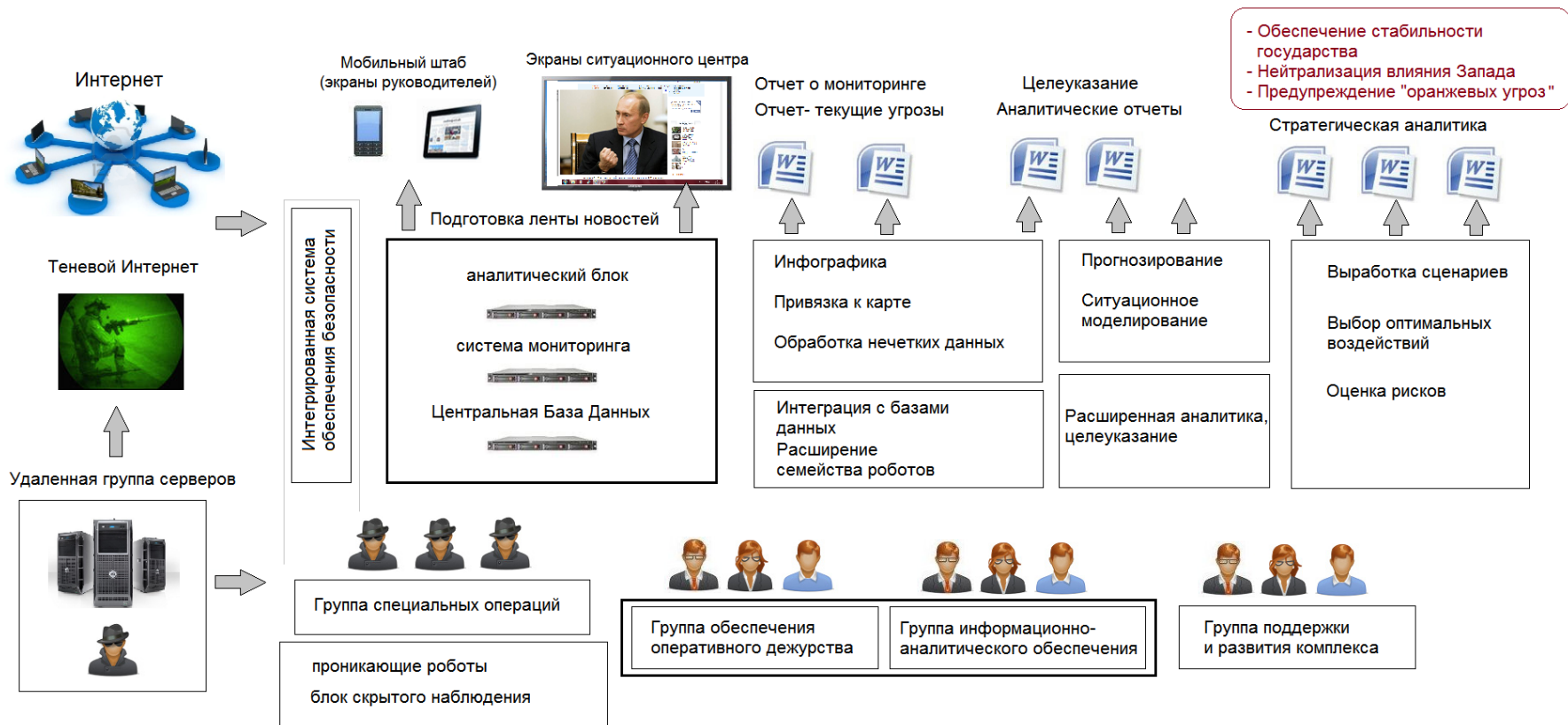


- ☐ Люди
- ☐ Идентичность в киберпространстве
- ☐ Информация
- ☐ Физическая инфраструктура
- ☐ Географическая среда



