ГАРДА
ТЕХНОЛОГИИ

КАК СОТРУДНИКИ СТАЛИ САМЫМИ ОПАСНЫМИ ХАКЕРАМИ ДЛЯ КОМПАНИИ

А ВЫ ЗЕМЕТИЛИ?

Роман Жуков

ДИРЕКТОР
ЦЕНТРА КОМПЕТЕНЦИЙ

О СПИКЕРЕ

ГАРДА ТЕХНОЛОГИИ

Роман Жуков

Директор центра компетенций

- 9+ ЛЕТ В СФЕРЕ ИБ
- ЗАКАЗЧИК ⇒ ИНТЕГРАТОР ⇒ ОПЕРАТОР ⇒ ВЕНДОР
- УЧАСТНИК ЭКСПЕРТНЫХ ГРУПП (ФСТЭК, ЦБ, МКС)
- ROZHUKOV.BLOGSPOT.COM

О РАЗРАБОТЧИКЕ

ГАРДА ТЕХНОЛОГИИ

ГАРДА ТЕХНОЛОГИИ — РОССИЙСКИЙ РАЗРАБОТЧИК СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Компания обладает многолетним опытом в сфере информационных технологий и разрабатывает решения для различных задач безопасности.

Разработки аппаратно-программных решений информационной безопасности ведутся с 2005 года. Решения Гарды Технологии внедрены в крупнейших компаниях финансового сектора, промышленных предприятиях, телеком-операторах и государственных структурах России и СНГ.

100 +
Внедрений на территории России и стран СНГ

150 +
Высококвалифицированных сотрудников

10 лет
Опыт разработки систем высокой сложности

5
Запатентованных технологий собственного исследовательского центра

ПОЛНОСТЬЮ РОССИЙСКИЕ РЕШЕНИЯ

- Собственная технологическая платформа для хранения информации не требует сторонних лицензий
- Решения сертифицированы ФСТЭК
- Включены в реестр отечественного программного обеспечения

