Ростелеком
Солар

Информационная безопасность. Потенциальные риски, ставшие реальностью

Роман Шапиро

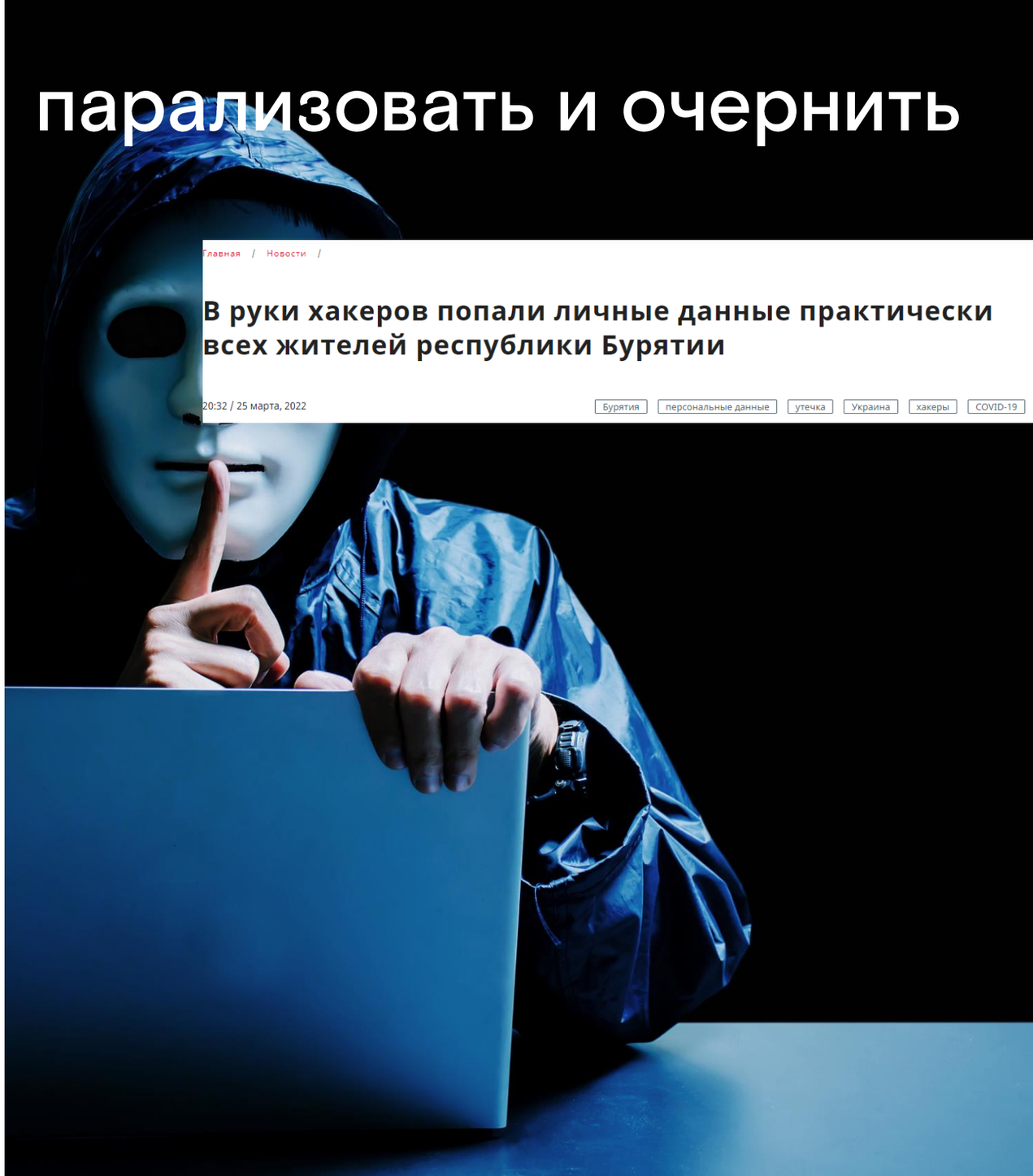
Текущая задача атакующих: парализовать и очернить

