



Кибергигиена

Кибербезопасность вашего личного цифрового пространства

Ростелеком
Солар

Кибератаки на компании и госсектор

Новые зоны внимания киберпреступников:



Госкомпании



РОИВы



Промышленность



Первые лица
компаний



ФОИВы и системы
госуправления

Новые векторы атак:

- Атаки через ИТ-поставщиков
- Атаки на разработчиков ПО
- Атаки через каркасные ИТ-системы

Цели атак:

- Контроль над ИТ-инфраструктурой
- Конфиденциальная информация
- Парализация работы и вымогательство

Зарубежные жертвы вымогателей:



Новое качество угроз:

в 90%

Компаний отсутствует автоматический или ручной процесс установки обновлений

60%

имеют в своей инфраструктуре признаки ВПО WannaCry, WannaMine

<5 дней

время от появления нового ресурса в домене gov.ru до первой целевой атаки на него

<24 часов

Проходит с момента опубликования уязвимости до появления эксплоита

Кибератаки на страну

Основные киберцели

- ФОИВы
- Федеральные и региональные Госуслуги
- Системообразующие компании
- Объекты критической информационной инфраструктуры

Три плоскости атак

1. **Информационные атаки**, направленные на дестабилизация ситуации
2. **Массовые атаки на web**, направленные на вывод из строя госсервисов
3. **Целевые атаки** на объекты жизнеобеспечения



Кибератаки на физических лиц

Потеря экаунтов и доступов

- Похищение доступов к служебным системам
- Похищение экаунтов к соцсетям и почтам
- Похищение биржевых и банковских экаунтов

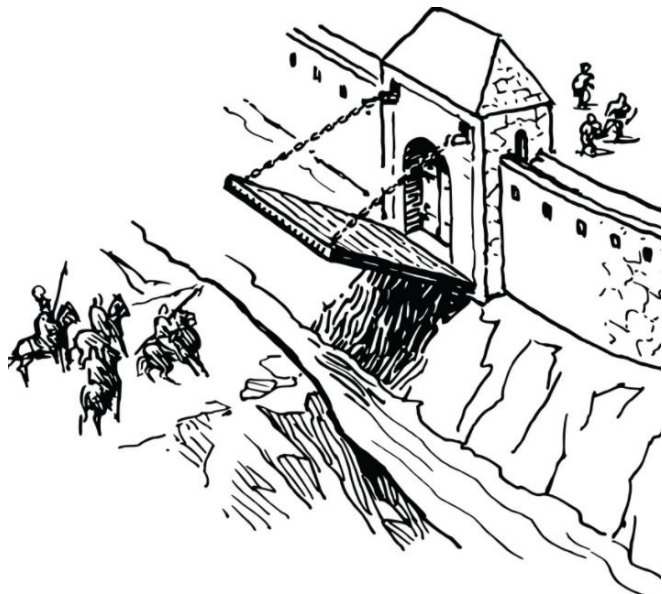
Потеря денег

- Похищение денег со счетов и карт
- Похищение криптовалютных кошельков
- Похищение баллов, кристаллов, танков, игрового прогресса

Шантаж и вымогательство

- Похищение персональных данных и архивов (переписки, фотографий)
- Вы – объект вымогательства
- Вы – объект информационной атаки

Взлом корпоративного ИТ через руководителей



Последствия:

- Утечки служебной информации
- Доступ в информационные системы с уровнем «топ-менеджер»
- Подписание корпоративными ЭЦП
- Бескрайние возможности социальной инженерии