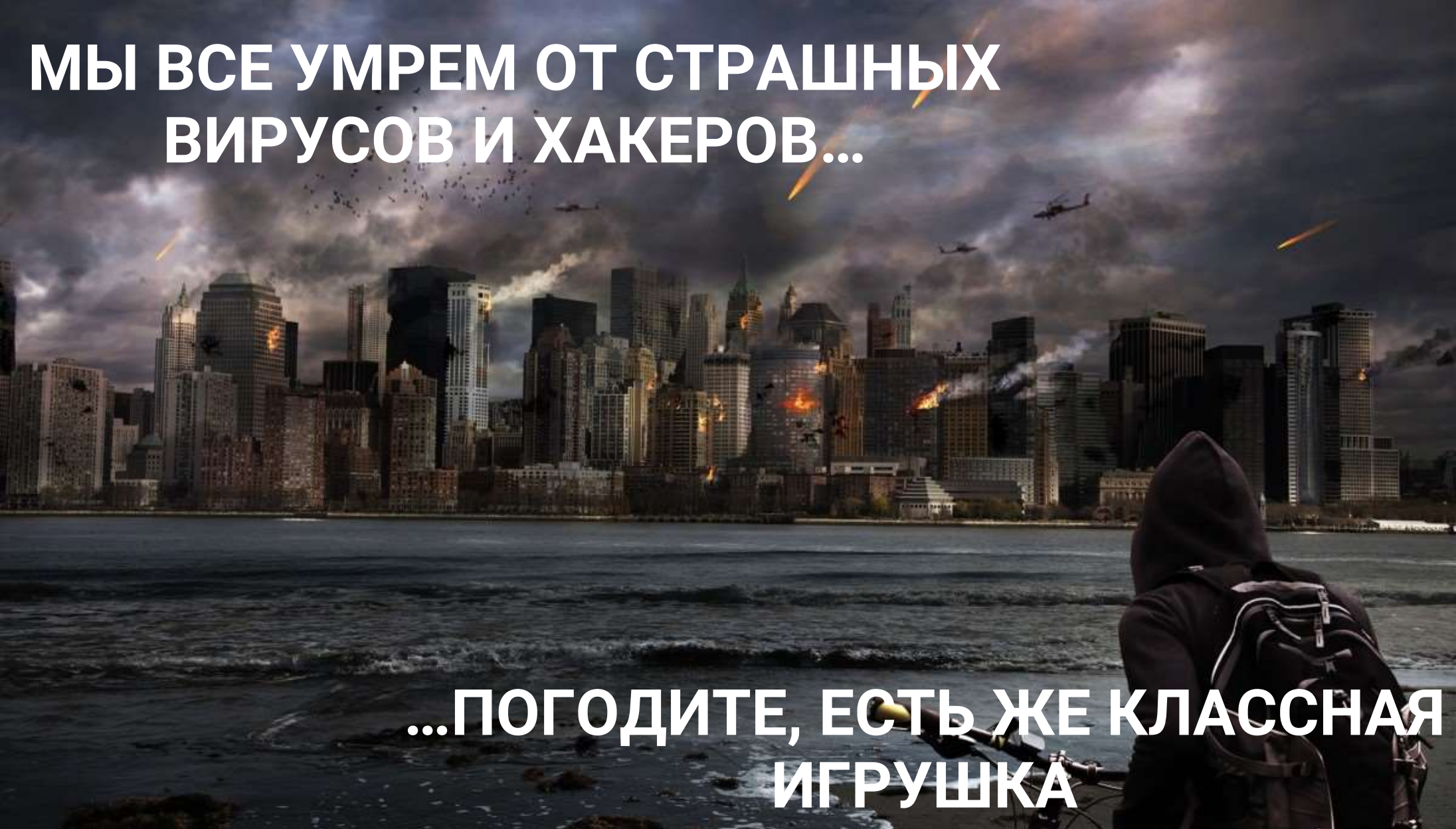
АНОНИМНЫЙ ОПРОС

SCAN ME

СОБЛЮДАЙТЕ РЕГИСТР

bit.ly/
2qfb9Uw

С ЧЕГО ЧАСТО НАЧИНАЮТСЯ ПРЕЗЕНТАЦИИ ПО ИБ


МЫ ВСЕ УМРЕМ ОТ СТРАШНЫХ ВИРУСОВ И ХАКЕРОВ…
…ПОГОДИТЕ, ЕСТЬ ЖЕ КЛАССНАЯ ИГРУШКА

DISCLAIMER

ГАРДА ТЕХНОЛОГИИ

НЕТ СКРЫТОЙ РЕКЛАМЫ,
ВСЕ СОВПАДЕНИЯ СЛУЧАЙНЫ

МАКСИМУМ СОЗИДАНИЯ, ПРИМЕРОВ И ПРАКТИКИ

КАРТИНКИ ПРИВЕДЕНЫ
ИСКЛЮЧИТЕЛЬНО
В ЦЕЛЯХ ДЕМОНСТРАЦИИ

ГАРДА
ТЕХНОЛОГИИ

НА ЧЕМ ГЛАВНЫЙ ФОКУС ИБ В КОМПАНИЯХ

ЧТО МЫ ЗАЩИЩАЕМ

ГАРДА ТЕХНОЛОГИИ

ПК VIP-ПЕРСОН

БИЗНЕС-СИСТЕМЫ

WEB-ПРИЛОЖЕНИЯ

ПОЛЬЗОВАТЕЛИ

АДМИНИСТРАТОРЫ

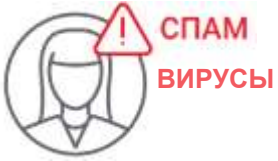
ОТ ЧЕГО МЫ, КАК ПРАВИЛО, ЗАЩИЩАЕМЩАЕМ

ГАРДА ТЕХНОЛОГИИ

ПК VIP-ПЕРСОН

БИЗНЕС-СИСТЕМЫ

WEB-ПРИЛОЖЕНИЯ



СПАМ

ВИРУСЫ

АРТ-АТАКИ

ПОЛЬЗОВАТЕЛИ

АДМИНИСТРАТОРЫ

БОТЫ

ХАКЕРЫ

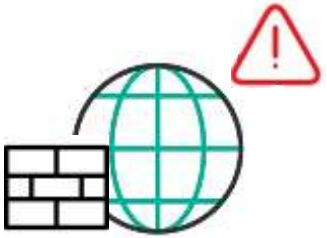
DDOS

КАК МЫ ЗАЩИЩАЕМ

ГАРДА ТЕХНОЛОГИИ

ПК VIP-ПЕРСОН

БИЗНЕС-СИСТЕМЫ



WAF WEB-ПРИЛОЖЕНИЯ

БОТЫ

UTM (FW/IDS)

ХАКЕРЫ

DDOS

ПОЛЬЗОВАТЕЛИ

АНТИВИРУС

СЗИ ОТ НСД

АДМИНИСТРАТОРЫ

СКАНЕРЫ КОНСОЛИ

ДОРОГИЕ И МОДНЫЕ «ИГРУШКИ»

ГАРДА
ТЕХНОЛОГИИ

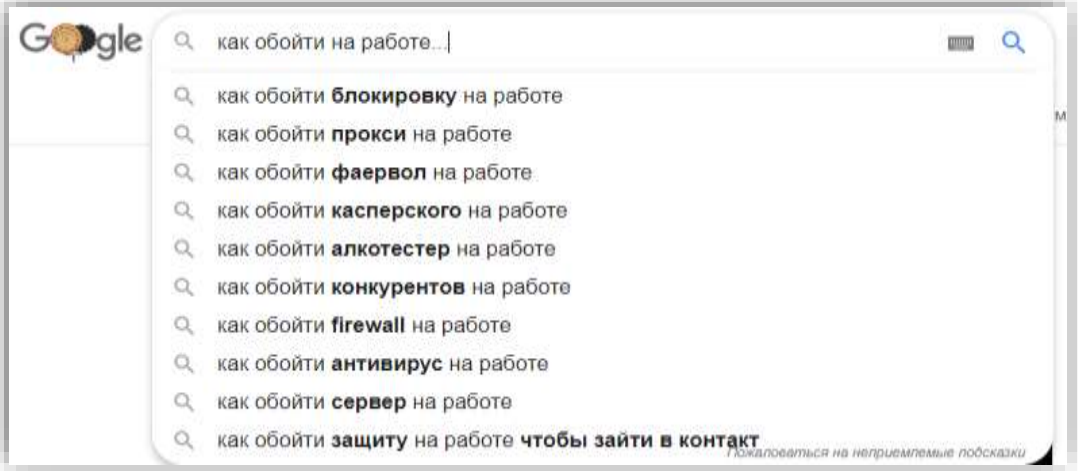
1. SIEM, IRP
2. AntiAPT, EDR
3. Deception
4. DAM/DFM
5. SOAR, BAS, CASB …

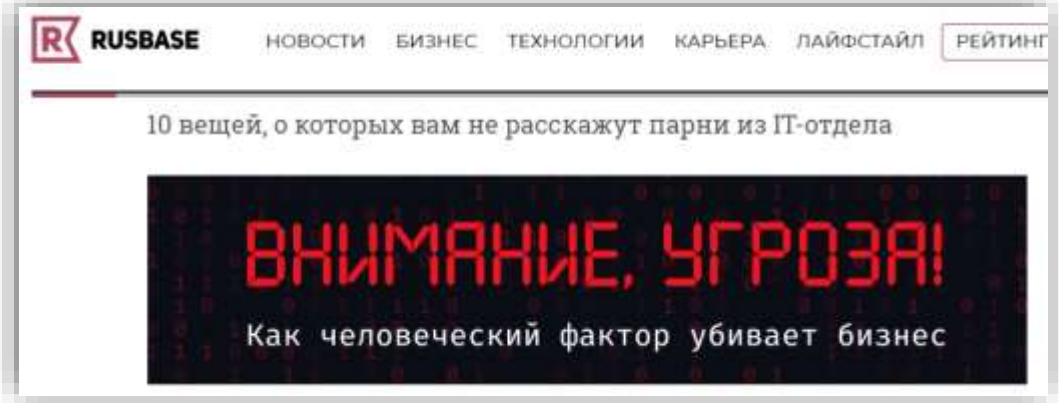
ГАРДА
ТЕХНОЛОГИИ

А ТЕМ ВРЕМЕНЕМ...