Структура системы раннего предупреждения и оперативного реагирования

Структура программного обеспечения Ситуационного центра

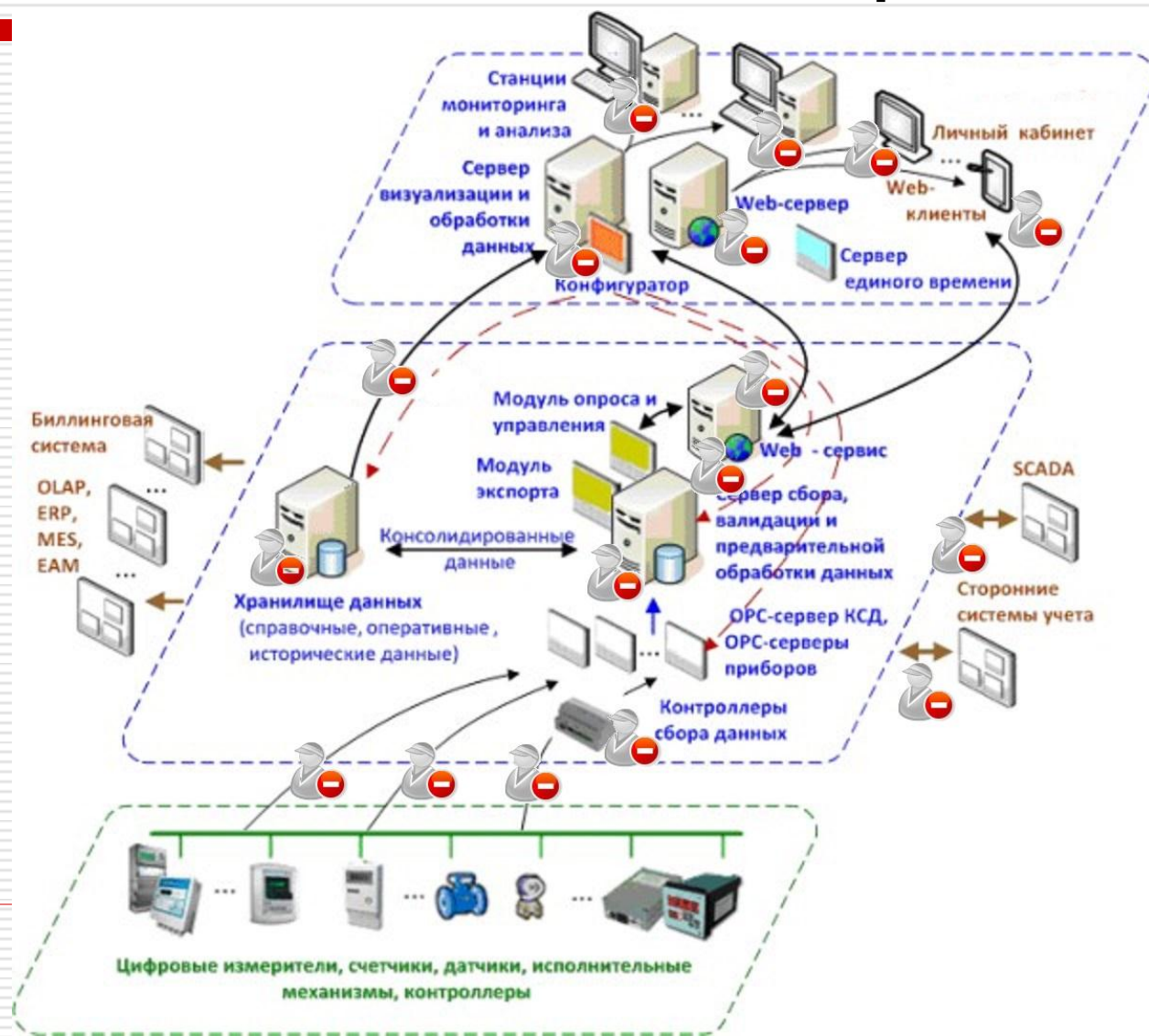


АНБ прослушивает коммуникации более 50 стран, включая дипломатов и ООН



1960 - Bernon F. Mitchell, William H. Martin, 1963 - Victor N. Hamilton
2013 - Эдвард Сноуден

