



# Комплексная кибербезопасность на базе российских решений и сервисов Softline

**Шкатов Александр**

Ведущим менеджер группы развития продаж решений  
информационной безопасности в ЦФО

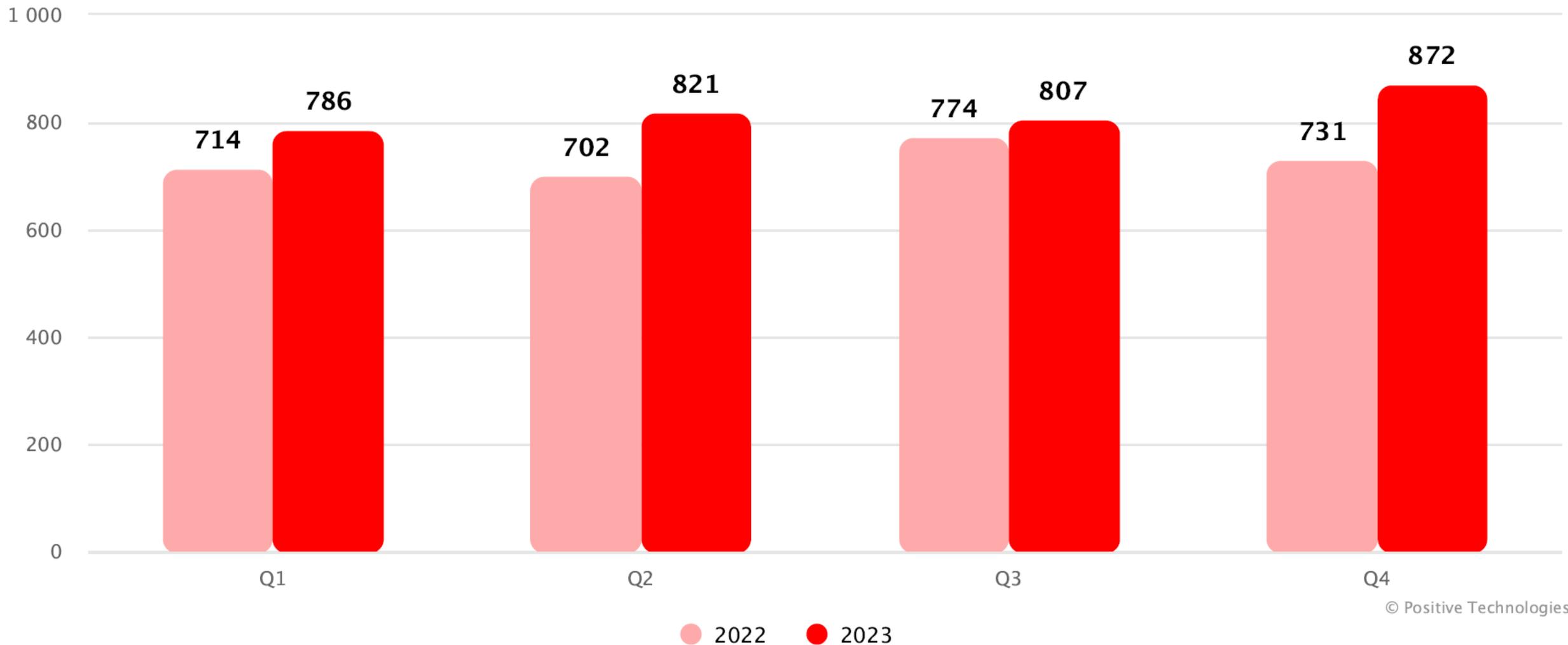
T +79601171278

[Alexander.Shkatov@softline.com](mailto:Alexander.Shkatov@softline.com)

**Фактическая ситуация**



# Сводная статистика по атакам на Россию



# Последствия атак



Россия

**375** атак  
2023–Н1 2024

## Топ категорий жертв:

Промышленность	11%
Телекоммуникации	10%
Госучреждения	9%
IT-компании	7%

## Топ объектов атак:

Компьютеры, серверы и сетевое оборудование	69%
Люди	56%
Веб-ресурсы	21%

## Топ методов атак:

Социальная инженерия	56%
Использование ВПО	51%
Эксплуатация уязвимостей	30%
DDoS	10%

## Топ последствий атак:

Утечка конфиденциальной информации	49%
Нарушение основной деятельности	31%
Прямые финансовые потери	9%

\*Доля от общего числа атак на страну за указанный период



# Информационная безопасность в Softline

# Кибербезопасность

## Инфраструктура

- Безопасное рабочее место
- Сетевая безопасность (NGFW, IPS, ATP)
- Защищенные каналы связи (VPN)
- Аудит изменений
- Безопасная совместная работа с контентом
- Защита баз данных (DAM)
- Безопасная мобильность (MDM, EMM)
- Контроль целостности
- Безопасность почтового и веб траффика
- Управление инцидентами (SIEM, IRP)

## Защита данных

- Тренинги/проверки сотрудников (awareness)
- Защита данных (DLP)
- Управление доступом (IDM, PAM, PIM, 2FA)
- Шифрование данных