ТОП ЗАПРОСОВ СОТРУДНИКОВ В ПОИСКОВИКАХ

ГАРДА ТЕХНОЛОГИИ





- ✓ **Как отправлять большие файлы по почте**
- ✓ **Как использовать ПО, которое компания запрещает**
- ✓ **Как заходить на сайты, заблокированные компанией**
- ✓ **Как замести следы на корпоративном ноутбуке**
- ✓ **Как найти рабочие документы из дома**
- ✓ **Как хранить рабочие файлы в онлайне**
- ✓ **Как сохранить тайну личной переписки**
- ✓ **Как получить удаленный доступ к рабочей почте с телефона**
- ✓ **Как сделать вид, что вы работаете**

ДЕЛУ – ВРЕМЯ, ПОТЕХЕ – ЧАС

ГАРДА ТЕХНОЛОГИИ

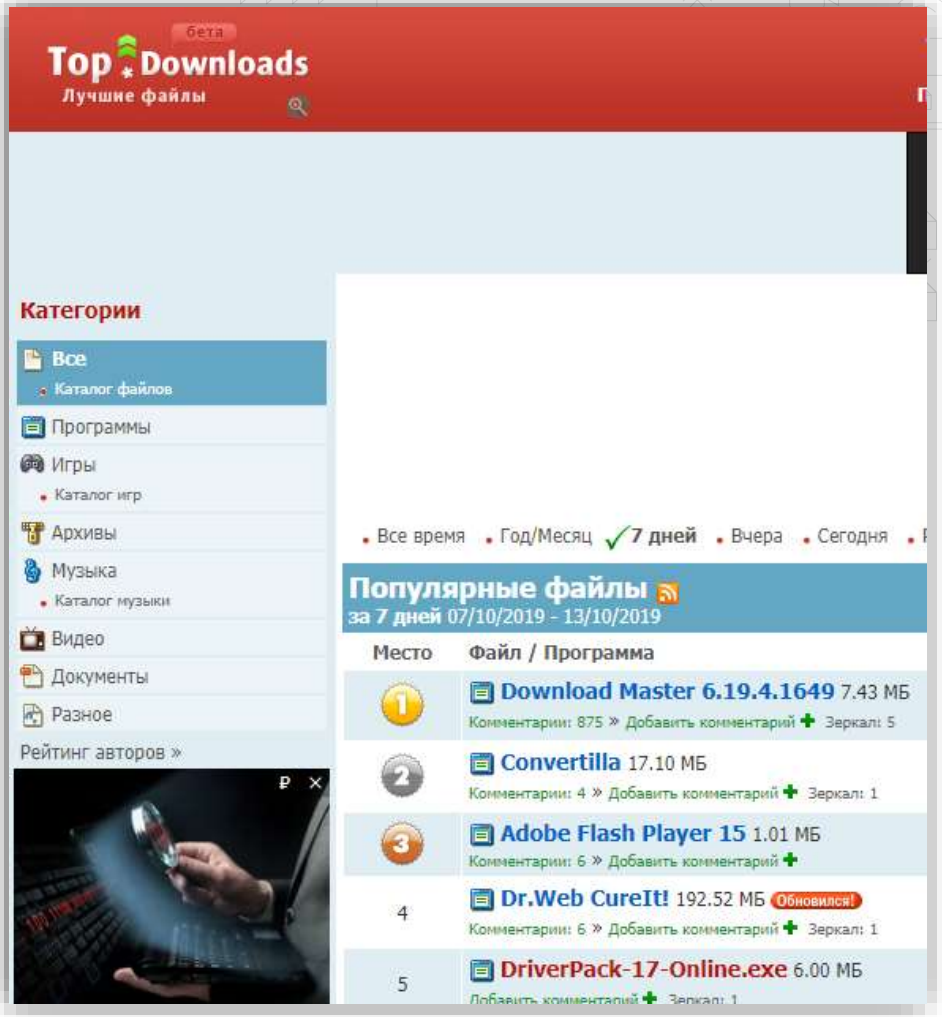
Протокол	UDP ▸ DNS ▸ PLAYSTATION
Списки	Нет данных
Политики	Игровой трафик
HTTP хост	Нет данных
Размер (Б	83.14
	DMZ
Продолжительность сессии	< 1с
IP отправителя	188.1
Порт отправителя	43484
MAC клиента	00:0F:24:57:9D:1B
Аккаунт отправителя	Нет данных
Компьютер клиента	Нет данных
Страна клиента	
IP получателя	83.14

No.		Протокол	Содержание
0		DNS	Standard query 0x73ea A trophy01.np.community.playstation.net
1		DNS	Standard query 0x73ea A trophy01.np.community.playstation.net
2		DNS	Standard query 0x73ea A trophy01.np.community.playstation.net
3	86	DNS	Standard query response 0x73ea CNAME trophy01.np.community.pla g.akamaiedge.net A 88.221.73.194
4	86	DNS	Standard query response 0x73ea CNAME trophy01.np.community.pla g.akamaiedge.net A 88.221.73.194
5	86	DNS	Standard query response 0x73ea CNAME trophy01.np.community.pla g.akamaiedge.net A 88.221.73.194

