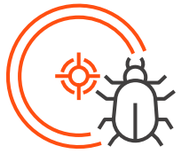
Ростелеком
Солар

Экономика ИБ: по обе стороны баррикад

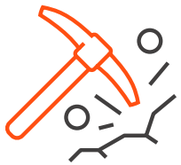
Дарья Кошкина
Руководитель направления аналитики киберугроз
«Ростелеком-Солар»

Аналитика «Ростелеком-Солар»

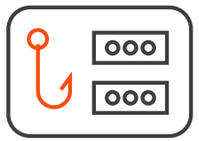


Самые распространенные инциденты: **заражение ВПО и сетевые атаки**

Наиболее часто атакам подвергаются **компании SMB**

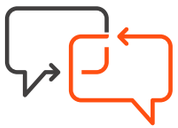


Стоимость проведения атаки постепенно **снижается** в связи с доступностью инструментария



Фишинг по-прежнему **остается основным инструментом** киберпреступников

10% российских компаний (30 тыс. юридических лиц) **уже заражены ВПО**



Предание инцидента огласке **увеличивает сумму убытков** как минимум **в 2 раза**

Это может привести к **ущербу** как минимум в **45 млрд руб.**

1,5-2% от общего числа подозрений на инциденты ИБ являются **подтвержденными критическими инцидентами**

