

# ДЕНЬ ИНВЕСТОРА POSITIVE TECHNOLOGIES

ноябрь 2023



# Влияние кибербезопасности

на предотвращение недопустимых  
событий в цифровом мире

**Инфобез появился  
задолго до появления  
компьютеров и ИТ  
и будет существовать  
даже если последние  
исчезнут!**





# Звериный оскал информационной безопасности

- Биологические NGFW – хатки бобров, защитный круг стадных животных, термитники...
- Обманные системы – кайенский стриж, болотный крапивник, койот, создающие ложные гнезда, норы и ходы
- Животная криптография – бабочка-павлиноглазка в период спаривания передает сигнал, который могут расшифровать только такие же, как и она
- Бионический пентест – клоп-хищнец маскируется под стройматериалы термитов и проникает внутрь термитника



Павлиноглазка

# Инфобез Древней Греции (VPN «на коленке»)

- Геродот (V век до н. э.) в своей «Истории» описывал, как Гистией обрил голову раба своего, выколол на ней послание и отправил этого раба брату своему Аристокору после того, как волосы выросли
- Эней (IV век до н. э.) в трактате «О перенесении осады» описал множество способов защиты информации и ее тайной передачи: «книжный шифр», листья деревьев, привязанные к ране, кожаный собачий ошейник, сандалии и многое другое
- Защита информации – преимущественно удел государства





# Недопустимое на уровне государства

- 2013 год — раскрытие секретных данных разведки США Эдвардом Сноуденом
  - «Эффект Сноудена» — последствия разоблачения, повлиявшие на общество, государства, технологические компании (потери, по данным Forrester, — около 180 миллиардов долларов только для американских бигтехов)
- 2019 год — кибератака на Венесуэлу, которая привела к отключению электроснабжения в столице Каракасе и во всех 23 штатах
  - Государственные алюминиевые компании Venalum и Vauxilum потеряли электроснабжение и все производство было остановлено, что нанесло ущерб на уровне всего государства



# Атаки на атомную энергетику – это вполне реальность

И это все без истории про Stuxnet

## Инциденты на АЭС, которые могли бы привести к реализации недопустимых событий



pt

### АЭС Browns Ferry, США (2006)

На АЭС произошел аварийный отказ рециркуляционного насоса реактора из-за неисправности контроллера Siemens Perfect Harmony VFD, который оказался перегружен потоком трафика, переданного по промышленной сети.

Операторы были вынуждены остановить третий блок АЭС, так как эта технология имеет важное значение для охлаждения реактора. Причина отправки больших объемов данных, которые можно было бы даже назвать DoS-атакой, так и не была опубликована.

pt

### АЭС Areva (с 2018 года – Orano), Франция (2011)

Этот инцидент, который, к счастью, не имел недопустимых последствий, покрыт завесой тайны, как и многие другие на атомных объектах.

Одни источники уверяли, что компьютерный вирус просто не задел критически важные узлы компании Areva, но другие утверждали, что неустановленные хакеры два года находились внутри инфраструктуры АЭС, а это ставит инцидент в один ряд со злополучным Stuxnet, но без наступления негативных последствий. Третий источник заявлял, что причиной трехдневного простоя стало неурядное обновление системы безопасности.

pt

### Игналинская АЭС, Литва (1992)

Программист, работавший на АЭС, загрузил вредоносный код в автоматизированную систему, отвечающую за работу одной из подсистем реактора, что было одновременно обнаружено. Но кто знает, что могло бы произойти, если бы это не выявили вовремя? Для проведения расследования АЭС была остановлена. Деталей по этому инциденту немного – все-таки с тех пор прошло 30 лет.

pt

### АЭС KHNP, Южная Корея (2014)

Серия кибератак на объекты южнокорейской корпорации Korea Hydro & Nuclear Power началась с заражением вредоносным ПО компьютеров партнеров и бывших сотрудников АЭС с помощью фишингового письма, что привело к утечке данных, касающихся ядерных объектов.

Затем последовал взлом сайта сообщества бывших сотрудников KHNP, а после – рассылка вредоносного письма уже для действующих сотрудников. На этом этапе инцидент был остановлен и ущерб ядерным объектам не был нанесен.

pt

### АЭС Monju, Япония (2014)

Один из восьми компьютеров в комнате управления АЭС оказался зараженным вредоносным кодом после того, как один из сотрудников установил бесплатное ПО, скачанное из интернета.

В результате была украдена конфиденциальная информация, что, судя по всему, и было основной целью хакеров, которые смогли проникнуть в сеть АЭС.