СКАЧИВАНИЕ ФАЙЛОВ – ПОД ЗАПРЕТОМ? НЕ БЕДА

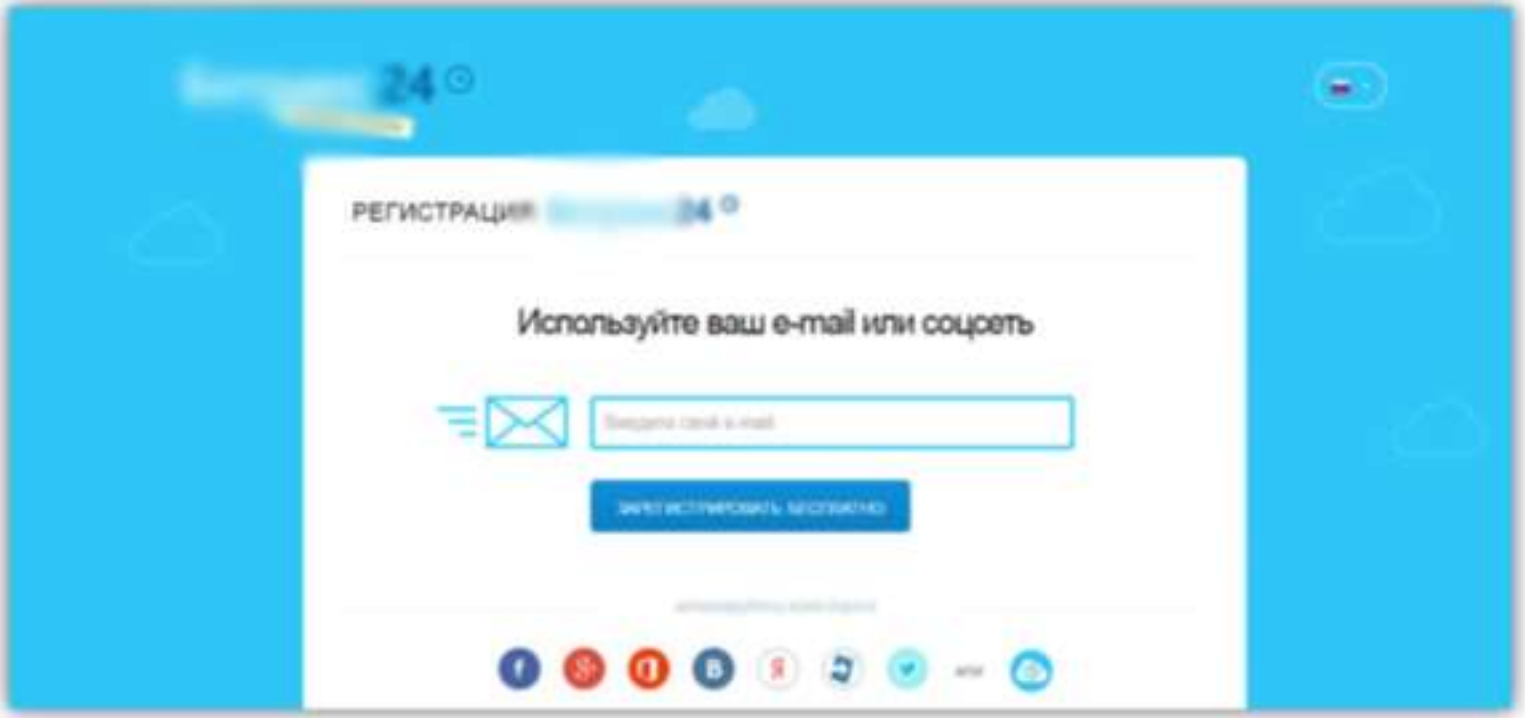
ГАРДА ТЕХНОЛОГИИ

Группа протоколов	Другие
Протокол	TCP ▸ HTTP
Списки	Нет данных
Политики	Нет данных
HTTP хост	Нет данных
Размер (Б)	1402
Продолжительность сессии	1м 0с
IP отправителя	.123.90
Порт отправителя	57435
Аккаунт отправителя	okozlovs@ ru
Компьютер клиента	wsus01. ON.R



АВТОРИЗАЦИОННЫЕ ДАННЫЕ – В ОТКРЫТОМ ВИДЕ

ГАРДА ТЕХНОЛОГИИ



5	0.000000	60	'5.117	.2	TCP	[TCP Dup ACK 5#1] 23545 > http [ACK] Seq=1 Ack=1 Win=8190 Len=0
6	0.000000	1132	'5.117		HTTP	POST /sso/oauth2/tokeninfo?access_token=82d8a60d-6874-4d9b-82d4-43c507923820 HTTP/1.1 (application/json)
7	0.000000	1132	'5.117			
8	0.000000	60	.71.2	3.117	TCP	http > 23545 [ACK] Seq=1 Ack=1079 Win=16170 Len=0