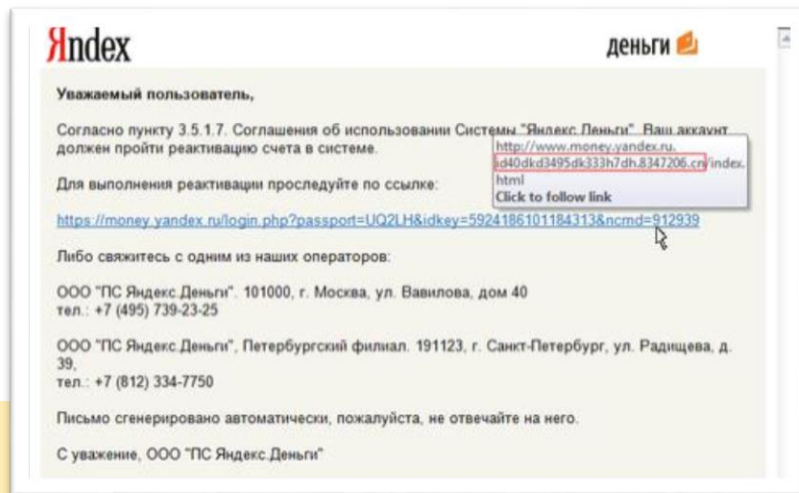
Как реализуется взлом

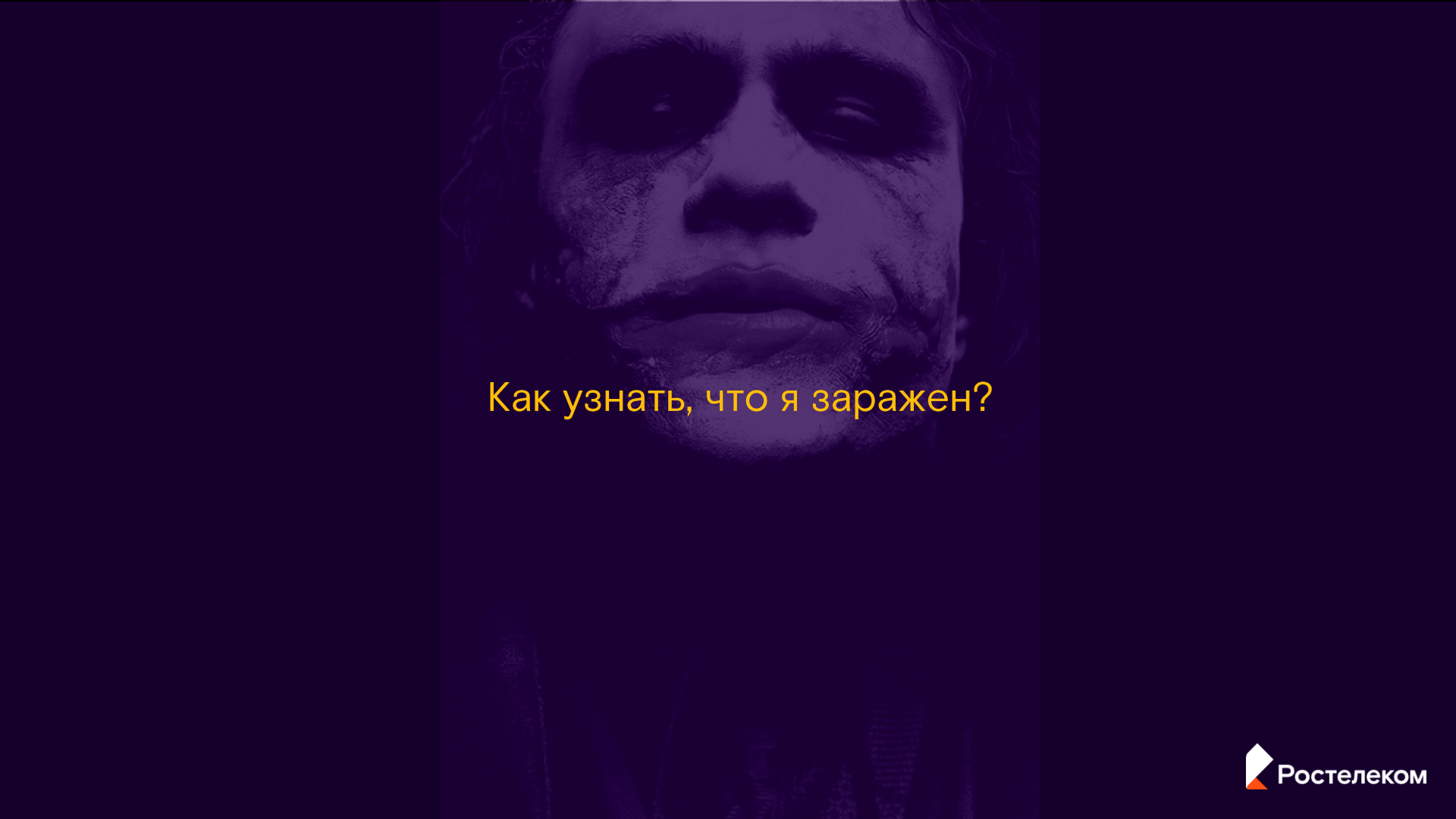
«Широковещательно»