При этом Японское агентство по атомной энергии позже признало, что проигнорировало требования по кибербезопасности атомных объектов. Стоит отметить, что само агентство в ноябре 2012 года уже пострадало от вредоносного кода, но уроков, видимо, не извлекло.

pt

### АЭС Bradwell, Великобритания (1999)

Сотрудник службы безопасности АЭС попытался удалить конфиденциальную информацию в системах предприятия. Это привело к блокированию доступа на АЭС, и персонал не имел возможности зайти и выйти из нее. После инцидента была сформирована рабочая группа и усилены проверки безопасности персонала.

pt

### АЭС Davis Besse, США (2003)

Сотрудник подрядной организации, проводивший регламентные работы на АЭС, в нарушение всех правил подключился к корпоративной сети предприятия. В результате в сеть АЭС попал червь SQL Slammer, который привел к отказу отдельных систем и невозможности мониторить параметры безопасности станции более шести часов.

pt

### АЭС Kudankulam, Индия (2019)

Вредоносное ПО DTrack вышло из строя контроллеры давления в компьютерной сети АЭС. Одни источники уверяли, что атаке подверглись только некоторые сотрудники, кликнувшие по фишинговым ссылкам.

Вместе с тем есть и другая версия, согласно которой вредоносный код все-таки попал внутрь АЭС, но никакой деструктивной функции в себе не нес, однако его целью была кража информации о реакции на бое тория, которую активно разрабатывала Индия.

pt



# Недопустимое на уровне компании

- 2023 год — Okta (производитель решений ИБ) — падение акций на 12% после третьего взлома за год
- 2022 год — Okta — снижение капитализации на 6 млрд долларов
- 2023 год — MGM — 110 млн долларов потерь в Q3 от атаки шифровальщиков (10% от оборота)
- 2017 год — Equifax — 575 млн долларов выплат пострадавшим, 300 млн — в фонд помощи, 1,6 млрд — на укрепление защиты
- 20+ банкротств из-за инцидентов ИБ





# Финансовый ущерб для компаний может измеряться сотнями миллионов долларов

Как отсутствие результативной кибербезопасности в компании приводило к потере крупной суммы денежных средств

Примеры недопустимых событий



pt

Гигант американского ритейла Target (2013)

После утечки 70 млн данных клиентов компания выплатила штраф в размере 18,5 миллиона долларов, 10 миллионов долларов в качестве выплат пострадавшим, 19 и 67 миллионов долларов составили выплаты Mastercard и Visa соответственно, а 39,4 миллиона долларов были выплачены банкам и кредитным союзам. Всего на различные выплаты Target потратил 154 миллиона долларов, а общие потери компании составили 292 миллиона долларов.

pt

Соцсеть Facebook\* (2022)

Компания выплатила штраф в размере 265 миллионов евро за нарушение GDPR.

pt

\*Приведенный Meta, которая признала историческую организацию и управление в России.

Бюро кредитных историй Equifax (2017)

Около 575 миллионов долларов выплатила компания пострадавшим от утечки персональных данных из ее 583 данных, перечислила 300 миллионов долларов в фонд помощи пострадавшим в части кредитного мониторинга, а также потратила 1,6 миллиарда долларов на укрепление системы защиты информации.

pt

Интернет-компания Yahoo (2017)

Из-за крупнейшей утечки в истории (более миллиарда учетных записей пользователей Yahoo) телеком-гигант Verizon Communications снизил сумму покупки Yahoo на 350 миллионов долларов по сравнению с первоначальной стоимостью.

pt

ИБ-компания Okta (2022)

Капитализация Okta снизилась на 6 миллиардов долларов в течение недели после того, как стало известно о взломе компании.

pt

Финансовая корпорация Capital One (2019)

Компания выплатила штраф в размере 80 миллионов долларов и перечислила 190 миллионов долларов пострадавшим от утечки данных из-за некорректно настроенного межсетевого экрана.

pt

Маркетплейс Amazon (2021)

За нарушение европейского регламента по защите персональных данных GDPR Amazon выплатила штраф в размере 746 миллионов евро.

pt

Компания Sony (2011)

Выведение злоумышленниками из строя игровой сети PlayStation Network на 23 дня обошлось компании в 171 миллион долларов.

pt

# Банкротства становятся мейнстримом для малого и среднего бизнеса

Как отсутствие результативной кибербезопасности приводило к банкротству компаний

Примеры недопустимых событий



pt

Юридическая фирма Mossack Fonseca (2016 год)

Фирма закрылась после кражи и публикации юридических документов («Панамского досье») о различных офшорных схемах, в которых участвовали известные политики.

pt

Коллекторское агентство American Medical Collection Agency (2019 год)

Компания объявила о банкротстве после взлома и утечки данных миллионов клиентов организации.

pt

Криптовалютная биржа Mt. Gox (2014 год)

Компания не смогла ответить по своим обязательствам перед клиентами после кражи 740 000 биткоинов (6% от общего объема этой криптовалюты в мире) и объявила о банкротстве.