Только двое знают Ваши секреты – Вы и Большой Брат



Avalanche (Лавина) – технология интернет-разведки

- ❑ Технология разработана более 10 лет назад и апробирована в ряде крупных структур
- ❑ Автоматический мониторинг Интернета
- ❑ Более 20 типов поисковых роботов
- ❑ «Проникающие роботы» для скрытого наблюдения за «Глубинным Интернетом»
- ❑ Автоматическое определение уровня угрозы и значимости информации
- ❑ и т.д.

Лавина Пульс – мониторинг ситуации в регионе

☰

←

Томская область

Администратор

⏻

<div>Губернатор и Администрация</div> <div>Мэрия: официально в 26 д... 04.06.2014 15:44:32 По информации, которой располагает департамент городского хозяйства, на сегодняшний день лишь в 26 домах http://www.tv2.tomskr.ru/news/ofitsialno-ly-26-domakh-</div> <div>Депутаты запретили подав... 04.06.2014 14:07:47 Это решение было принято на очередном собрании думы Томска. http://news.vtomske.ru/news/83567.html</div>	<div>Социально-экономическая обстановка</div> <div>Экспозиция Томской облас... 04.06.2014 16:09:35 Томская область представляет продукты и технологии IT-компаний и университетов региона на выставке http://www.70rus.org/more/36006/</div> <div>На теплоэлектроцентрали ... 04.06.2014 16:09:35 На ТЭЦ ОАО «Сибирский химический комбинат» состоялись тактико-специальные учения систем ГО и ЧС, где http://www.70rus.org/more/36005/</div>	<div>Настроения общественности</div> <div>Народные новости: за сро... 04.06.2014 15:53:39 В нашу рубрику «Народные новости» обратилась читательница с ником pi-fulya, которая пытается http://news.vtomske.ru/news/83646.html</div> <div>Быть или не быть парковка... 04.06.2014 13:48:52 Еще один вопрос слушаний будет посвящен введению параметра озеленения городских территорий http://tomsk.sibnovosti.ru/business/270257-byt-ili-ne-</div>	<div>Репутационные угрозы</div> <div>Томич пытался устроить ак... 04.06.2014 07:28:14 На томском предприятии МУП «Спецавтохозяйство», на прошлой неделе произошел весьма резонансный http://novo-tomsr.ru/index.php?newsid=19560</div> <div>Назначение нового и.о. ре... 03.06.2014 10:50:43 На минувшей неделе губернатор Томской области Сергей Жвачкин наконец избавился от постоянной http://novo-tomsr.ru/index.php?newsid=19545</div>
<div>Критика, компромат, негатив</div> <div>Бывший полицейский, треб... 04.06.2014 13:50:57 Суд апелляционной инстанции не изменил меру наказания сотруднику полиции, приговоренному к 2,4 годам http://vesti70.ru/news/boivshiy_politsayjskiy_trebovavshiy_</div> <div>«Межениновку» оштрафов... 04.06.2014 12:54:02 Агрофирма «Межениновская» оштрафована на 40 тысяч рублей по результатам проверки http://www.tomsr.ru/news/view/89981/</div>	<div>Криминал, экстремизм</div> <div>Полиция закрыла наркома... 03.06.2014 10:50:48 Как сообщает пресс-служба областного управления Госнаркоконтроля, очередная оперативная разработка http://news.vtomske.ru/news/83543.html</div> <div>В Томской области заверш... 30.05.2014 11:25:45 Отделом по расследованию особо важных дел следственного управления Следственного комитета Российской http://70.sledcom.ru/news/detail.php?news=11629</div>	<div>Массовые акции</div> <div>Томские школьники вышли... 04.06.2014 14:24:09 Тринадцатая ежегодная экологическая акция «Городским рекам - чистые берега» состоялась сегодня. http://www.tv2.tomskr.ru/news/tomskie-shkolniki-vyshli-</div> <div>На митинг в защиту телеко... 04.06.2014 07:28:14 На митинг-концерт в поддержку телекомпании ТВ-2, который прошел на площади перед СФТИ, пришли томские http://novo-tomsr.ru/index.php?newsid=19554</div>	<div>Происшествия</div> <div>Томские спасатели укрепл... 04.06.2014 16:09:36 Томские сотрудники МЧС ведут укрепление дамбы в поселке Затон в Барнауле, в котором началось http://www.tv2.tomskr.ru/news/tomskie-spatelli-</div> <div>МЧС: Из-за наводнения на... 04.06.2014 14:24:09 Томичам не стоит опасаться последствий наводнения на Алтае: специалисты не прогнозируют в нашем http://www.tv2.tomskr.ru/news/mchs-liz-zh-</div>