## Безопасность приложений

- Анализ кода
- Безопасность приложений (WAF)
- Управление конфигурациями
- Тесты на проникновение (pentest)

## Управление и соответствие

- Security Operation Center (SOC)
- Индустриальные стандарты
- Управление рисками
- Соответствие законам (152ФЗ, GDPR, СТОБР, 382П. Гост 57580. 187ФЗ)
- Авторские продукты (ETHIC)

### НАШИ СЕРВИСЫ:



Проектирование



Пилотирование



Внедрение



Техподдержка



Управляемые сервисы

# Портфель импортонезависимых вендоров

**Безопасность инфраструктуры**

NGFW • VPN • Web filtering • Mail security • NTA (ex ATP) • NAC • Firewall management  
 AV&EDR • MDM • DB Security • DAM/DBF • SIEM • IRP • SOAR • vSecurity

R-Vision	T-Soft	RUSIEM	AVSOFT	Wise-Mon MONITORING SOLUTIONS
TCC	SECURITY VISION УБЕДИТЕЛЬНОСТЬ	ГАРДА ТЕХНОЛОГИИ	КОА БЕЗОПАСНОСТИ	GROUP IB
NGRSOFTLAB	positive technologies	kaspersky	s•terra®	infotecs®
xello Deception	SMART-SOFT®	Dr.WEB®	SOLAR SECURITY	ФАКТОР.Т
UserGate	ФАКТОР.Т	SkyDNS	ПАНГЕО РАДАР	DALLAS LOCK
GIS ГАЗИНФОРМ СЕРВИС	ideco	SAFEPHONE	SEARCHINFORM INFORMATION SECURITY	IT EXPERTISE

**Безопасность приложений**

WAF • Anti-DDoS • Vulnerability Management • Pentest • Security code source • Secure IoT  
 Data Masking • Container Security • Configuration Management • DevSecOps

CLOUDFLARE®	positive technologies	REDCheck	STAR FORCE®	RCNTEC
Эшелон информационные технологии	TRLHACK	SOLAR SECURITY	QRATORLABS	kaspersky
PENTESTIT	R-Vision VM	solidlab	Вебмониторэкс защита веб-приложений	ГАРДА ТЕХНОЛОГИИ
КОА БЕЗОПАСНОСТИ	SCAN FACTORY	Vulns.io VM		

**Безопасность данных**

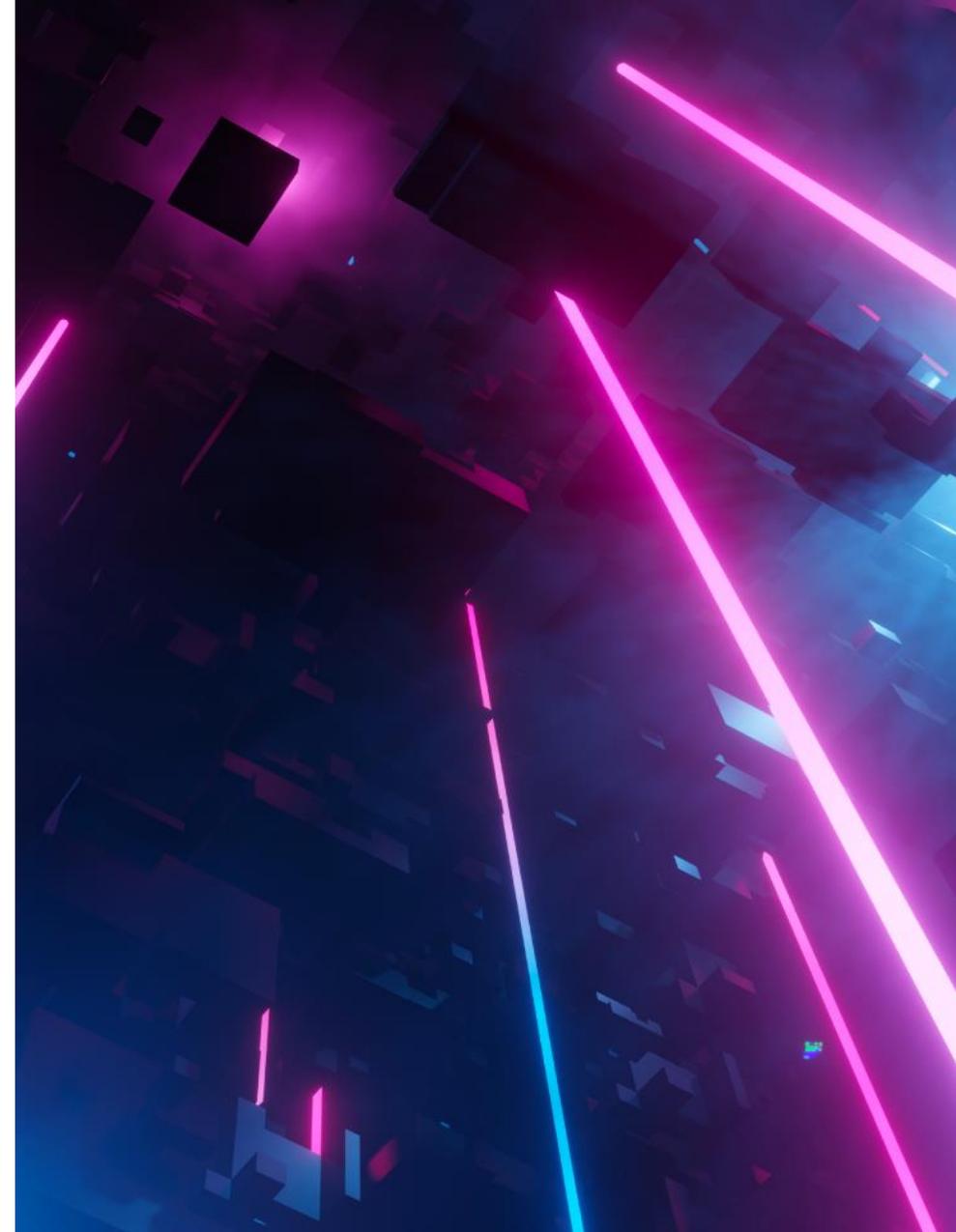
DAG • DLP • VDR • IDM • PAM • Audit File Access • MFA • Encryption