pt

Облачный хостинг-провайдер Code Spaces (2014 год)

Компания начала процедуру банкротства после уничтожения в результате хакерской атаки большинства виртуальных серверов с пользовательскими данными и их резервными копиями.

pt

Онлайн-сервис для малого бизнеса по мониторингу финансовых метрик MyBizHomepage (2009 год)

Уволенный СТО компании смог получить доступ к личным электронным почтам и аккаунтам руководства, после чего рассылал от их имени фальшивые сообщения клиентам и инвесторам, а также уничтожил все резервные копии данных с серверов компании. В результате MyBizHomepage объявила о банкротстве.

pt

Небольшая промоутерская компания Little & King LLC (2010 год)

Компания потеряла все оборотные средства из-за банковского трояна Zeus и признала банкротство.

pt

Интернет-провайдер Cloud Nine (2002 год)

Провайдер объявил себя банкротом после продолжительной DDoS-атаки, сделавшей невозможной оказание услуг клиентам.

pt

Технологическая компания HVGary Federal, работающая в сфере безопасности (2011 год)

Компания объявила о банкротстве после взлома сайта и последующей кражи десятков тысяч конфиденциальных документов, за которой последовал удар по репутации и массовый отток клиентов.

pt



# Недопустимое на уровне руководителя компании

- 2023 год – Генеральный директор Optus Келли Байер Розмарин уволена за крупнейшую утечку данных в истории Австралии
- 2023 год – CISO SolarWinds Тимоти Браун обвинен в обмане инвесторов и нарушении правил внутреннего контроля
- 2016 год – Генеральный директор FACC AG Вальтер Стефан уволен после фишинга от имени гендиректора, приведшего к краже 50 миллионов евро
- 2015 год – Генеральный директор Sony Public Entertainment Эми Паскаль уволена после раскрытия ее переписки, украденной хакерами после взлома компании в 2014 году

Всего лишь несколько примеров



# Недопустимое на уровне конкретного человека

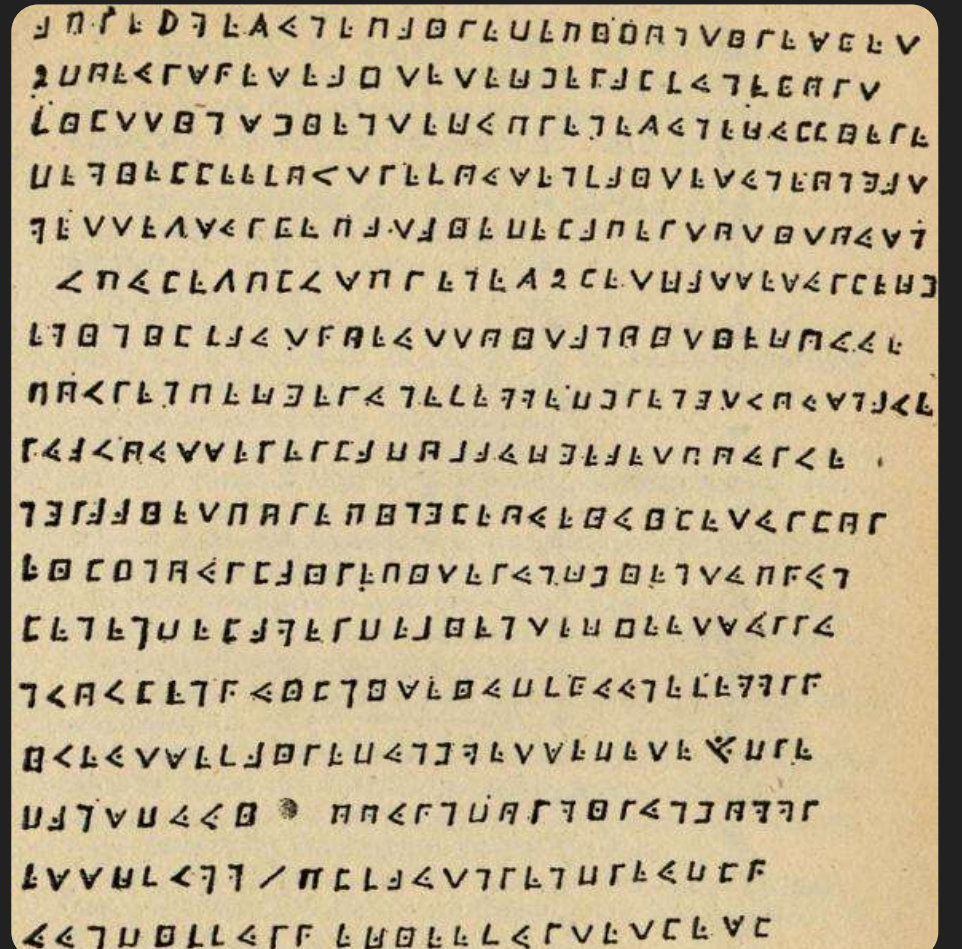
- Уязвимости в кардиостимуляторах и инсулиновых помпах с возможностью удаленного воздействия
- Блокировка тормозной системы в автомобилях с современным бортовым компьютером
- Кейс: Отслеживание геолокации через Strava с последующим нападением
- Кейс: смерть новорожденного в больнице из-за невозможности оказания первой медицинской помощи
- Кейс: удаленное блокирование пояса целомудрия