POST /sso/oauth2/tokeninfo?access_token=82d8a60d-6874-4d9b-82d4-43c507923820

МАЛО ПРАВ – НЕ ПОВОД УНЫВАТЬ

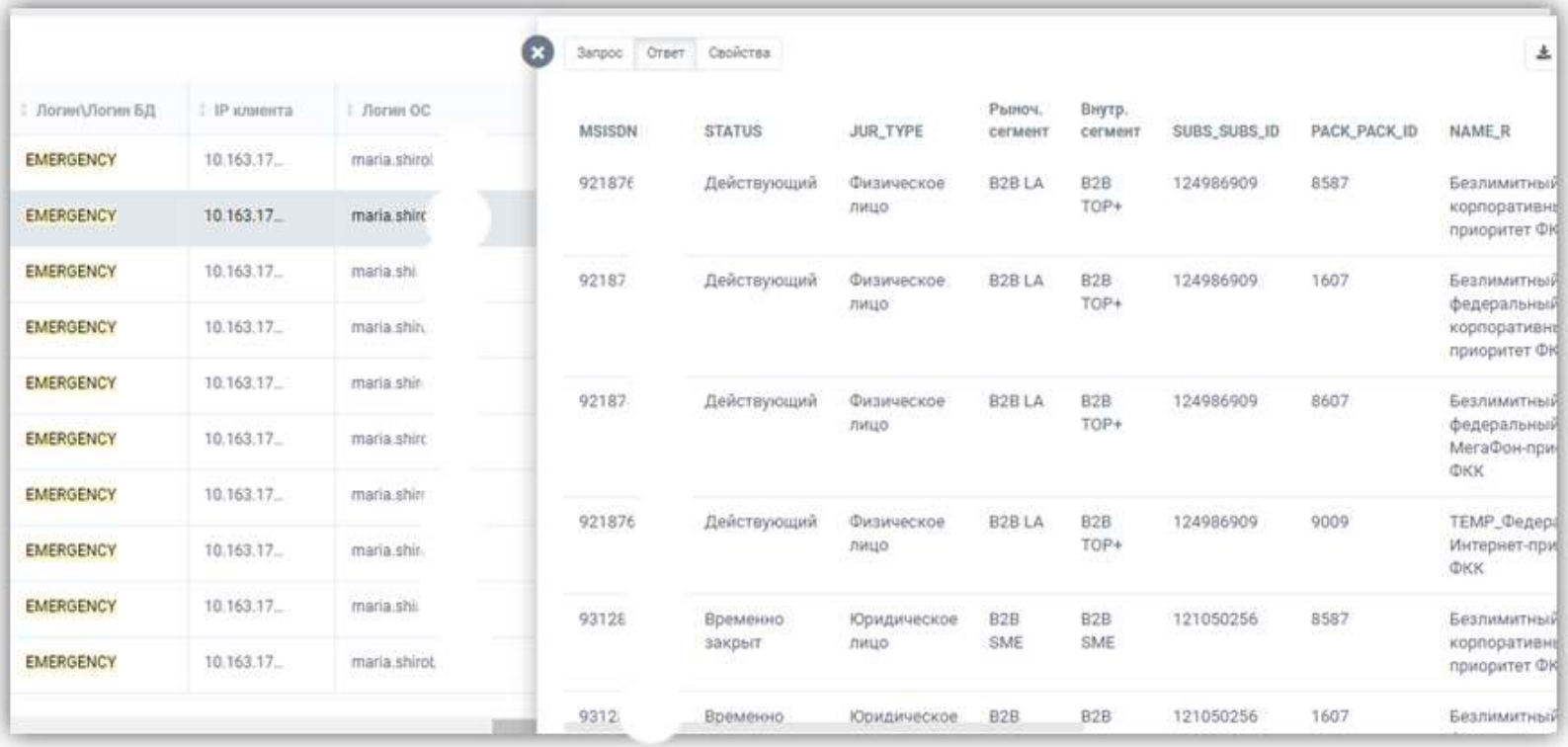
ГАРДА ТЕХНОЛОГИИ

Дата и время	IP источника	IP цели	Название угрозы	Тип угрозы	Уровен...
14.10.2019 12:13:28	5.23	0.230	GPL SQL user name buffer overflow attempt	Попытка повышения привилегий	Высокий
14.10.2019 12:13:28	23	0.230	GPL SQL user name buffer overflow attempt	Попытка повышения привилегий	Высокий
14.10.2019 12:13:27	5.23	0.230	GPL SQL service_name buffer overflow attempt	Попытка повышения привилегий	Высокий
14.10.2019 12:13:27	25.23	0.230	GPL SQL service_name buffer overflow attempt	Попытка повышения привилегий	Высокий
14.10.2019 12:13:26	5.23	0.230	GPL SQL user name buffer overflow attempt	Попытка повышения привилегий	Высокий
14.10.2019 12:13:26	23	0.230	GPL SQL user name buffer overflow attempt	Попытка повышения привилегий	Высокий

Время	Имя БД	Экземпляр БД	Логин\Логин ...	IP клиента	Логин ОС	Приложение	Операции
14 октября 2019 12:07:52	bis_stb	service_g	ps_aniv	63.17...	aniv	plsqldev.exe	Grant
14 октября 2019 12:00:41	bis_stb	service_g	ps_ani	63.17...	aniv	plsqldev.exe	Grant
14 октября 2019 12:00:37	bis_stb	service_g	ps_ani	63.17...	aniv	plsqldev.exe	PL/SQL
14 октября 2019 07:49:14	bis_stb	service_g	ps_an	63.17...	aniv	plsqldev.exe	Grant
14 октября 2019 07:49:02	_stb	service_g	ps_aniv	3.17...	an	plsqldev.exe	Grant
14 октября 2019 07:37:30	s_stb	service_g	ps_aniv	63.17...	aniv	plsqldev.exe	Grant