				STAFFCOP
perimetrix	GROUP IB	Avanpost®	MULTIFACTOR	Аладдин
КРИПТОПРО	MFLASH	WorksPad	INFOWATCH®	АЙТИБАСТИОН
ZECURION	Стахановец	INDEED ID	SOLAR SECURITY	NGRSOFTLAB
SEARCHINFORM INFORMATION SECURITY	falcongaze	CyberPeak	ГАРДА ТЕХНОЛОГИИ	АПР ОКС
ОРЛАН	MAKVES	RCNTEC	EVERYTAG	identity Blitz

# Ключевые решения

# Защита конечных точек

АНТИВИРУСЫ	  <b>КОД</b> безопасности 
EDR	   POSITIVE TECHNOLOGIES



# Защита сети и почтового трафика

МЕЖСЕТЕВЫЕ  
ЭКРАНЫ

 UserGate

 **Эшелон**  
комплексная безопасность

 SMART-SOFT

 **КОД**  
безопасности

**с•терра®**

 **infotecs®**

 **ideco**

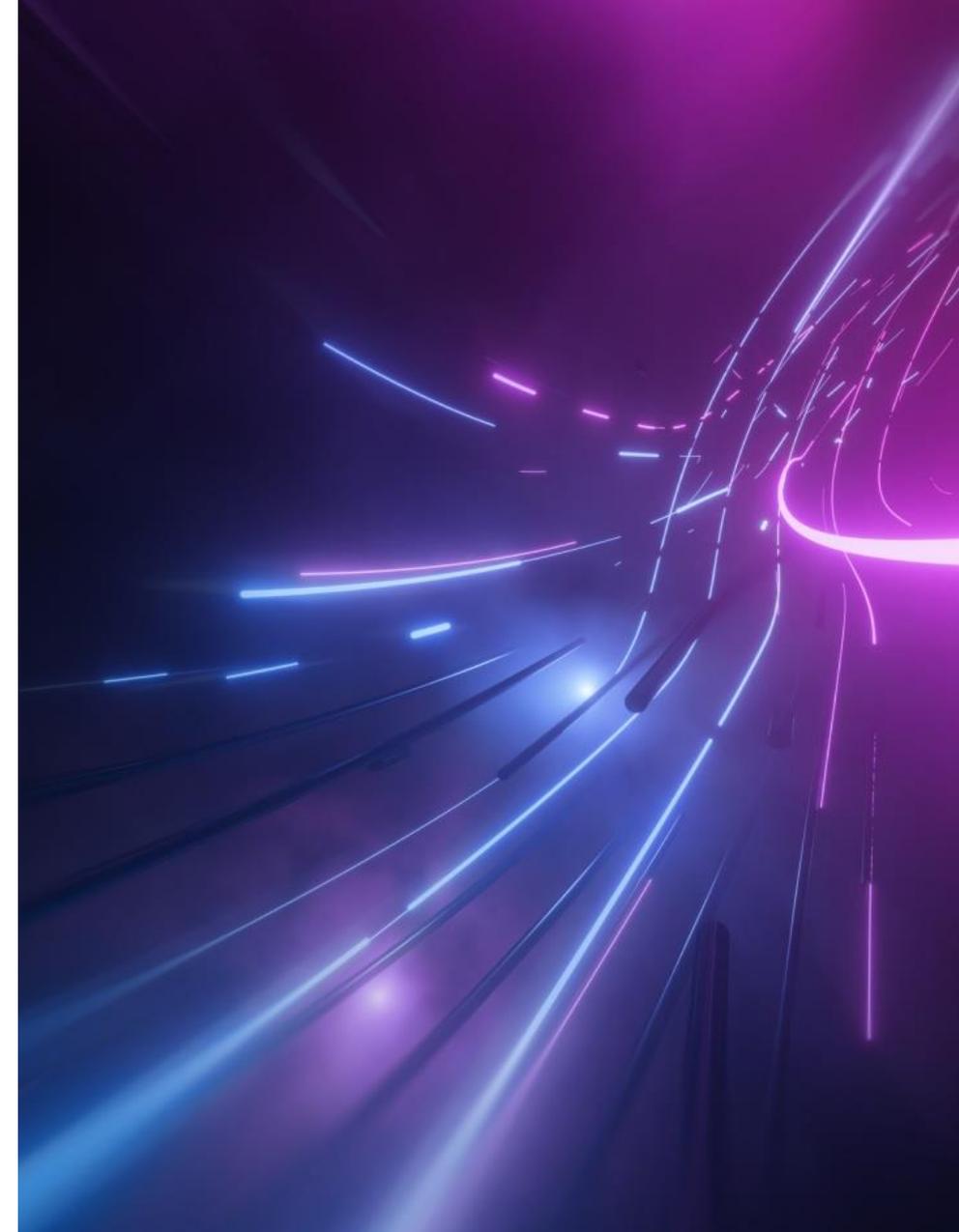
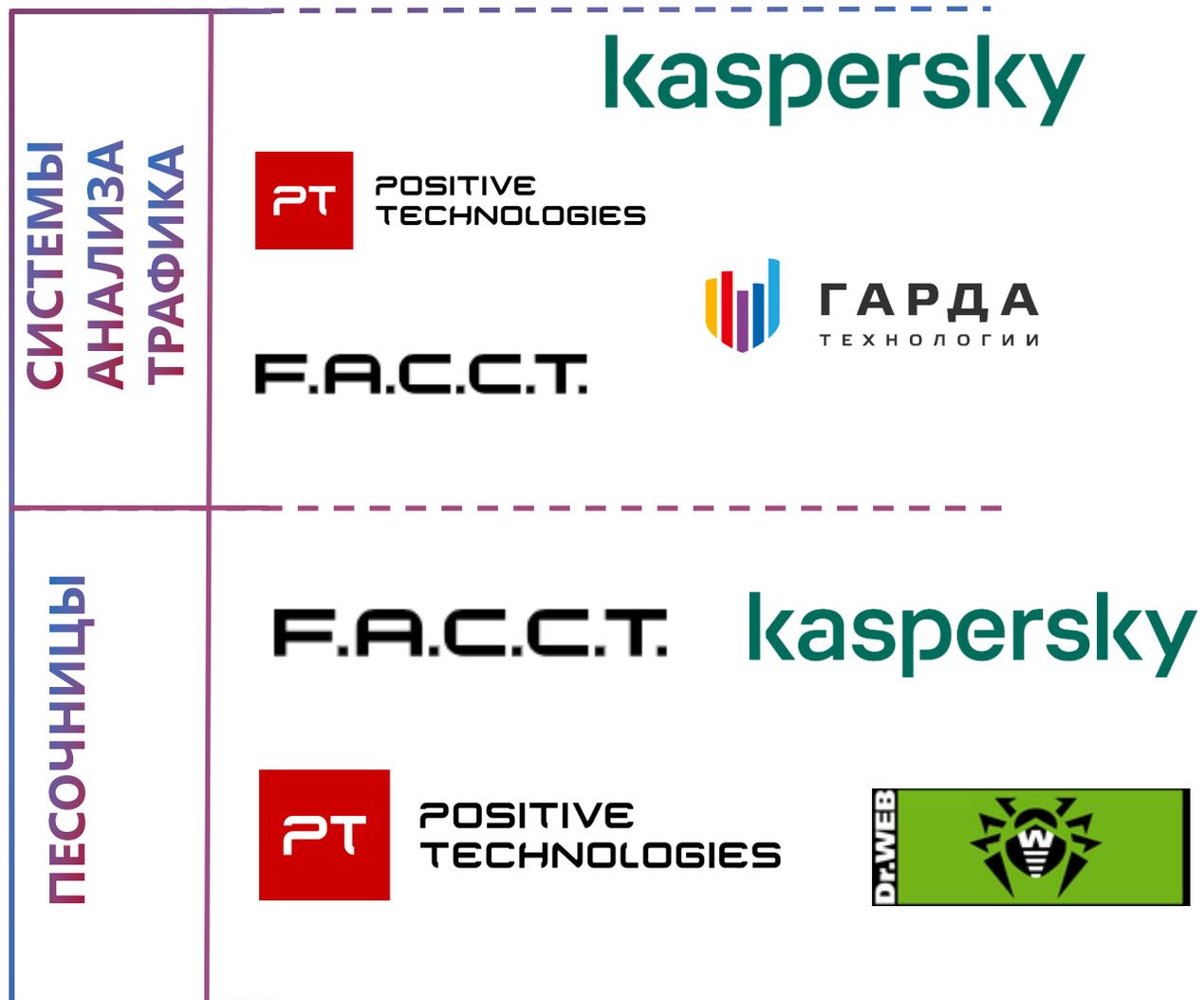
ЗАЩИТА ПОЧТЫ