# Клад пирата Левассера

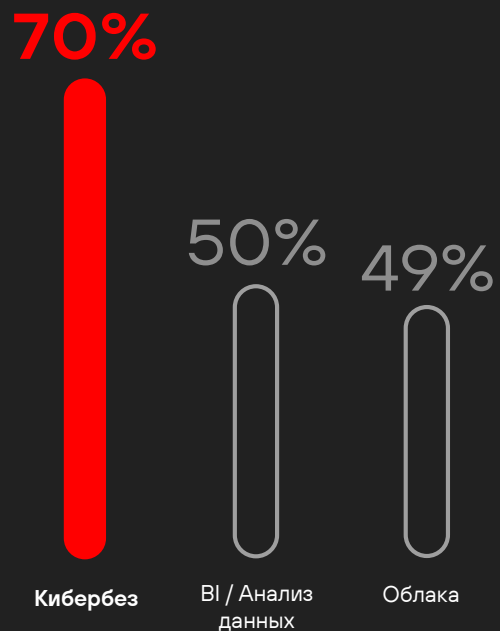
До сих пор неразгаданная тайна пиратского клада на 1 млрд фунтов стерлингов зашифрована в 17 строках, записанных на бусах



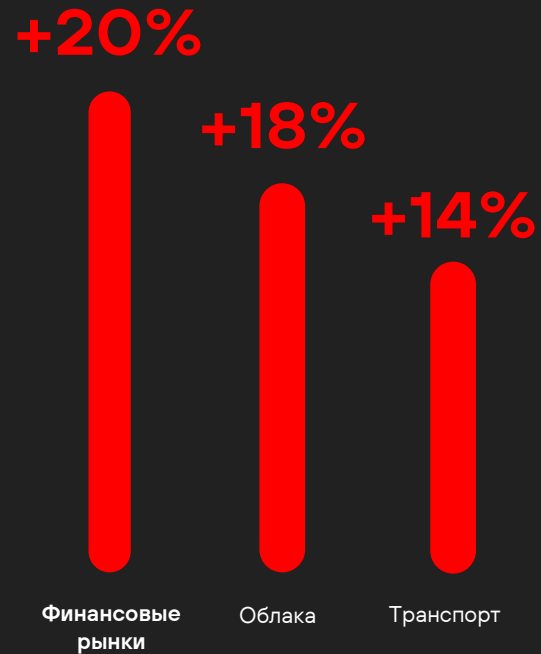
У П Г Е D Г Е A < Г Е П Н О Г Е U E П O O P V O Г Е V E E V  
2 U P E < G V F E V E J O V E V E U J E F J C L < Г Е E P G V  
L O C V V O T V J O E T V E U < П Г E T E A < Г Е U < C C O E G E  
U E T O E C C E L L A < V Г E L P < V E T L J O V E V < Г E P T E J V  
T E V V E L V < G E E П J V J O E U E C J П E G V P V O V P A < V T  
< П < C E L A П C < V П Г E T E A 2 C E V U J V V E V < G C E U J  
L T O T O C L J < V F P E < V V P O V J T P O V O E U P < E E  
П P < G E T П E U E E G < T E L E T T E U J G E T E V < P < V T J < E  
T < J < P < V V E T E G C J U P J J < U E E J E V P P < G < E  
T E J J J O E V П P G E П O T E C E P < E O < O C E V < G C P G  
E O C O T P < G C J O G E П O V E G < T E J J O E T V < П F < T  
C E T E T U E C J T E G U E J O E T V E U O E E V V < G G <  
T < P < C E T F < O C T O V E O < U L E < < T E L E T T E G F  
O < E < V V E L J O G E U < T J T E V V E U E V E X U G E  
U J T V U < < O P P < F T U P G T O G < T J P T T G  
E V V U L < T T / П C L J < V T G E T U G E < U C F  
< < T U O L L < G F E U O E E L < G V E V C E V C