1. Фишинг
2. Социальная инженерия
3. Зловреды на сайтах
4. Утечки баз паролей

«Прицельно»

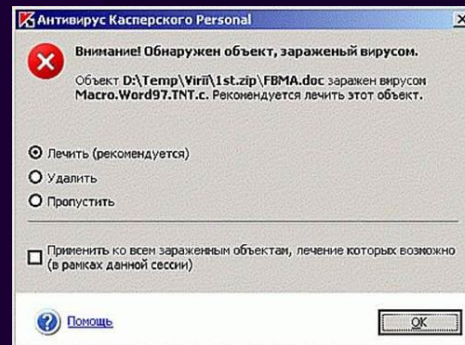
1. Брутфорс эккаунтов
2. Зараженные флешки
3. Взлом через ваших близких и помощников
4. Физический доступ к устройствам



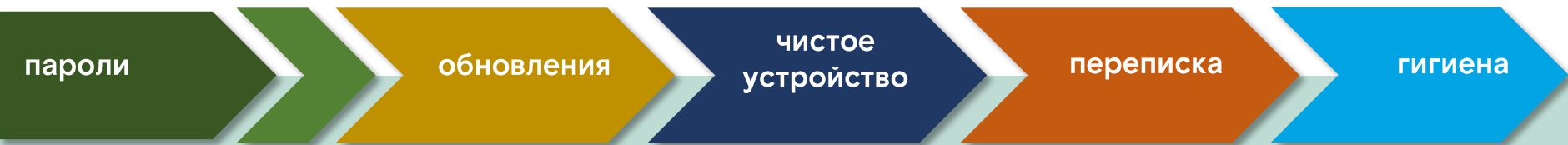


Как узнать, что я заражен?

1. Сообщения антивирусов
2. Правила переадресация почты, которые вы не ставили
3. Запросы подтверждения входов со странных адресов или устройств
4. «Промаргивания» окон особенно в корпоративных системах
5. Сообщения всему вашему контакт-листу от вашего имени



Пять шагов к безопасности



Пароли, пароли и еще раз пароли

пароли

обновления

чистое устройство

переписка

гигиена

Четыре простых правила:

1. Каждому экаунту – свой пароль
2. Сложный пароль
3. Пароль часто меняемый
4. Изменяемый с надежного устройства

!!! А еще нужно везде включить двухфакторную аутентификацию

12345678

Jxtym ckj;ysq gfhjkm!!!

7Ftx3!#

Обновления

пароли

обновления

чистое устройство

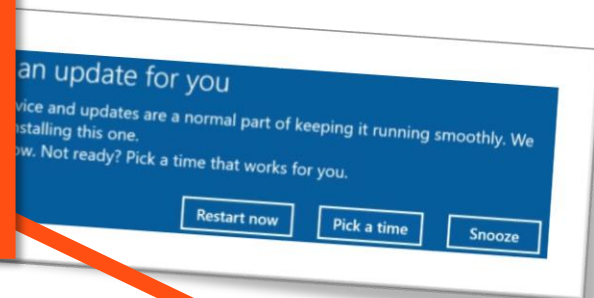
переписка

гигиена

Сколько обновлений
не установлено на телефоне



Сколько дней не обновлен
Windows?



ПОКА ОБНОВЛЕНИЯ
ОТКЛЮЧАЕМ!

Чистое устройство

пароли

обновления

чистое устройство

переписка

гигиена

«Чистое» устройство



Задачи:

- Корпоративные/служебные эккаунты
- Мобильные банки
- Официальные эккаунты социальных сетей
- «Чистый» почтовый ящик
- Мессенджеры

«Грязное» устройство



Задачи:

- Серфинг по интернету
- Игры
- Интернет-магазины
- Почтовый ящик для рассылок
- Фильмы/Музыка
- Торренты
- Дети

Переписка



Публичные почтовые ящики



Обычные
смс-ки



Чаты в whatsapp и telegram



Секретные чаты



Секретные чаты с
автоудалением



ОЧЕНЬ ПЛОХО

ПЛОХО

Корпоративная
почта



А еще важно:

1. Удалите почтовые архивы в личных ящиках, которые лежали «на всякий случай»
2. Включите второй фактор аутентификации

Переписка

пароли

обновления

чистое устройство

переписка

гигиена

1. Не ходите на сомнительные сайты
2. Не открывайте любопытные письма и не нажимайте в них на ссылки
3. Не устанавливайте непонятные программы, тем более не через appstore, google play или официальные сайты
4. Забудьте про публичные wi-fi и автоподключения
5. Чужие флэшки и флэшки с конференций – угроза!