 **Dr.WEB**

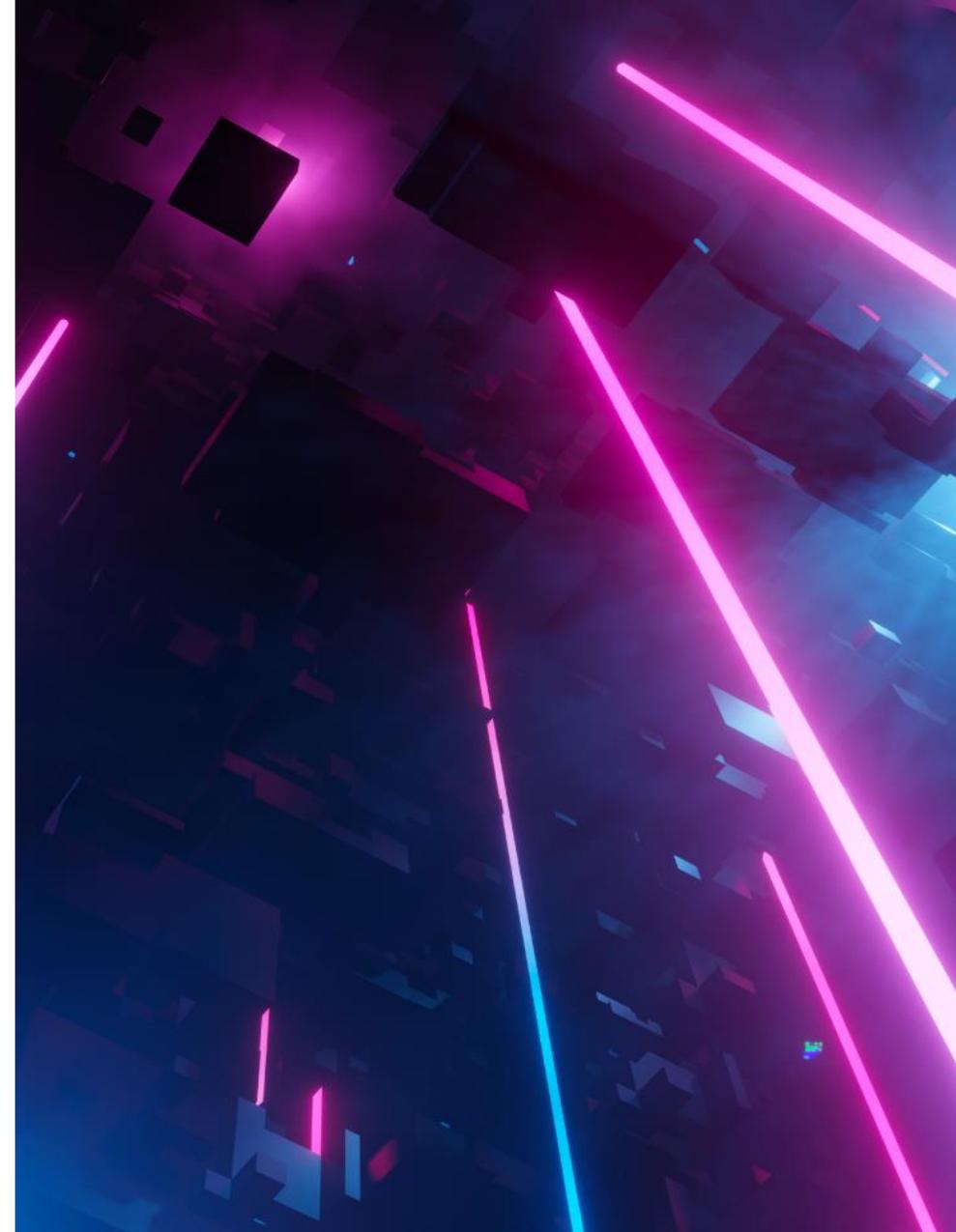
**kaspersky**

**F.A.C.C.T.**

# Защита от целенаправленных атак



# Защита приложений



# Защита от утечек\контроль пользователей

**СИСТЕМЫ ЗАЩИТЫ ОТ УТЕЧЕК  
ИНФОРМАЦИИ**

The complex block contains six logos of security systems. On the left, a vertical label reads 'СИСТЕМЫ ЗАЩИТЫ ОТ УТЕЧЕК ИНФОРМАЦИИ'. The logos are: 1. Infowatch: a green eye icon above the text 'INFOWATCH'. 2. Stakhanovets: a red 'T' icon above the text 'Стахановец' and 'система контроля сотрудников'. 3. Searchinform: the text 'SEARCHINFORM' in orange and blue, with 'INFORMATION SECURITY' below it. 4. Solar Security: a circular icon of a sun with rays, above the text 'SOLAR SECURITY' and 'software&services'. 5. Staffcop: a white shield icon with a crown, above the text 'staffcop' on a dark blue background. 6. Zecurion: a red and white diagonal striped icon, followed by the text 'ZECURION'.