# Инвестиции в ИБ растут

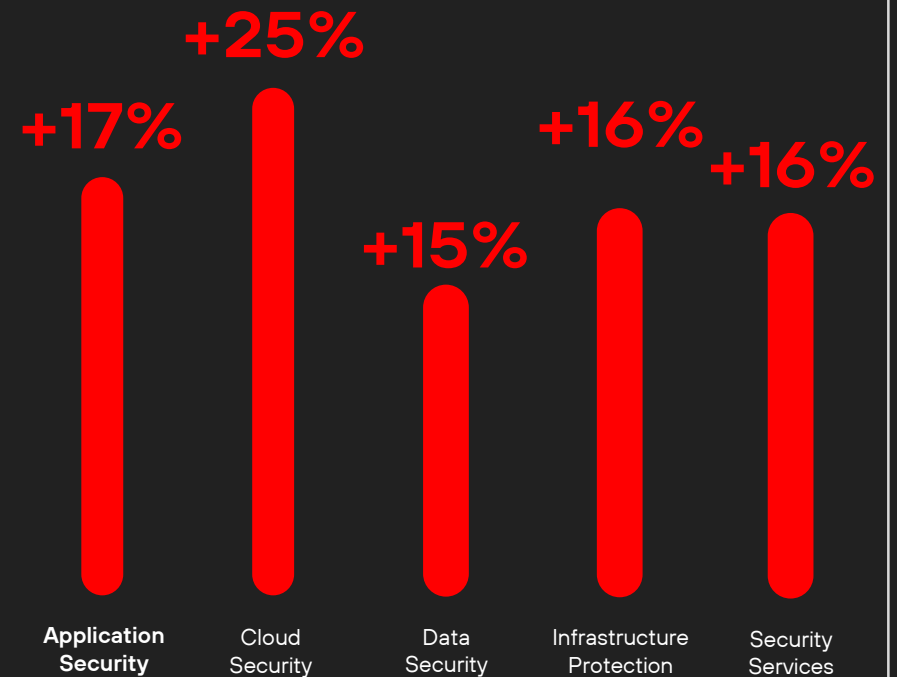
Топ-3 инвестиций  
в технологии в Европе  
в 2023 году



Рост доли ИБ  
в бюджете ИТ



Рост инвестиций  
в различные сегменты ИБ





**Хакеры  
объединяют  
свои усилия.  
Пора и отрасли  
ИБ объединиться  
под одной  
крышей!**



# ДЕНЬ ИНВЕСТОРА POSITIVE TECHNOLOGIES

ноябрь 2023



The background features a series of vibrant red, wavy, layered lines that create a sense of depth and movement, set against a dark, almost black, background. The lines are most prominent on the right side of the image, curving and overlapping to form a dynamic, organic shape.