СЛУЖЕБНАЯ УЧЕТКА – ВСЕГДА ЛУЧШЕ

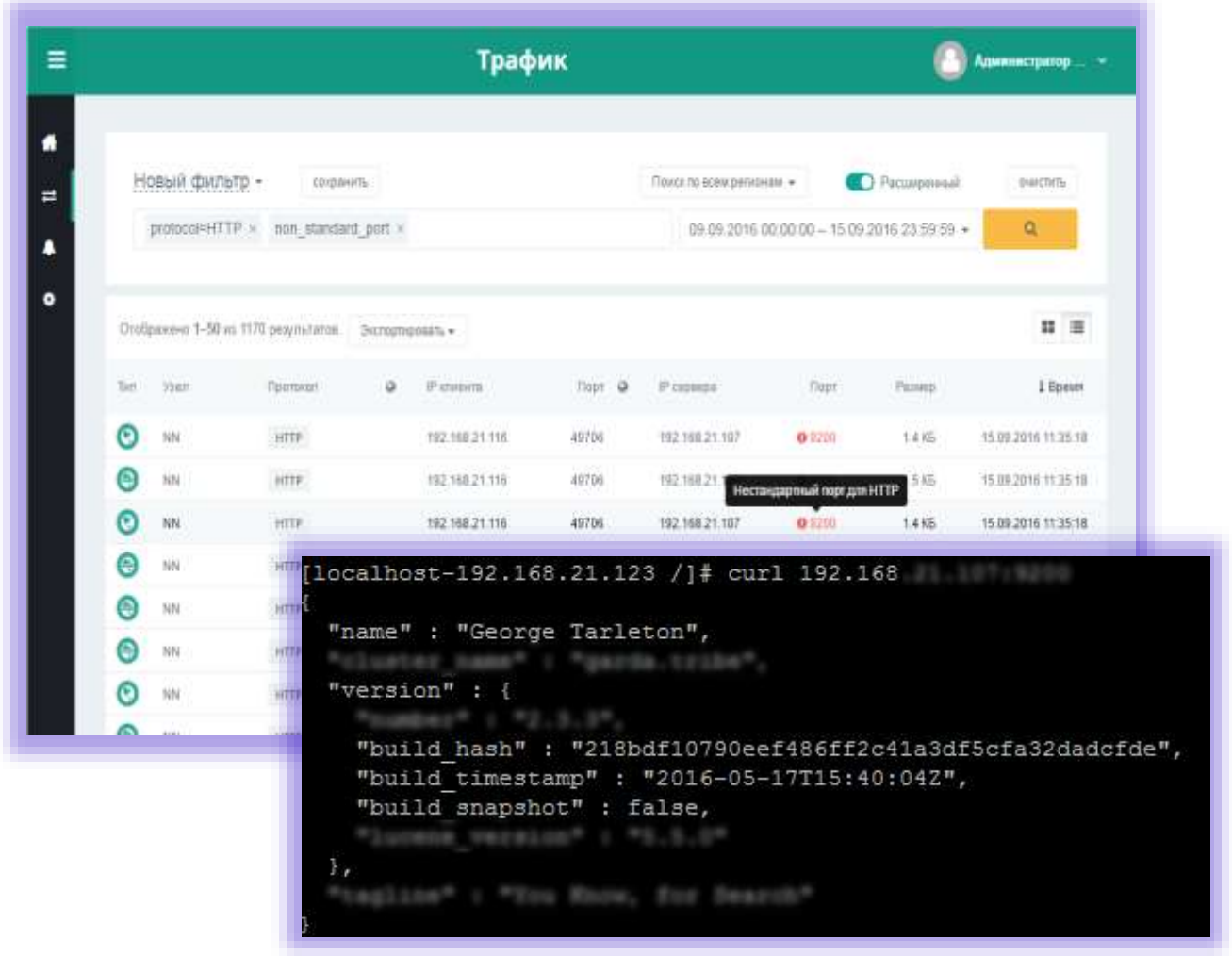
ГАРДА ТЕХНОЛОГИИ



PASSPORT

ПРОТОКОЛ НА НЕСТАНДАРТНОМ ПОРТУ

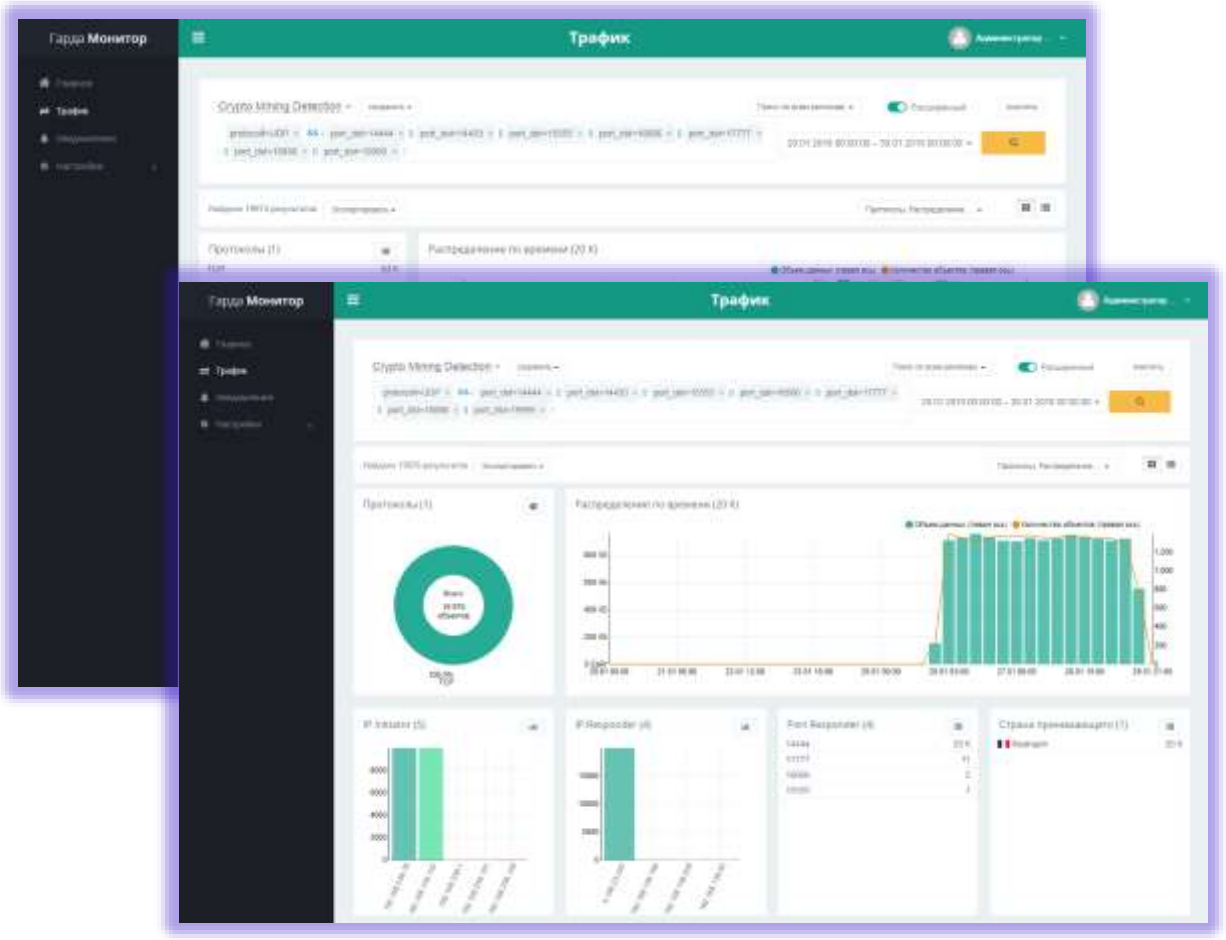
ГАРДА ТЕХНОЛОГИИ



- Обнаружили использование протокола HTTP на нестандартном порту
- Выяснилось, что на сервере компании сотрудник для удобства доступа установил open source продукт
- Default-настройки: открытые порты
- Кто-то уже стучался