# Сканеры уязвимостей

СКАНЕРЫ УЯЗВИМОСТЕЙ



POSITIVE  
TECHNOLOGIES



# Двухфакторная аутентификация

СИСТЕМЫ ДВУХФАКТОРНОЙ  
АУТЕНТИФИКАЦИИ

**Avanpost**

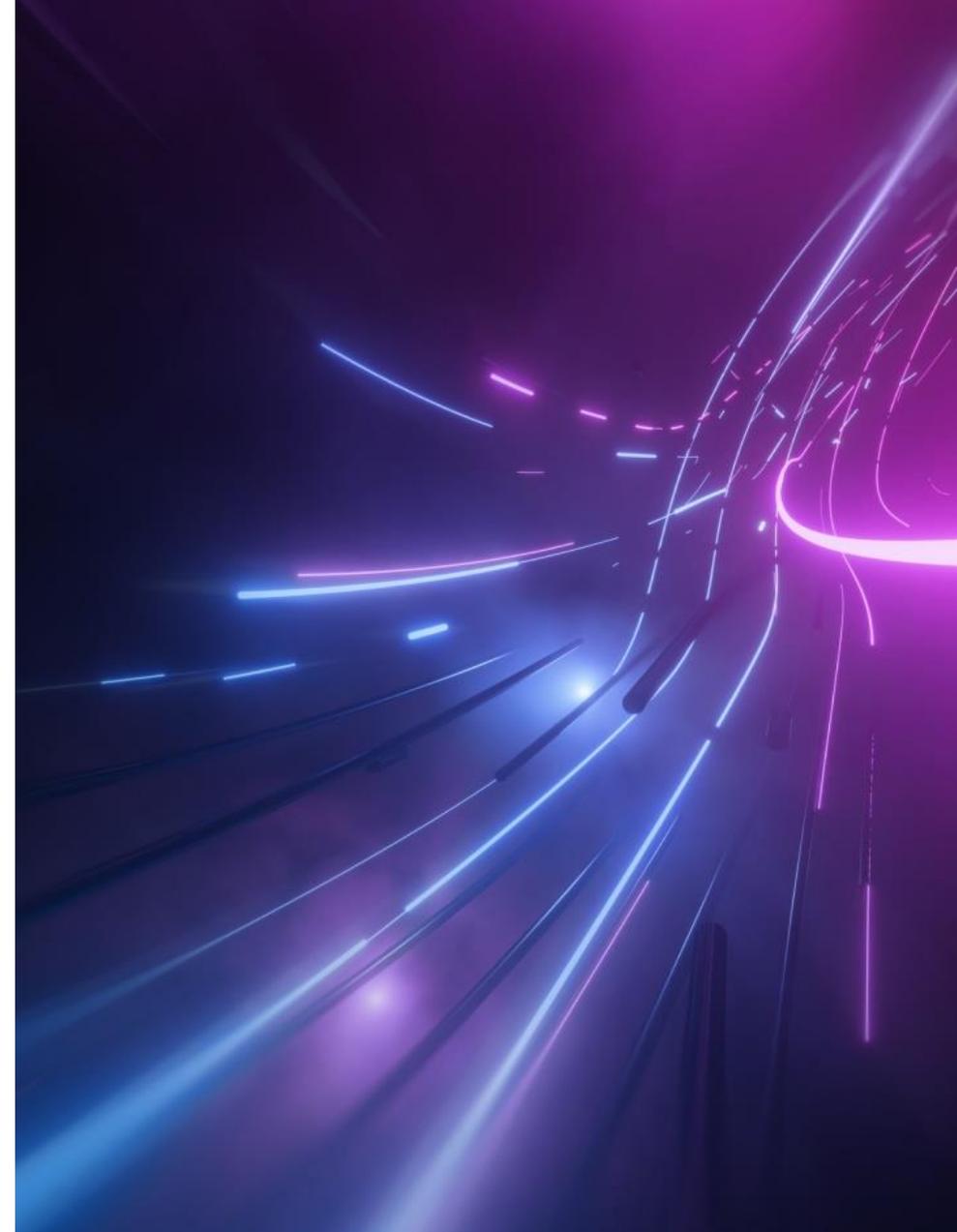
**Identity Blitz**

**Аладдин**

**СКБ Контур**

**MULTIFACTOR**

**INDEED ID**



# Реагирование на события ИБ

СИСТЕМЫ СБОРА  
И КОРРЕЛЯЦИИ  
СОБЫТИЙ



POSITIVE  
TECHNOLOGIES



RUSIEM

Всё под контролем



NGRSOFTLAB



{KOMRAD}  
Enterprise SIEM

kaspersky

SEARCHINFORM

INFORMATION SECURITY

СИСТЕМЫ  
АВТОМАТИЗАЦИИ  
РЕАГИРОВАНИЯ



Security Vision

R-Vision



# Осведомленность пользователей в сфере ИБ

Awareness

kaspersky

 StopPhish

 phishman

secure-t

# Киберполигон



**Киберполигон Ampire** – программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак.

Данный комплекс предназначен для обучения, подготовки и тренировки специалистов по информационной безопасности для государственных организаций, кредитно-финансовой сферы, объектов критической информационной инфраструктуры, телекома и других отраслей.