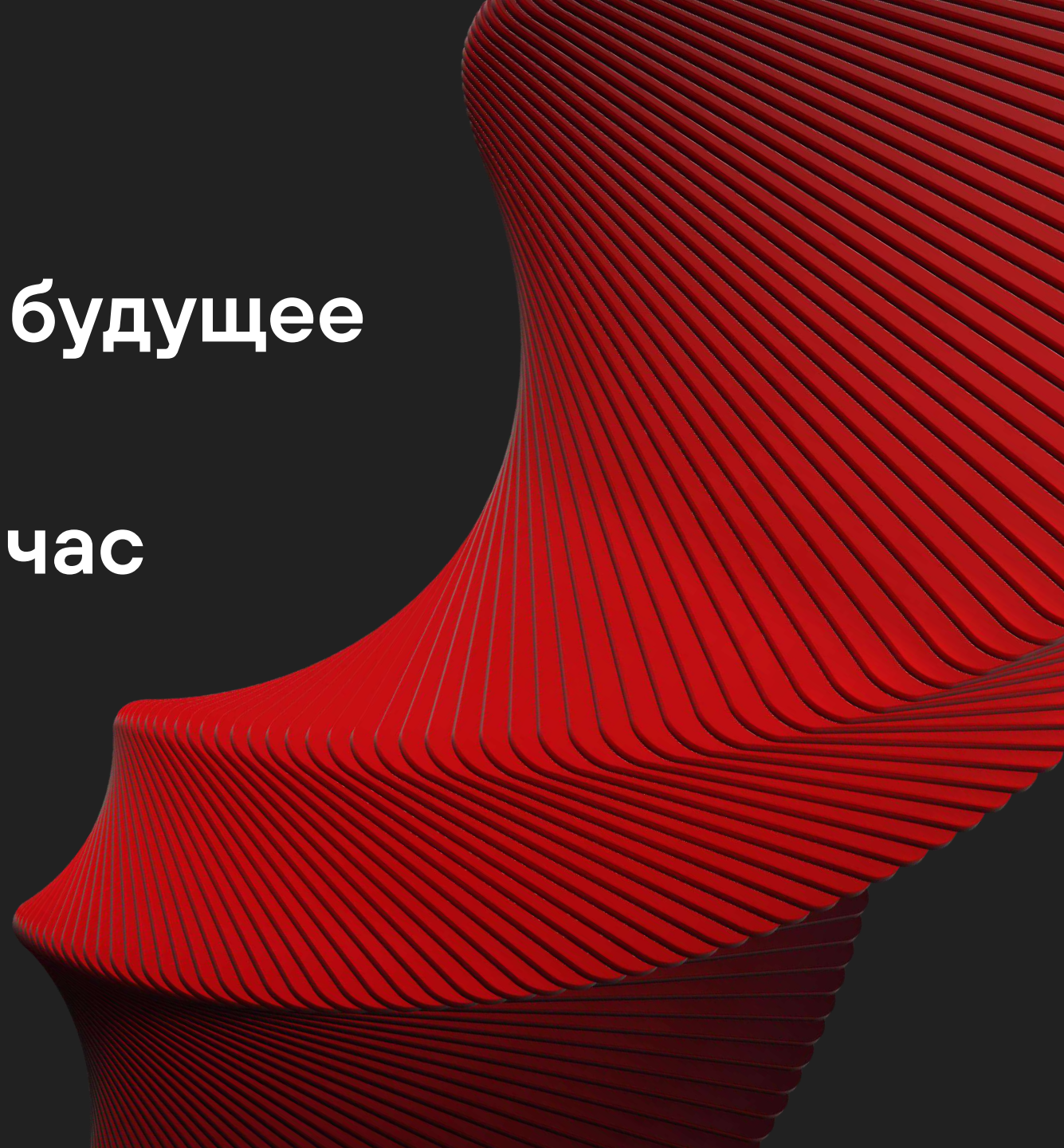
# Бизнес и прогнозы на 2023



**2023 – инвестируя в будущее**

**2024 – стартуем сейчас**

**Бизнес-контекст**





# Немного цифр про рынок ИБ

Прогноз ЦСР (июль 2023) о рынке кибербезопасности 2022-2025, млрд руб. и оценки ведущих игроков рынка

	2022	2023П	2024П	2025П
<b>ЦСР</b> млрд. руб	193	252	334	399
<b>ЦСР</b> рост рынка, г-к-г	X	+31%	+33%	+19%
<b>Ведущие игроки</b> усредненная оценка, рост бизнеса, г-к-г	X	+35%	+50%	?

## Цифры и динамика Positive Technologies

Таргетировали в начале года: **20 – 30 млрд руб.**

Видимость с момента 23.11.23: **22,5 – 27,5 млрд руб.**

Наиболее вероятный сценарий: **25 млрд руб.**

	2022	2023П	2024П	2025П
<b>Отгрузки</b> млрд. руб	14,5	25	40-50	70-100
<b>Рост</b> г-к-г	X	+72%	+60-100%	+75-150%

**Наша динамика роста в 2 – 2,5 раза выше рынка!**

# Как мы чувствуем 2023

## Новые клиенты

Количество новых клиентов

**+21%**

с 2022 года

1

## Retention

Высокая доля продлений лицензий

**91% > 94%**

2022

2023

2

## PT FS

Финансовые сервисы для заказчиков

7

## Территории

Продолжаем активный custdev на рынках Азии, Ближнего Востока, Африки, Латинской Америки  
Первые результаты.

8

## Cross-sell

**4,23**

4,8 в 2022

- очень крупные клиенты 50+ млн руб.