🖨

💻

Досье на персону

Персоны

Админ
Админов

+

Создать

Поиск...

Изменить

Фильтр по типу: Все

ОАО "Воентелеком"

Компания

Московская Коллегия Адвок...

Компания

ООО «Системы и связь»

Компания

Давыдов Александр Евгень...

Персона

Воловельский Константин ...

Персона

Колесниченко Александр П...

Персона

Черноярский Борис Анатол...

Персона

Тамодин Николай Васильев...

Персона

Линник Сергей Александро...

Персона

(812) 295-51-65

Телефон

7495 223-33-40

Телефон

7-926-900-25-62

Телефон

8(499)250-24-82

Телефон

Давыдов Александр Евгеньевич

Тип: Персона

Данные объекта

Новости

Заметки

Связи

Схема

Документы

Логи

Открыть расширенный просмотр

314, г. Москва, ул. Большая Оленья, д. 15А, стр.1

Адрес работы (Локализация)

(812) 295-51-65

Телефон (Владение/Пользование)

Давыдов Александр Евгеньевич

Адрес проживания в

Санкт-Петербург, ул. Кантемировская, 5, литер А.

Сотрудник (Функциональная роль)

Работа основная (Функциональная роль)

Персона (Локализация)

Адрес (Локализация)

Пользователь (Владение/Пользование)

ВОЕНТЕЛЕКОМ

Досье на организацию

Avalanche 2.7 - project : Экспедиция

Проекты Лента новостей Источники Рубрики Объекты Связи объектов Настройки О программе

Объекты

Создать объект Удалить объект

Список объектов мониторинга


1246041
Адрес Руан-Города
Кравцов Александр Павлович
107150, г Москва, ул Бойцовая, д 22, стр 3
ООО "ЭКСПЕДИЦИЯ РИТЕЙЛ"
г.Москва, ул.Ливиченкова, д.7, кв.68
Экспедиция-Трофи 2013
+7 (495) 660-30-35
Руан-Город
Мерседес-Бенц У474KE99

Тип объекта: Компания

ООО "ЭКСПЕДИЦИЯ РИТЕЙЛ" [изменить](#) [Сохранить](#)

Данные объекта | Новости | Заметки | Связи

Аватар



Название: ООО "Экспедиция ритейл"
Оргформа: ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
Тип:
Причина интереса: Основное место работы Александра Кравцова

Идентифицирующая информация

Латинское название: Limited liability company "Enkspeditsiya Ritejl"
Краткое название: ООО "ЭКСПЕДИЦИЯ РИТЕЙЛ"
Бренд: Экспедиция
☒ Дата регистрации: 23.10.2009

Место регистрации

Улица	Квартира, оф...	Примечание	Дом	Индекс	Населенный ...