Ampire зарегистрирован в **Едином реестре** российских программ для электронных вычислительных машин и баз данных **20.09.2019 г. (рег. номер ПО 5861)**

# Ключевые сервисы SOFTLINE

# Полный цикл реализации проекта

От подбора решения и поставки до внедрения и технической поддержки

- Собственный Производственный блок
- Развитая экспертная команда:  
ИТ, ИБ и Консалтинг
- Собственный Учебный центр
- Собственная система Service Desk, Служба технической поддержки и Сервисный центр
- Гибкая модель предоставления услуг – от внедрения и сопровождения до аутсорсинга
- Выделенные и разовые услуги по запросу



# Техническая поддержка

Сопровождение функционирования и эксплуатации систем информационной безопасности на протяжении их жизненного цикла

## Состав услуги:

- Базовая, 1-я линия: регистрация и ведение заявок, передача информации/логов в поддержку Производителя и отслеживание статуса
- Стандартная (консультационная), 2-я линия: базовая + консультационные услуги по функционалу, настройке, восстановлению работоспособности
- Расширенная (инцидентная), 3-я линия: стандартная + подключение эксперта к решению инцидентов

Service Level Agreement



Service Desk



Персональный сервис-менеджер



Компания Softline становится **единой точкой входа** по всем вопросам, связанным с технической поддержкой ИБ-решений

# Аутсорсинг

Регулярное администрирование систем информационной безопасности

## Состав услуги:

- Запрос на физическое обслуживание на месте размещения объекта
- Регламентные выезды в рамках профилактического визита
- Услуги конфигурирования: создание и внесение изменений
- Обновление: установка и применение
- Мониторинг 24x7:
- Подключение обслуживаемых систем к средствам мониторинга
- Реагирование на инциденты и эскалация выявленных событий

Цифровая Трансформация. Успешная. Эффективная.



# Сервисные модели

## Security as a Service

- Лицензия, программное обеспечение
- Вычислительные ресурсы Softline Cloud – Infrastructure as a Service

Тип Сервиса	Позиции	Детализация
Managed Security Service, MSS	Security as a Service, SECaaS	Лицензия, ПО
		Лицензия на право использование средства защиты информации
	Infrastructure as a Service, IaaS SL Cloud (вычислительные ресурсы)	IaaS, vCloud, vCPU
		IaaS, vCloud, vRAM
		IaaS, vCloud, SAS
		Интернет-канал
		Veeam B&R, vCloud, VM
Cloud Veeam, хранение на СХД		
Постановка на Сервис		
Управление Сервисом		

## Managed Security Service

- Лицензия, программное обеспечение
- Вычислительные ресурсы Softline Cloud – Infrastructure as a Service
- Интеграция и постановка на Сервис
- Техническая поддержка, сопровождение эксплуатации и управление Сервисом



# Сервисы вокруг систем контроля и предотвращения утечек информации



## Разовые услуги:

- Анализ потребностей и подбор оптимального решения;
- Внедрение системы и подключение источников данных;
- Сбор перечня критичных для организации документов;
- Настройка индивидуальных правил, удобных Заказчику;
- Подготовка сопроводительной документации или её доработка.



## Аналитика:

- Оперативное информирование о потенциальных инцидентах;
- Сбор информации из архива по запросу Заказчика;
- Актуализация настройки при изменениях в компании;
- Помощь в построении процессов реагирования;
- Обеспечение детального контроля критичных элементов.



## Техподдержка:

- Выявление проблемы, проведение диагностики и её устранение;
- Решение проблем совместно с вендором, сбор диагностической информации для её передачи;
- Оптимизация процесса обработки и хранения данных;
- Проведение обновления системы.