**1,72**

1,63 в 2022

- остальные клиенты

3

## Up-sell

Расширение инсталляционной базы у крупных клиентов

4

## Внутренние трансформации бизнес-юнита ЦПиРБ

**(+55%) +30%**

высококласных специалистов

Появление треков стратегических проектов и продаж

Перестройка работы с новыми заказчиками: работа на захват рынка

9

## Новые продукты

Количество новых продуктов

**+3 > +5**

2022/всего 17

2023/всего 22

5

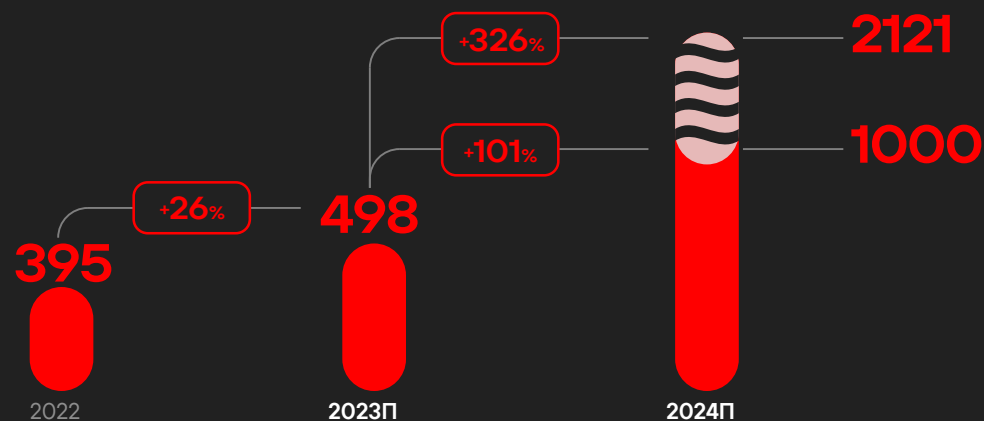
## Метапродукты

MaxPatrol O2  
MaxPatrol Carbon

2



# Новые клиенты



## Количество продуктов на клиента в сегментах:

	2022	2023
Холдинговые структуры	4,19	5,42
Продажи в регионах и через канал	1,53	1,63

### Рост общего числа заказчиков

	2022	2023П	2024П
Рост общего числа заказчиков	+20%	+21%	+74% (+35%)

Из них: более 10 млн руб. в отгрузках

Из них: более 10 млн руб. в отгрузках	+35%	+31%	X
---------------------------------------	------	------	---

Из них: менее 10 млн руб. в отгрузках

Из них: менее 10 млн руб. в отгрузках	+11%	+48%	X
---------------------------------------	------	------	---

### НОВЫЕ ЗАКАЗЧИКИ очень крупные

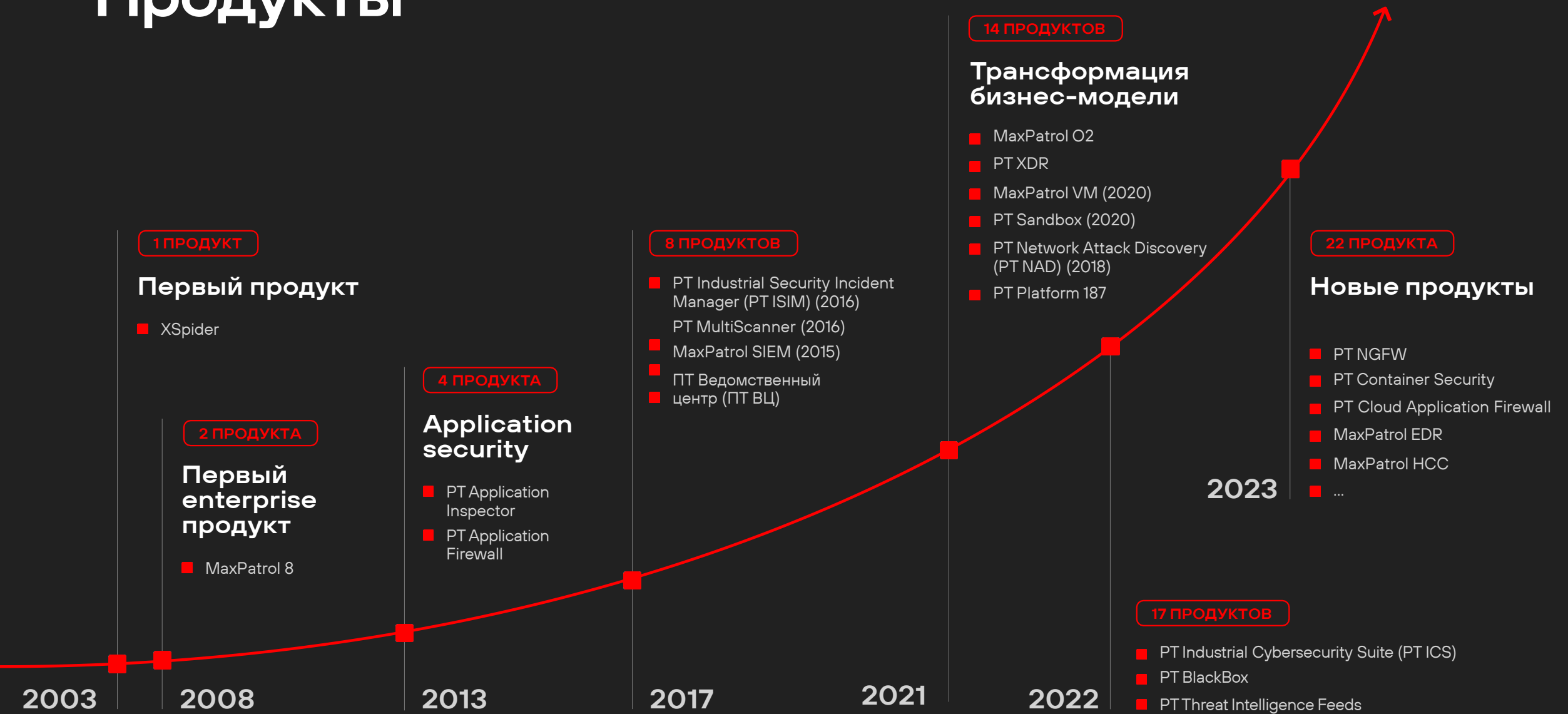
	2022	2023П	2024П
НОВЫЕ ЗАКАЗЧИКИ очень крупные			

Более 50 млн руб. доля в отгрузках

Более 50 млн руб. доля в отгрузках	21%	26%	?
------------------------------------	-----	-----	---

**94% – 95%**  
продления лицензий

# Продукты





# Продукты

## Воплотили наши ожидания: #1 новых продуктов



PT NGFW – в пилоты для early adopters, воронка 2024 уже 5+ млрд руб.