6. И не забудьте, что принцип «один раз не считается» в кибербезопасности не работает!!! 😊

Технологическая не независимость

Устройство

- Купите китайский телефон
- Отключите обновления

Отслеживание

- Отключите геометки
- Проверьте отслеживание

Облачные хранилища

- Перенесите iCloud, Google
- Удалите весь DropBox

Gmail

- Заведите российскую почту
- Сделайте ящик основным при восстановлении

Контакты

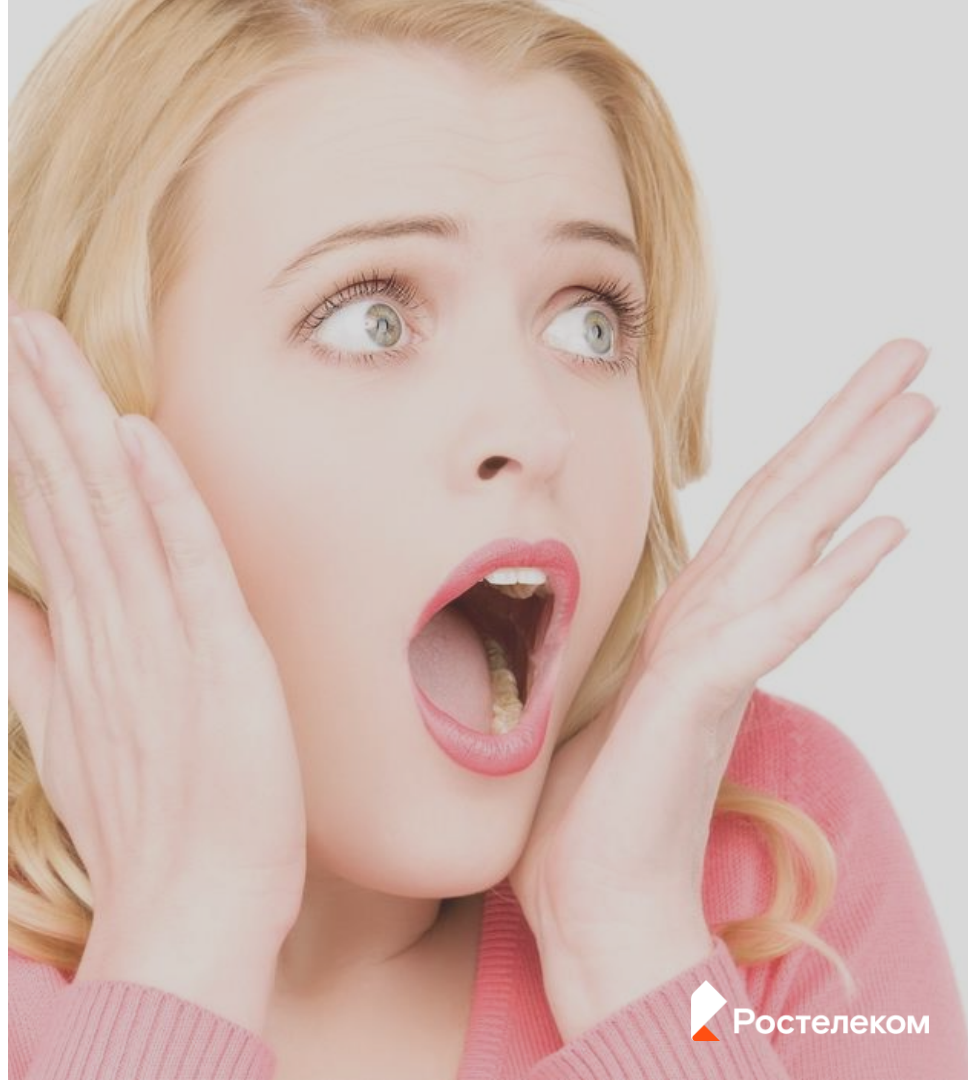
- Ваши контакты в облаке!
- Сделайте резервную копию