Изменить
Удалить
Просмотр

Налоговая: 771801001, Межрайонная инспекция Федеральной налоговой службы №46 по г. Москве.
ИНН: 7718780656
ОГРН: 1097746648999
Продукция: Специализированная розничная торговля непродовольственными товарами, не включенными в другие группировки, 52.48.3

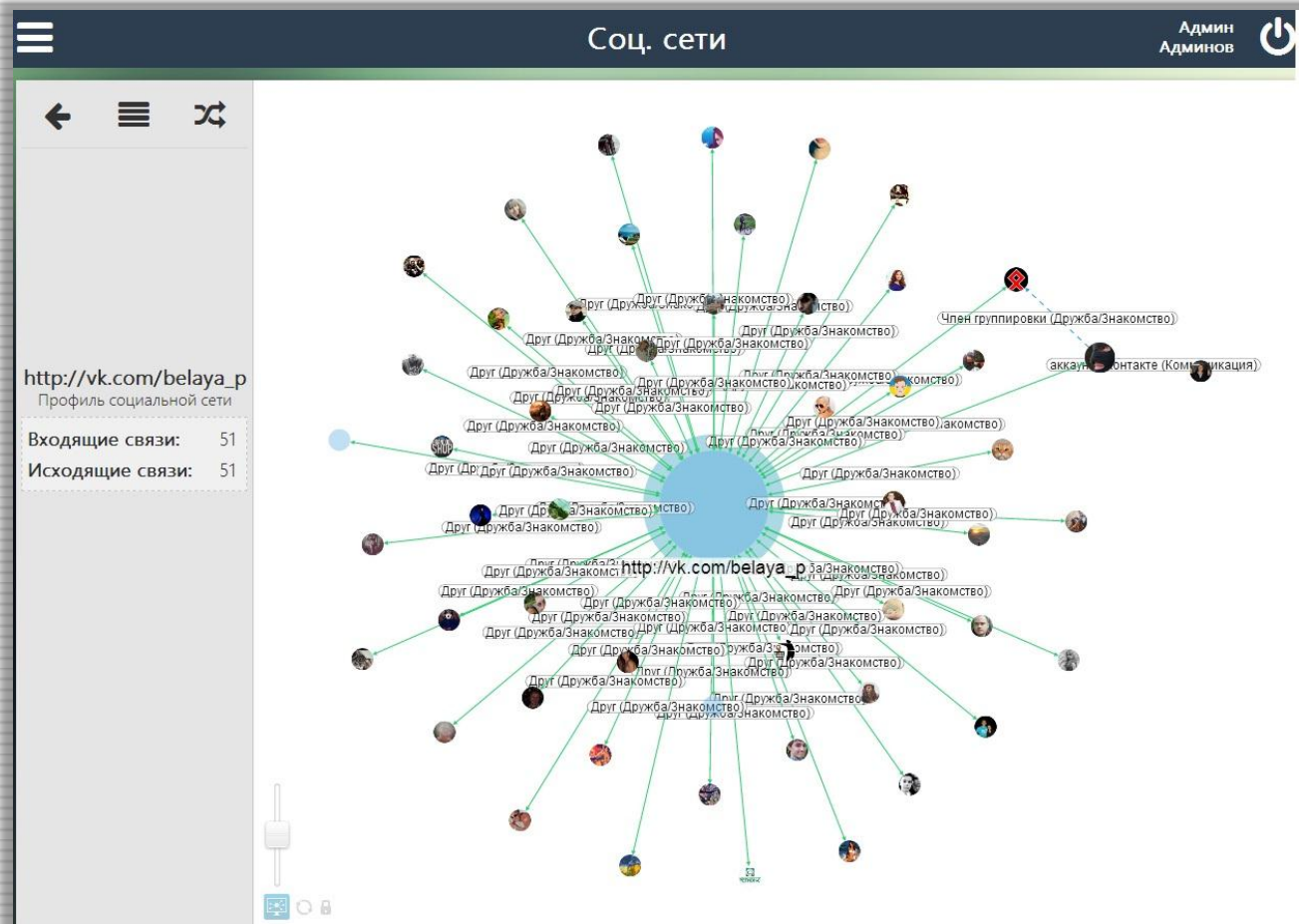
Контактная информация

Адреса

Улица	Квартира, оф...	Примечание	Дом	Индекс	Населенный ...
Бойцовая	строение 3		22	107150	Москва

Создать
Удалить
Просмотр

Связи объекта



Мониторинг события

+

Создать

Поиск...