Ростелеком Солар

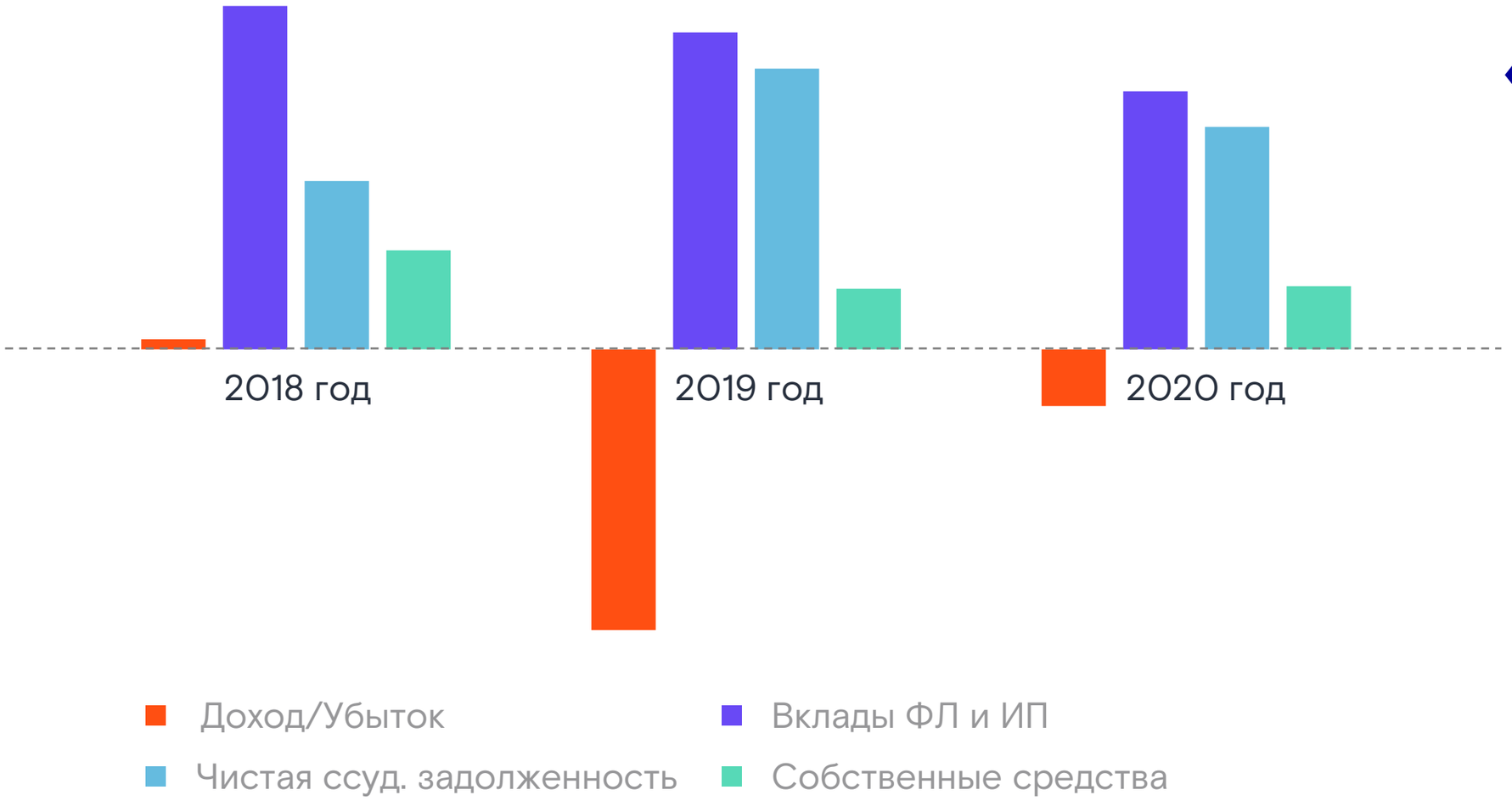
Уровни злоумышленников

	УСЛОВНАЯ КАТЕГОРИЯ НАРУШИТЕЛЯ	ТИПОВЫЕ ЦЕЛИ	ВОЗМОЖНОСТИ НАРУШИТЕЛЯ
1	Автоматизированные системы	Взлом устройств и инфраструктур с низким уровнем защиты для дальнейшей перепродажи или использования в массовых атаках	Автоматизированное сканирование
2	Киберхулиган/ Энтузиаст-одиночка	Хулиганство, нарушение целостности инфраструктуры	Официальные и open-source-инструменты для анализа защищенности
3	Киберкриминал/ Организованные группировки	Приоритетная монетизация атаки – шифрование, майнинг, вывод денежных средств	Кастомизированные инструменты, доступное вредоносное ПО (приобретение, обфускация или разработка), доступные уязвимости, социнжиниринг
4	Кибернаемники/ Продвинутые группировки	Нацеленность на заказные работы – сбор информации, шпионаж в интересах конкурентов, последующая крупная монетизация, хактивизм, деструктивные действия	Самостоятельно разработанные инструменты, приобретенные zero-day-уязвимости ПО
5	Кибервойска/ Проправительственные группировки	Кибершпионаж, полный захват инфраструктуры для возможности контроля и применения любых действий и подходов, хактивизм	Самостоятельно найденные zero-day-уязвимости ПО и АО, разработанные и внедренные «закладки»

Ростелеком Солар

Атака на «ИТ Банк»

В начале 2019 года кибератаке подвергся омский «ИТ Банк».
Атака имела массовый характер и была нацелена на весь банковский сектор.



«ИТ Банк»

294-е место в
рейтинге по активам

20+ млн

было выведено в
результате атаки

Ростелеком Солар

Стоимость инцидента: нападение

- ✓ **Минимальный набор**, необходимый для проникновения и фактически поддержания своего присутствия, **в который входят:**
  - **технология fast-flux**
  - **5 УЗ для входа**
  - **RAT**
  - **простой шифровальщик**
  - **PROXY**
- ✓ **Готовое разноплановое ВПО**
- ✓ **Ботнет для спама, майнинга**
- ✓ **Покупка набора готовых уязвимостей** для последующей компрометации
- ✓ Проведение **фишинговой атаки**
- ✓ Проведение **атаки программы-вымогателя/трояна** (одна кампания)
- ✓ **Шаблоны** для поддельных документов, веб-сайтов, мобильных приложений
- ✓ **Набор инструментов на этапе закрепления и горизонтального перемещения (для 3-го и 4-го уровней)**
- ✓ **Расширенная версия сертификата** для подписи кода

<0,5 млн ₽ - стоимость базовой атаки с применением шифровальщика

Ростелеком Солар

Стоимость инцидента: атакуемый объект

Атака на средний банк

Использован шифровальщик

20 сотрудников пострадали

Основной простой – 2 рабочих дня

Полное восстановление – 14 дней

Прямой ущерб от простоя (простой специалистов + восстановление + снижение эффективности)	**1 407 272,73 ₽**
Ущерб для бизнес-процессов (утраченная информация, причинение вреда инфраструктуре)	**900 000,00 ₽**
Пострасходы (упущенная выгода, восстановление репутации, отток клиентов)	**1 700 000,00 ₽**
Итого:	**4 007 272,73 ₽**

Ростелеком Солар

Базовый инструментарий для защиты

Элементы ИБ*, обеспечивающие защиту от злоумышленников 2-го и 3-го уровней:

- Антивирус
- Песочница (Sandbox)
- Базовый SOC
- Защищенный Wi-Fi
- Грамотная политика безопасности
- Патч-менеджмент
- Периодическое сканирование на наличие уязвимостей

6-7 сотрудников
службы ИБ/аутсорсинг

регулярное **повышение их квалификации**

Компания развивается

Наращивается ИБ

** Компаний с примерной численностью 1000 сотрудников*

Ростелеком Солар

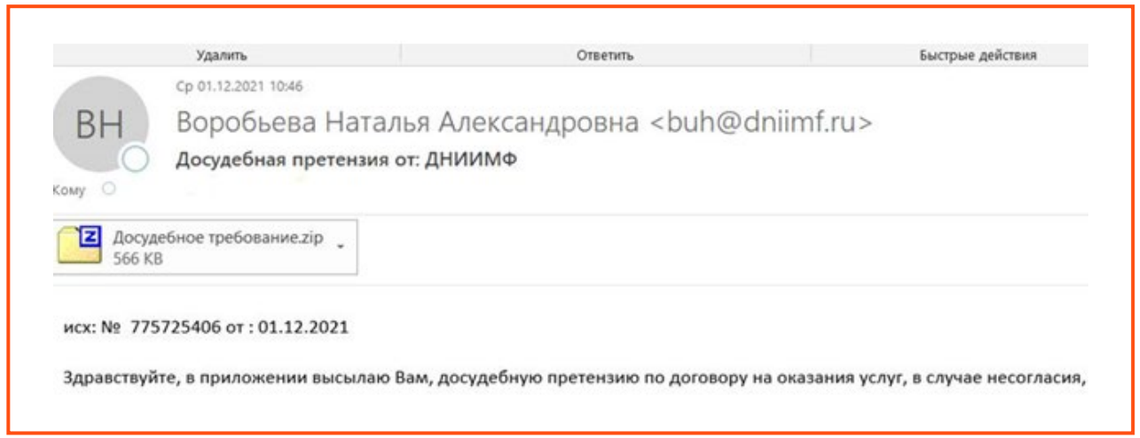
А траты оправданны?

	Инвестиции	Потенциальные потери
Для компании до 1 тыс. сотрудников	**10–15 млн ₽**	**13 млн ₽ совокупно***, в последующие 2–3 года: • отрицательные финансовые показатели (снижение прибыли, отток клиентов, задолженность и т. д.) • расходы на восстановление (ИБ, PR, расследование, контрагенты)
Для компании в 2–3 тыс. сотрудников	**25–30 млн ₽**	**28 млн ₽ совокупно***, в последующие 2–3 года: • отрицательные фин. показатели (снижение прибыли, отток клиентов, задолженность, страховая премия и т. д.) • расходы на восстановление (ИБ, PR, расследование, контрагенты) • падение стоимости акций • предание инцидента огласке

** От атак 2 и 3го уровней нарушителей*

Ростелеком Солар

Возврат инвестиций: миф или реальность?



Sandbox на почтовый трафик:
800 тыс. ₽/год

Сведение к минимуму фишинговых атак и, как следствие, **заражений ВПО**

Заражение ВПО в результате фишинговой атаки*:

- расходы на ИТ-специалистов: **36 тыс. ₽**
- простой сотрудников: **290 тыс. ₽**
- ущерб для бизнес-процессов: **250 тыс. ₽**

х 2-3 инцидента в год

1,5 млн ₽ минимальный ущерб от киберинцидентов за год (без учета проведения техрасследований и «пострасходов»)

Решение – превентивная защита

Экономия средств **уже в первые 2 года** пользования сервисом

**По данным «Ростелеком-Солар», 75% всех атак – это фишинг*

Ростелеком Солар

Прогнозы и выводы

1

ИБ – необходимый элемент в развитии бизнеса

2

ИБ оказывает положительное влияние на репутацию компании

3

Построение системы защиты – это не всегда дорого, в отличие от возможных убытков

4

Система защиты должна быть релевантна уровню злоумышленника, под прицел которого может попасть компания

5

Внедрение ИТ может способствовать увеличению дохода

6

Киберстрахование остаточных рисков может стать эффективным элементом защиты

Ростелеком Солар

Ростелеком
Солар

Центральный офис

125009, г. Москва, Никитский переулок, 7с1

+7 (499) 755-07-70

solar@rt-solar.ru