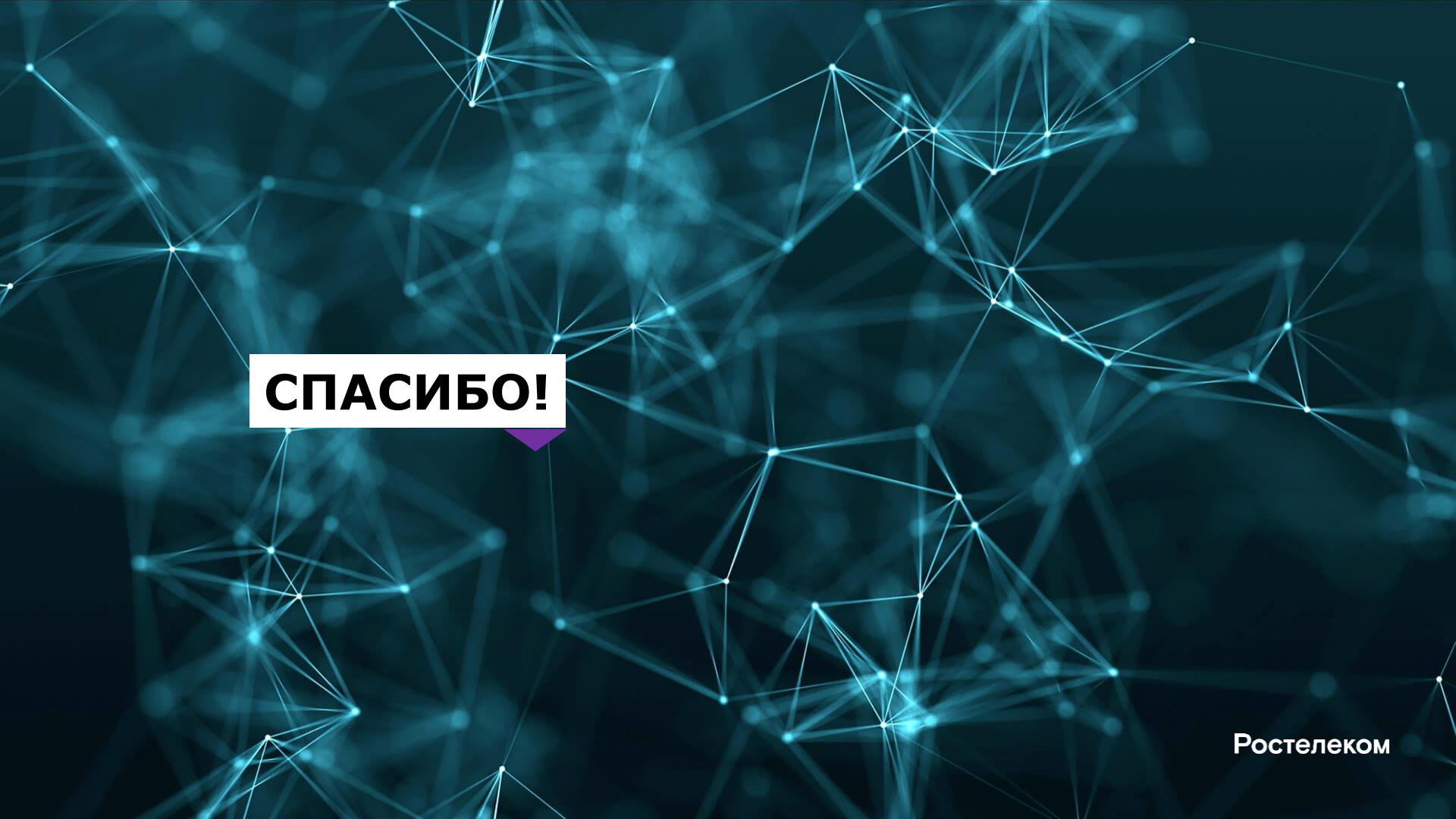
Мессенджеры

- Ключи от них лежат где надо
- Доверенных мессенджеров нет

Если что-то пошло не так...

1. Если у меня вирус...
2. Если я не могу войти в свой экаунт (игровой, почтовый)...
3. Если на моей странице написано что-то странное...
4. Если от меня друзьям приходят странные сообщения...
5. Если у меня украли деньги...





СПАСИБО!

Ростелеком