Изменить

Все

Махачкалинская бандгруппа

Сообщество

Взрыв автобуса, Волгоград, 2...

Событие

Асиялова Наида

Персона

Гучучалиев Сиражудин Маго...

Персона

Абдулатипов Рамазан Гаджи...

Персона

Взрыв автобуса, Волгоград, 21.10.2013 14:05

Тип: Событие

Данные объекта

Новости

Заметки

Связи

Схема

Геопривязка

Документы

Логи

+

Добавить

17:10 СК: террористка-смертница Наида Асиялова

17:10. Официальный представитель СК Владимир Маркин заявил, что взрывное устройство привела в действие террористка-смертница - фрагменты ее тела найдены на месте трагедии. Как выяснилось, это 30-летняя уроженка Дагестана Наида Асиялова. Кроме того, под злополучным автобусом была обнаружена ручная граната.

04.06.2014 08:18:32

17:00 Теракт стал самой обсуждаемой темой в Твиттере

17:00. Теракт в Волгограде стал одной из самых обсуждаемых тем в Twitter. Каждую секунду пользователи Twitter публикуют одну или несколько записей, посвященных трагедии. Таким образом, в час в микроблогах появляется десять или больше тысяч "твитов", связанных с этим событием. Пользователи как пересылают друг другу свежие новости, так и выражают возмущение и соболезнования родным и близким погибшим и пострадавшим.

Заслон утечкам – сканер защищенности

Webbez			
Министерство Обороны	Госструктура	Банк	Коммерческая компания
09.04.2014 12:24 Сайт: www.redstar.ru обнаружены критические проблемы и уязвимости	16.04.2014 23:42 Сайт: www.mosoblonline.ru обнаружены критические проблемы и уязвимости	14.04.2014 23:03 Сайт: www.mtsbank.ru обнаружены проблемы безопасности	14.04.2014 17:18 Сайт: www.masterdata.ru обнаружены проблемы безопасности
09.04.2014 12:24 Сайт: www.pansion-mil.ru обнаружены проблемы безопасности	14.04.2014 10:52 Сайт: www.moduma.ru обнаружены проблемы безопасности	14.04.2014 12:34 Сайт: www.rgs.ru обнаружены проблемы безопасности	14.04.2014 11:21 Сайт: www.jet.msk.su обнаружены проблемы безопасности
МОЭСК	Олимпиада	Сколково	GreenPeace
14.04.2014 00:52 Сайт: holding-mrsk.ru обнаружены проблемы безопасности	16.04.2014 08:20 Сайт: sochi.yuga.ru обнаружены критические проблемы и уязвимости	14.04.2014 00:53 Сайт: www.sk.ru обнаружены проблемы безопасности	14.04.2014 01:20 Сайт: www.greenpeace.org обнаружены проблемы безопасности
14.04.2014 00:52 Сайт: mail.moesk.ru проблем не обнаружено	16.04.2014 08:20 Сайт: www.roc.ru обнаружены проблемы безопасности	14.04.2014 00:53 Сайт: www.conject.com обнаружены проблемы безопасности	07.04.2014 01:03 Сайт: www.greenpeace.org обнаружены проблемы безопасности

Сканеры безопасности

WebBez (Web Безопасность)