Здесь могла бы быть большая статистка:

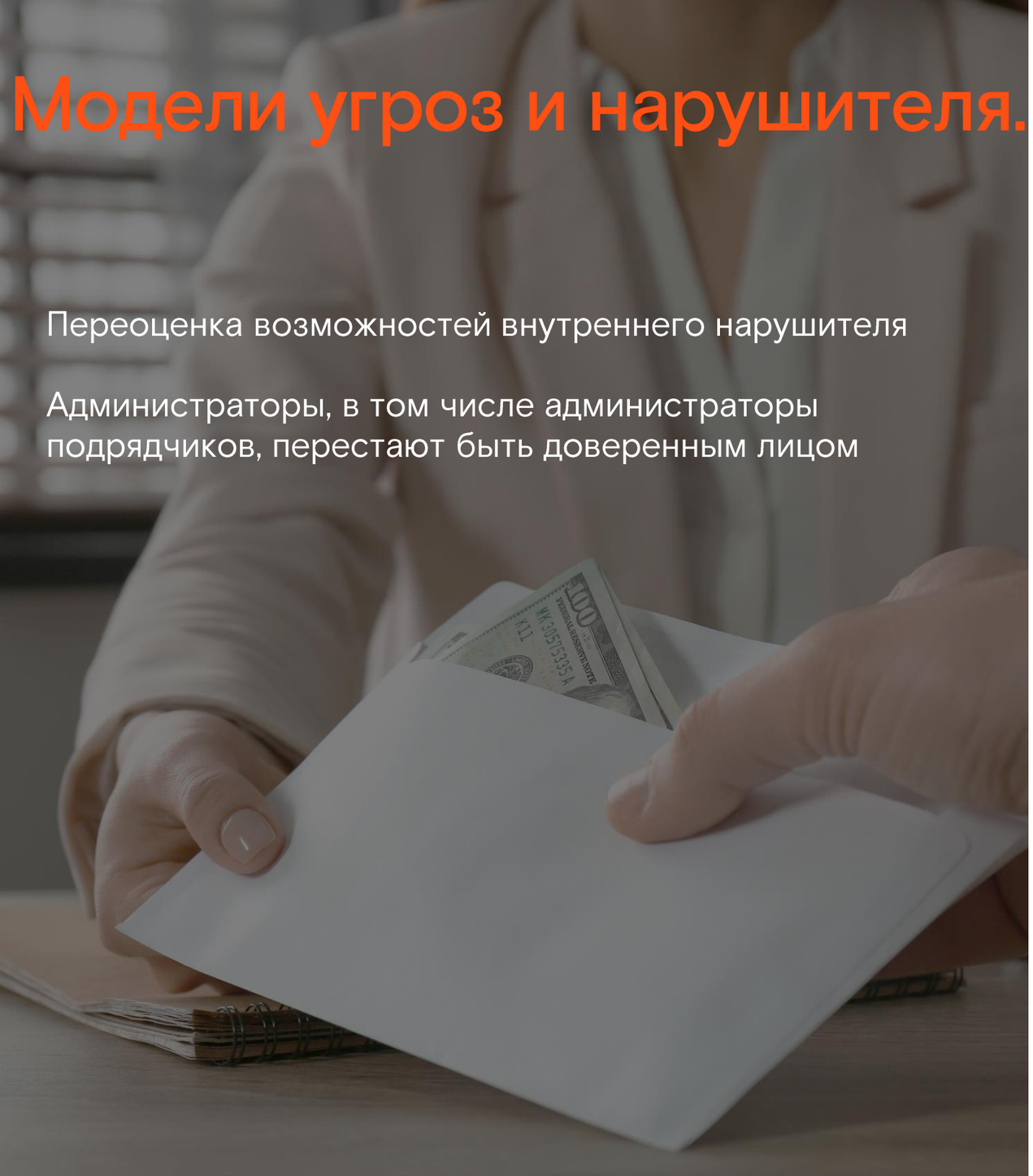
- Об увеличении объема атак, направленных на отказ в обслуживании (включая атаки на удаление DNS-записей, каналы связи и атаки на порталы и сайты на уровне приложений)
- Об иностранных компаниях, прекративших свою работу на территории Российской Федерации
- О взломах и рассказах об успешных взломах, выложенных на суд общественности