Первые продажи MaxPatrol O2 на 100+ млн руб.



PT Application Firewall Pro: бодрый старт! Почти на 0,8 млрд руб. ожидаем отгрузок в 2023, Воронка 2024 – более 1 млрд руб.



MaxPatrol EDR: первые продажи стартанули, воронка 2024 активно формируется, уже близко к 0,5 млрд руб.



PT Container Security: первые продажи уже в воронке 2024, 100+ млн руб.

**В 2024  
Году  
ожидаем**

**#1** MaxPatrol Carbon

**#2** BAS – платформа для автоматических пентестов

**#3** Новые продукты класса Threat Intelligence

**#4** Новые модули продуктов классов Incident Management, Log Management, анализ Netflow



# 2024: точки роста и дальнейшего развития



Драматическое расширение клиентской базы, минимум x2 рост числа новых заказчиков



Cross-sell и up-sell в текущих заказчиках



PT NGFW! Старт отгрузок!



Новые продукты 2023: go to market



Перезагрузка MSSP и прочих партнерских сервисов на наших продуктах



Продажи MaxPatrol O2



Трансформация продаж и развития бизнеса



PT FS – финансовые сервисы для заказчиков



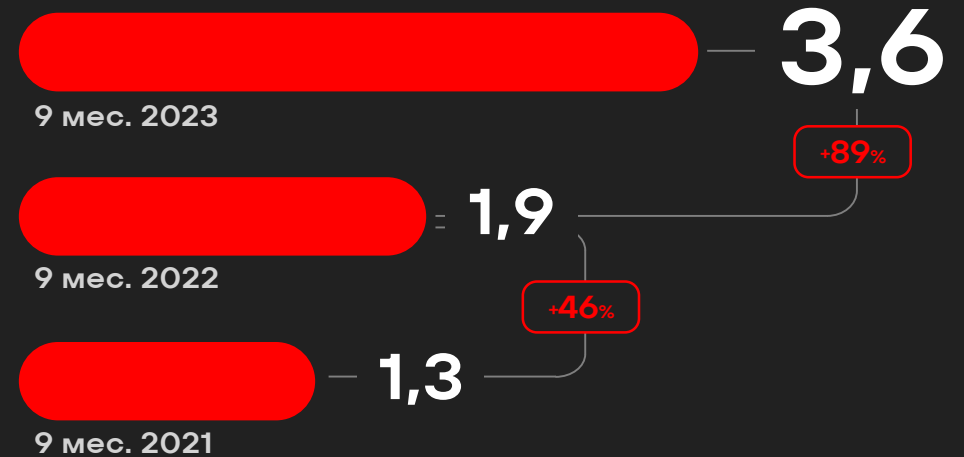
Международный бизнес: продолжаем путь



# Мы инвестируем в наше развитие:

- 1 Разработка и запуск новых продуктов, диверсификация портфеля продаж
- 2 Выход на комплементарные рынки – защита конечных устройств, ИТ инфраструктура
- 3 Рост и развитие сильной команды для поддержания высоких темпов роста бизнеса
- 4 Создание доступных инструментов финансирования для заказчиков
- 5 Нарращивание целевой клиентской базы
- 6 Выход в новые географические ниши

Общие R&D расходы, млрд руб.



**Мы заняли первое место в рейтинге ИТ-брендов работодателей 2023 года!**

(\*всероссийское исследование ИТ-брендов работодателей, которое проводит ЭКОПСИ и Хабр)

Планируем поддерживать высокую маржинальность по НИС – **30 +%**  
 ... и наращивать дивидендный потенциал **50-100% от НИС**

# Контакты для инвесторов

[shareholder@ptsecurity.com](mailto:shareholder@ptsecurity.com)



Наш телеграм-канал  
IT's Positive Investing —  
[@positive\\_investing](https://t.me/positive_investing)



**Юрий Мариничев**  
IR-директор

[yumarinichev@ptsecurity.com](mailto:yumarinichev@ptsecurity.com)  
+7 (985) 761-84-63



Сайт для инвесторов  
и аналитиков:  
[group.ptsecurity.com](https://group.ptsecurity.com)