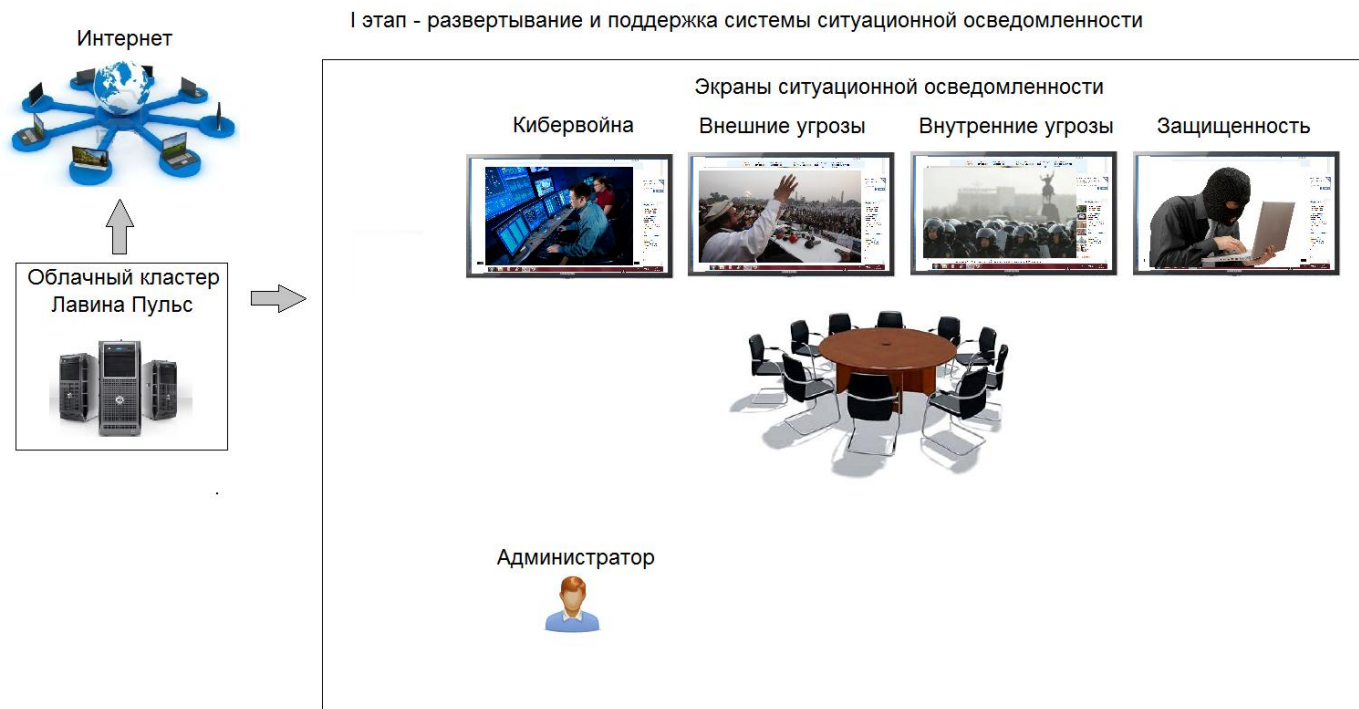


CLOUD
SECURITY

- ❑ Расширяемое семейство сканеров защищенности Web-приложений
- ❑ 18 сканеров в базовом комплекте
- ❑ Экспресс-режим: 2000 тестов за 10 минут
- ❑ Расширенный режим: 10000 тестов
- ❑ Любой регламент проверок: ежечасно и др.
- ❑ Сканирование в режиме Black Box
- ❑ Основные уязвимости OWASP Top 10