Текущая задача атакующих: парализовать и очернить

- DDoS-атаки (уровни канальный и приложений)
- Атаки на DNS-серверы
- Автоматизированный анализ с попыткой эксплуатации любых доступных уязвимостей
- Публикация, в том числе ложная, данных, полученных в ходе атак



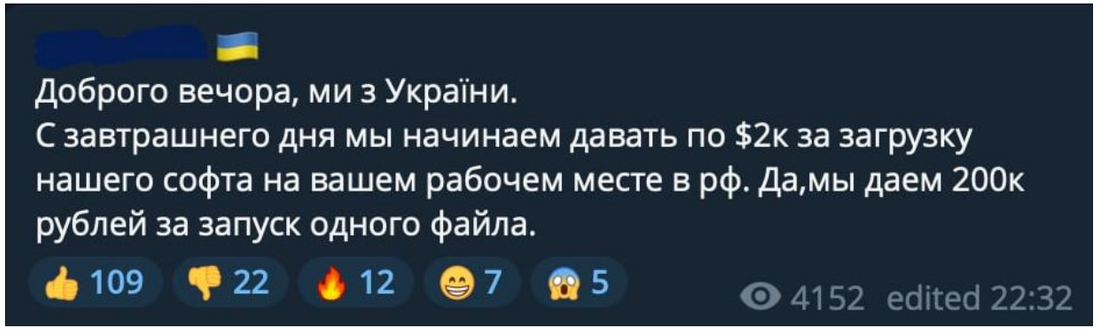
Модели угроз и нарушителя.



Переоценка возможностей внутреннего нарушителя

Администраторы, в том числе администраторы подрядчиков, перестают быть доверенным лицом

Предпосылки переоценки



Ростелеком Солар

Модели угроз и нарушителя.