МАЙНИНГ НА РАБОЧЕМ МЕСТЕ

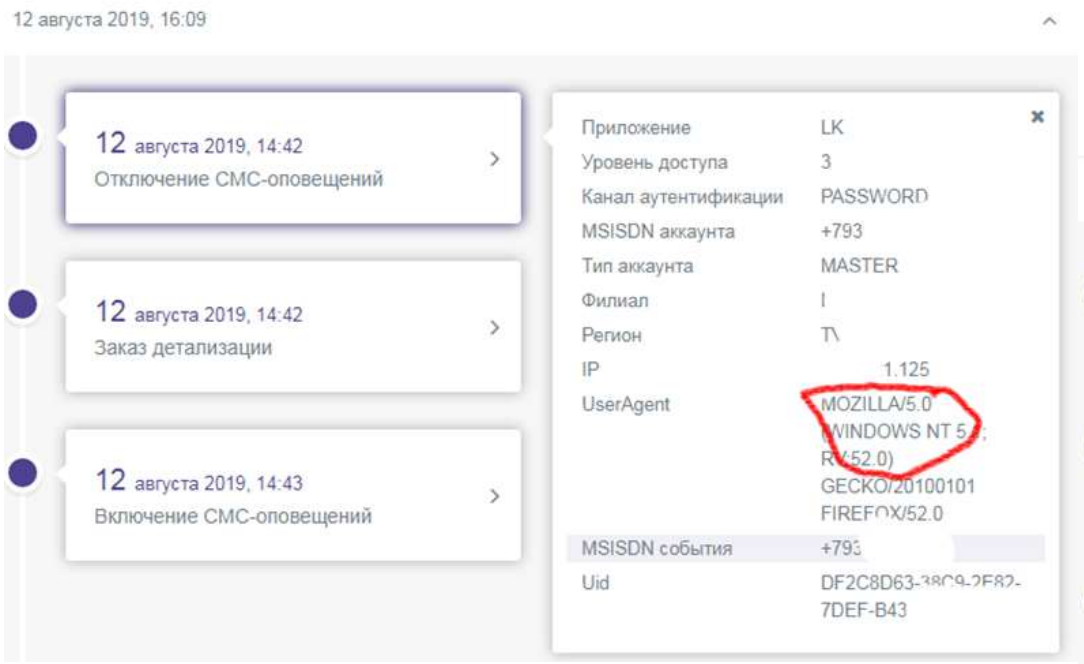
ГАРДА ТЕХНОЛОГИИ

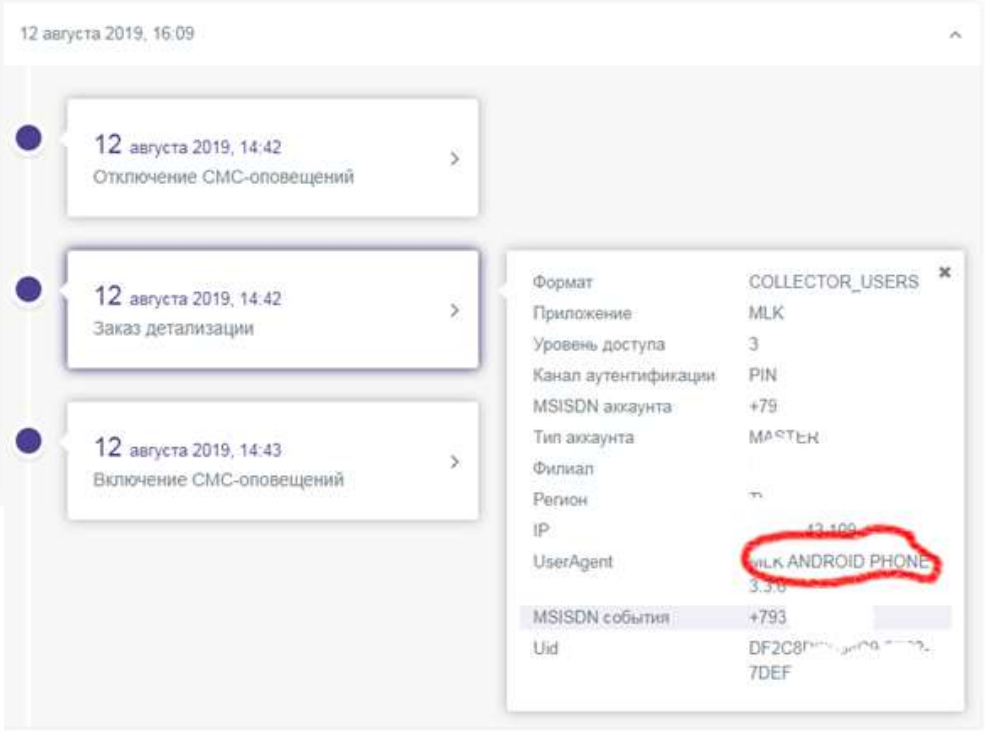


- IP-адрес из «подозрительного» пула
- Обнаружили постоянный трафик на компьютере
- Ретроспектива – не первый случай

МОЖНО ДАЛЕКО ЗАЙТИ...

ГАРДА ТЕХНОЛОГИИ





ГАРДА
ТЕХНОЛОГИИ

ПОЧЕМУ ТАК ПРОИСХОДИТ

ТОП ПРИЧИН

ГАРДА ТЕХНОЛОГИИ

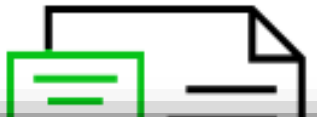
1. Внимание на атаки, а не на инциденты
2. Оповещение – уже по факту атаки
3. Формальные модели угроз
4. Модель нарушителя (даже спецслужбы)
5. Мотивация – только внешняя

МОДЕЛЬ УГРОЗ – В 1 КЛИК

ГАРДА ТЕХНОЛОГИИ

Не нужны специальные знания

Чтобы получить готовый документ вам необходимо только заполнить анкету. Вопросы в анкете просты, поэтому заполнять их может человек, не имеющий специальных знаний в области информационной безопасности. После ввода информации в анкете



Модель угроз безопасности ИСПДн

Сохранить, скачать или распечатать этот документ вы сможете ср
после оплаты

Оплатить 250 рублей

100%
ГАРАНТИЯ

Вернем деньги, если документ не подошел

ВЫСОКИЙ УРОВЕНЬ ДОВЕРИЯ К «СВОИМ»

ГАРДА ТЕХНОЛОГИИ

Модель угроз и нарушителя:

«Наша кадровая политика по подбору персонала – самая лучшая» (с)