Лавина Пульс: этапы развертывания

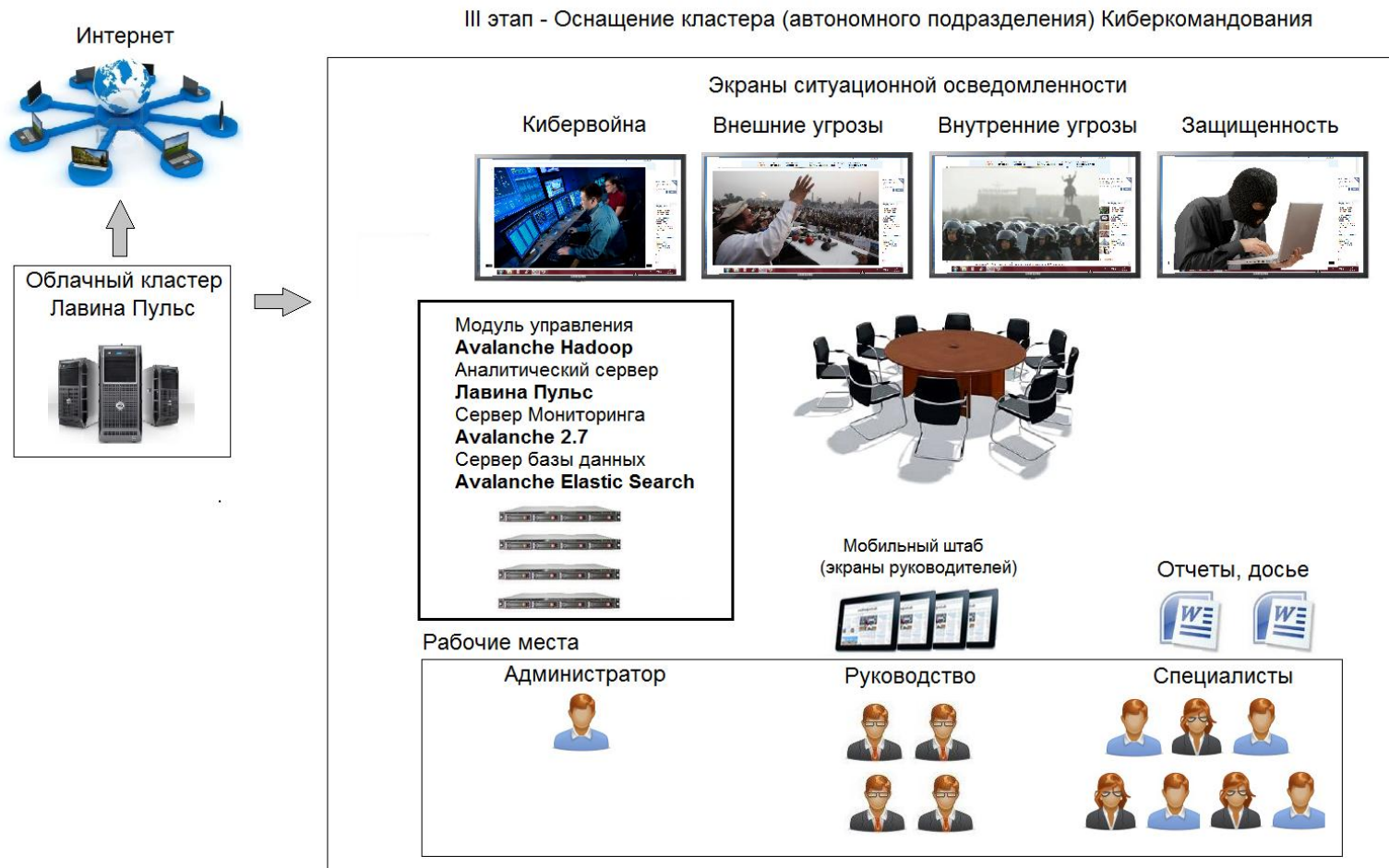
Этап 1 – боеготовность за неделю



Этап 2 – ситуационный центр за 1 месяц



Этап 3 – «Под ключ» за 3 месяца



Этап 4 – центр активного сетевого противоборства

IV этап - Оснащение Ведомства средствами активного противодействия в киберпространстве



Возможности сотрудничества

- ❑ Учебный курс «**Конкурентная разведка в Интернете**» - 2 дня
- ❑ Учебный курс «**Информационная безопасность в Интернете**» – 3 дня
- ❑ Учебный курс «**Технологии информационного противоборства в Интернете**» – 2 дня
- ❑ Контакт: **Дарья Неверова**
- ❑ +7 (495) 231-30-49



Практическое пособие по поиску в глубинном (невидимом) Интернете



Спасибо за внимание ☺



Масалович Андрей Игоревич

☐ E-mail: am@inforus.biz

☐ Phone: +7 (964) 577-2012