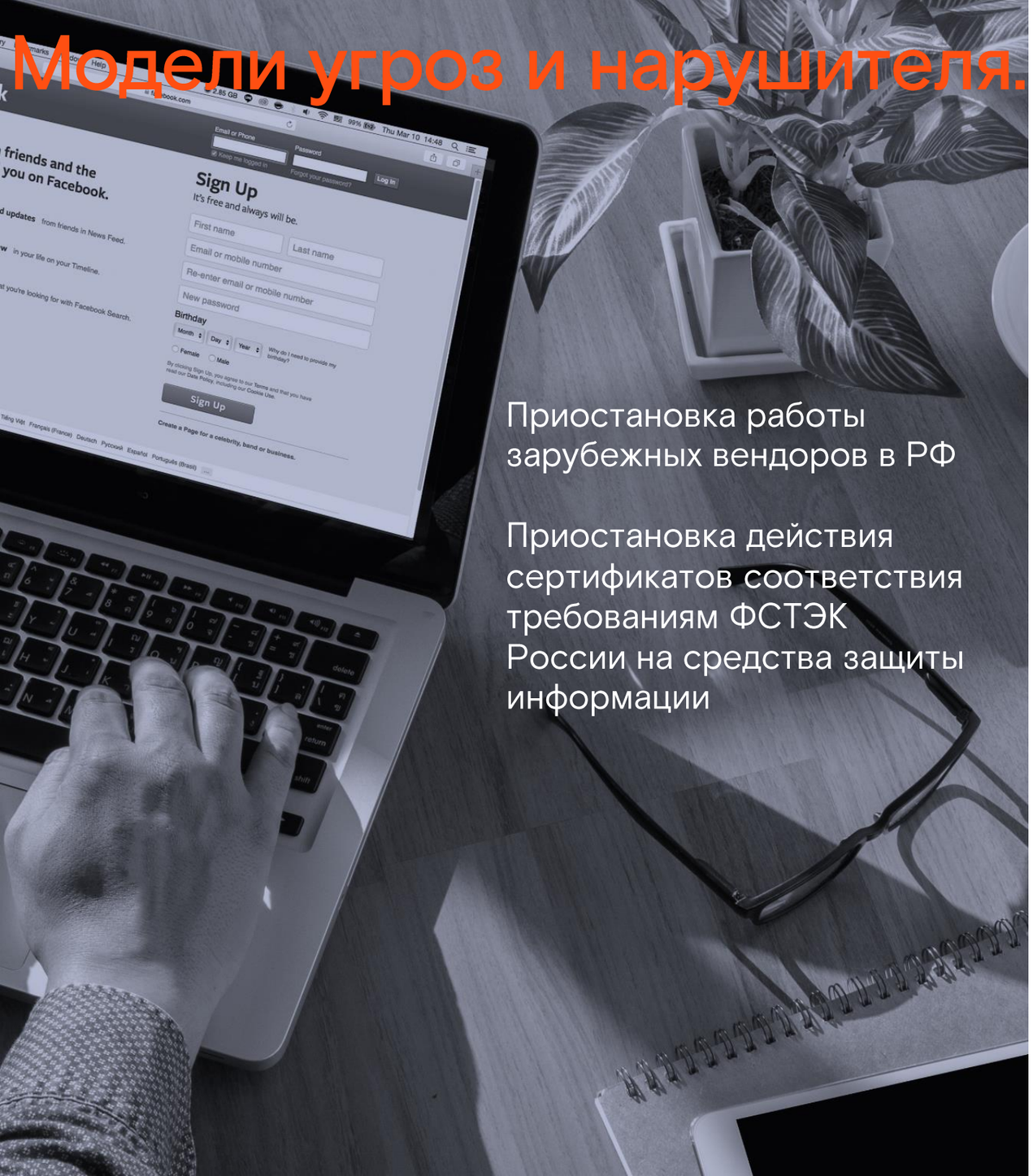
Неисполнение требований SLA по заключенным государственным контрактам в части выполнения требований ИБ

Предпосылки переоценки

- Операторы, предоставляющие услуги Anti-DDoS
- Организации-лицензиаты, предоставляющие услуги центров мониторинга
- Организации-лицензиаты, предоставляющие сервисы в области ИБ

Ростелеком Солар

Модели угроз и нарушителя.



Приостановка работы зарубежных вендоров в РФ

Приостановка действия сертификатов соответствия требованиям ФСТЭК России на средства защиты информации

Предпосылки переоценки

Вендор	Сертификаты соответствия требованиям ФСТЭК России			
	Всего	Действующие	Приостановленные	Действующая ТП
CISCO	223	**42**	2	3
FortiNet	5		3	1
Microsoft	31	**1**	9	10
VMWare	9		4	2
Oracle	11	**1**	1	1
Veeam	2		1	
Huawei	13	**1**	6	
Red Hat Enterprise Linux	3		2	
SUSE Linux Enterprise	4		2	

Ростелеком Солар

Модели угроз и нарушителя.

Администраторы, в том числе прошедшие повышение квалификации по защите информации, не готовы к реальному противостоянию атакам

Предпосылки переоценки

- Средства защиты информации требуют постоянной работы с ними
- План действий, которые будут предприняты при защите, не тождественен реальным действиям
- Режим работы администратора чаще всего не подразумевает круглосуточной работы