НЕТ ОСНОВАНИЙ НЕ ДОВЕРЯТЬ

ПРОНИКНОВЕНИЕ ИТ ТЕХНОЛОГИЙ

УДОБСТВО VIP ПОЛЬЗОВАТЕЛЕЙ

ПСИХОЛОГИЯ, ОТНОШЕНИЯ, ЗАКОН

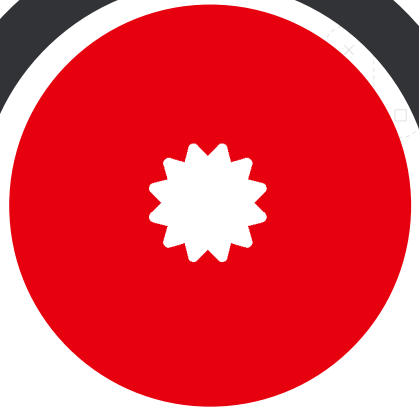
ГАРДА ТЕХНОЛОГИИ

ДОВЕРИЕ «BY DESIGN»

ПОСТОЯННЫЙ КОНТРОЛЬ = ДИСКОМФОРТ

УВАЖЕНИЕ PRIVACY

ЗАКОНЫ ГОСУДАРСТВА



СЛУЖБА ИБ – ВРАГ НАРОДА

ГАРДА ТЕХНОЛОГИИ

1. Всегда все запрещают
2. Создают невыполнимые требования
3. Не понимают трудностей персонала
4. Умеют только наказывать
5. Инструкции – не читабельны

ГАРДА
ТЕХНОЛОГИИ

…ЧТО ДЕЛАТЬ

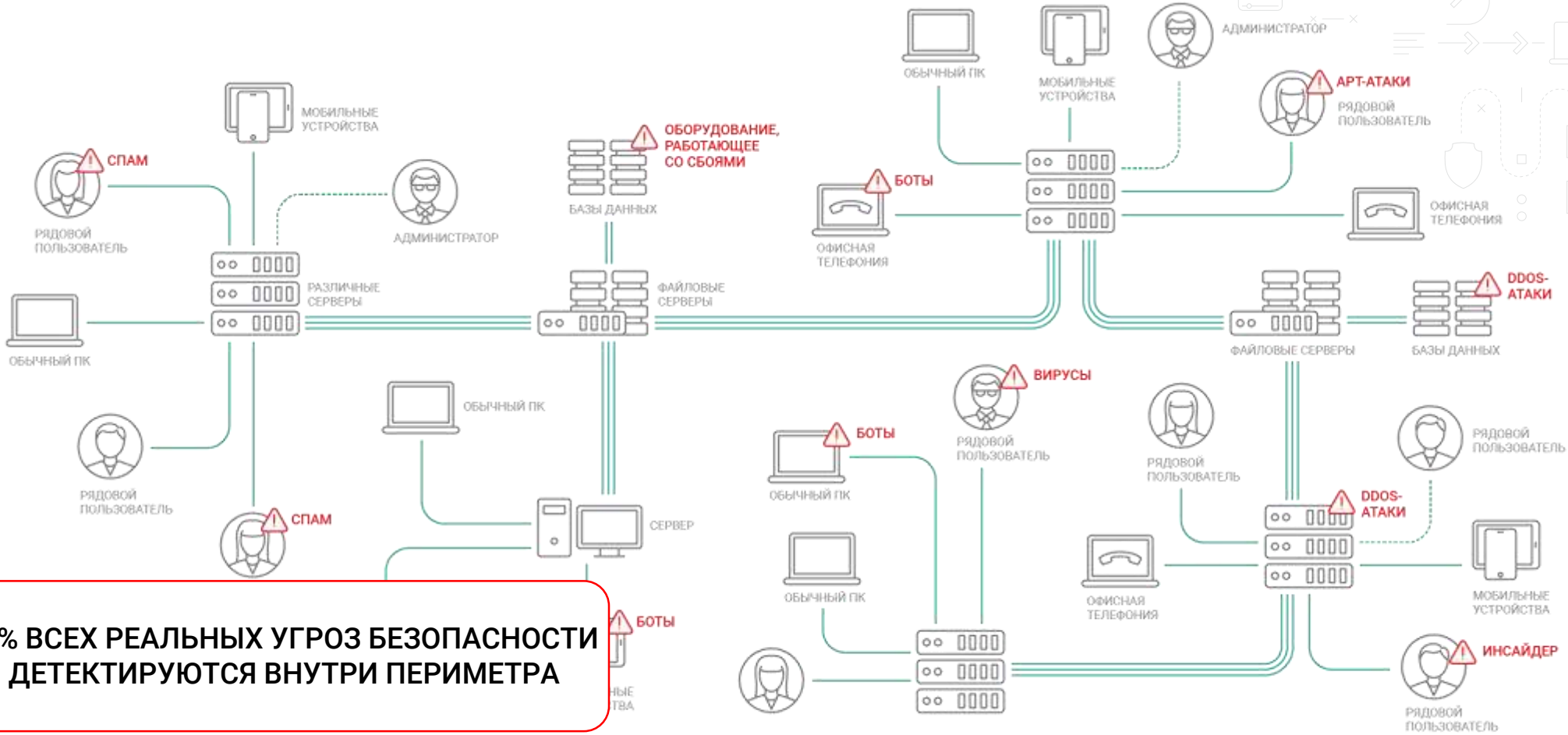
ИНФОРМАЦИОННЫЙ ВАКУУМ

ГАРДА ТЕХНОЛОГИИ

ПЕРИМЕТР VS ENDPOINT

ЧТО ПРОИСХОДИТ У МЕНЯ В СЕТИ?

ГАРДА ТЕХНОЛОГИИ



80% ВСЕХ РЕАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ДЕТЕКТИРУЮТСЯ ВНУТРИ ПЕРИМЕТРА

ЧТО ДЕЛАТЬ БЕЗОПАСНИКУ

ГАРДА ТЕХНОЛОГИИ

1. **Повышать удобство, вводя безопасные сервисы**
2. **Контролировать максимум, запрещать минимум**
3. **Проверки извне и изнутри**
4. **Программы Security Awareness**
5. **Повышение престижа службы ИБ**

РЕЗУЛЬТАТЫ ОПРОСА

ГАРДА
ТЕХНОЛОГИИ

СПАСИБО ЗА ВНИМАНИЕ!

г. Москва, Ленинская слобода, 26\5
8 (495) 116 56 61
info@gardatech.ru
/gardatechnologies
/garda_tech