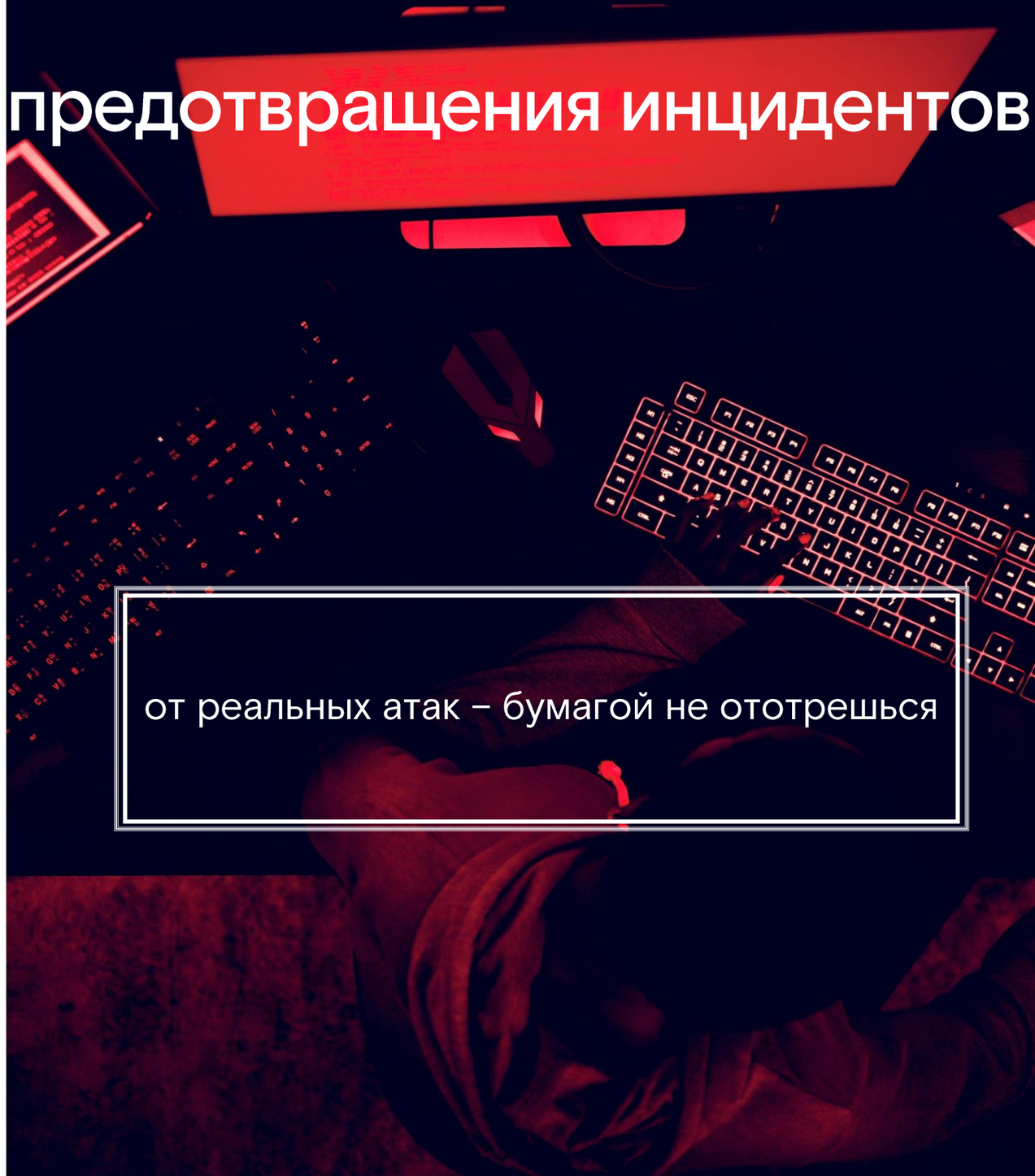
Ростелеком Солар

Оперативные действия для предотвращения инцидентов

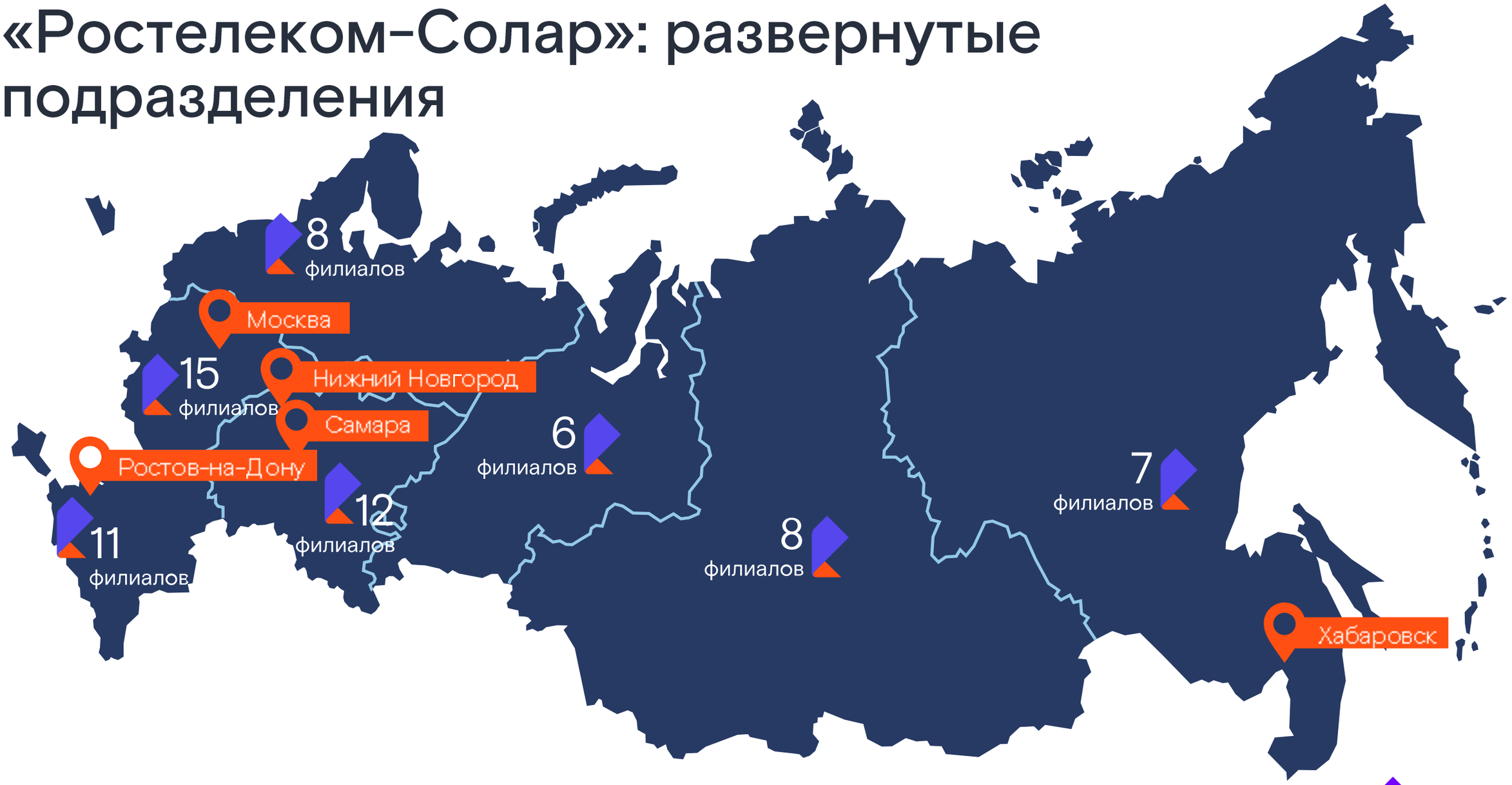
Быстрое развертывание сервисов ИБ, в том числе под атакой: Anti-DDoS (уровень канала связи и уровень приложений), защита электронной почты, межсетевое экранирование, анализ уязвимостей, повышение осведомленности сотрудников

Обеспечение мониторинга и реагирования совместно с организациями-лицензиатами в форматах: обучение и построение собственного SOC; внешний постоянный мониторинг; внешний мониторинг и реагирование

Проведение киберучений или тестирование на проникновение в формате Purple Team (атаки и анализ работы защищающейся стороны)



«Ростелеком-Солар»: развернутые подразделения



ПАО «Ростелеком»

Филиалы Solar JSOC

Ростелеком Солар

Центральный офис:

125009 г. Москва, Никитский переулок, 7с1

+7 (499) 755-07-70

info@rt-solar.ru