# Сервис SOC

## Что это

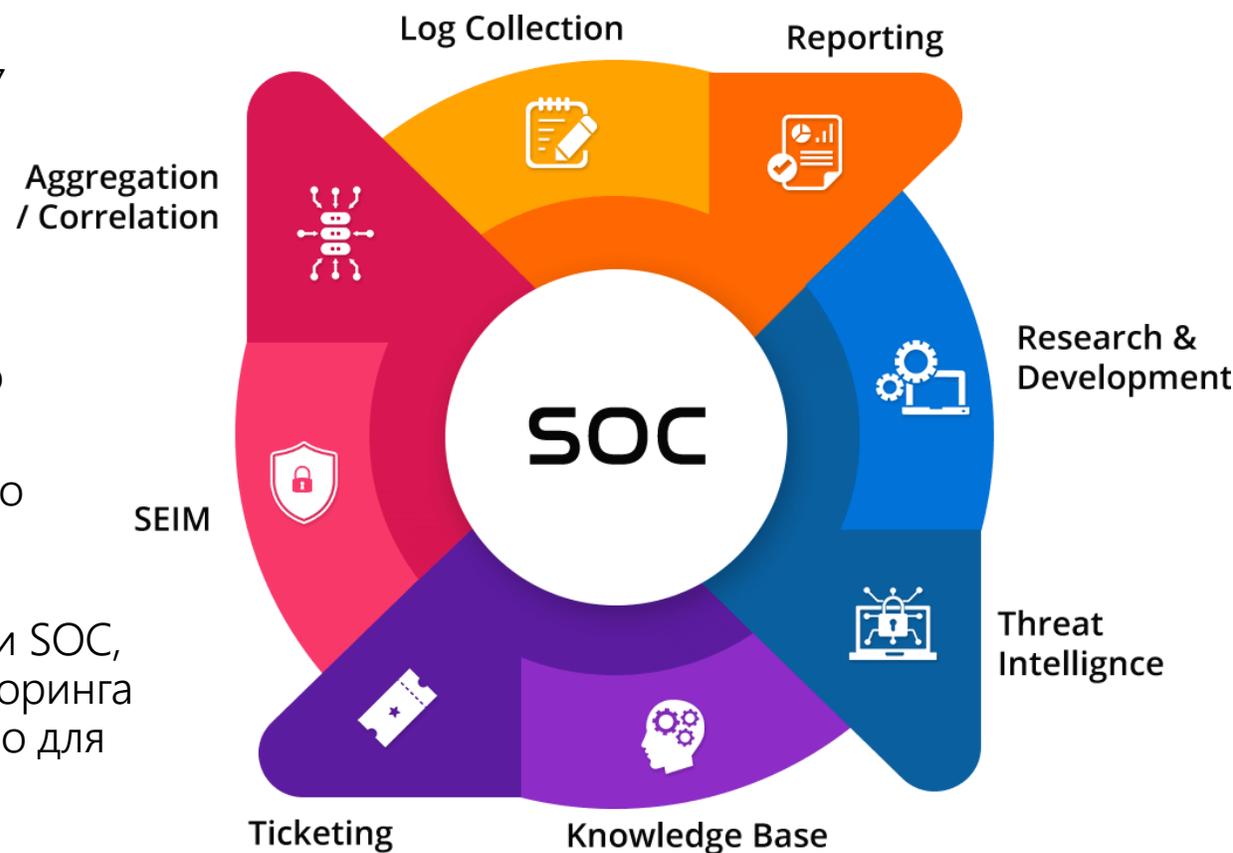
- Мониторинг состояния ИБ в режиме 24x7
- Выявление кибератак на ранних стадиях
- Минимизация потерь за счет оперативного разбора инцидентов

## Зачем нужно клиенту

- Возможность оперативно и сравнительно недорого запустить SOC
- Уникальные компетенции, которые сложно найти и еще сложнее удержать

## Варианты реализации

- Basic – базово необходимые возможности SOC, позволяющие запустить процессы мониторинга в круглосуточном режиме. Рекомендовано для средних компаний (1000 – 1500 ПК)
- Extended – расширенные возможности, включающие автоматизированную реакцию и углубленный разбор инцидентов ИБ



# Преимущества сервиса iSOC

## Предустановленные настройки

Относительно быстрый старт сервиса за счёт постоянно пополняемых набора сценариев реагирования и коннекторов к различным источникам событий для большинства техник матрицы MITRE ATT&CK

## Экспертиза в удовлетворении требований регуляторов

Мы имеем обширный опыт в реализации требований ФЗ 187, ГОСТ 57580 и т.д. Имеем соглашение с НКЦКИ, являемся центром ГОССОПКА, можем осуществлять обмен данными с ФИНЦЕРТ и НКЦКИ

## Сертифицированные российские решения в ядре SOC

KUMA и IRP/SOAR Security Vision составляющие ядро ISOC, сертифицированы ФСТЭК России и находятся в реестре отечественного ПО

## Автоматизация реагирования

Экспертный набор playbooks для реагирования на инциденты, включающий управление ИБ в компании (от обучения до разработки документации). Оперативное обнаружение и реагирование на уровне конечных устройств – интеграция ISOC с KEDR

## Кастомизация сервиса

Оперативно самостоятельно разрабатываем новые правила корреляций и плейбуки как по требованиям заказчика, так и при появлении новых угроз

## Экосистема сервисов Infosecurity

Интеграция ISOC с другими сервисами Infosecurity по защите от киберугроз и сопровождению ИТ-инфраструктуры заказчика – зона ответственности по реагированию в единой точке

# Повышение осведомлённости пользователей

Оценка текущего состояния осведомлённости сотрудников, профессиональных компетенций



тестирование сотрудников заказчика

Платформы класса Awareness



PHISHMAN, ASAP, Антифишинг, СтопФиш, Secure-T

Сервис повышения осведомлённости



- Платформа в облаке
- Платформа в облаке+сервис
- Эл.курсы по подписке
- Фишинг по подписке

Коробочные электронные учебные курсы для СДО заказчика



Более 30+ курсов по разным темам ИБ

Разработка материалов для заказчика



- Электронные курсы и тесты
- Видеоролики
- Плакаты, скринсейверы
- Дайджесты
- Комиксы
- Игры
- День по ИБ
- Вебинары

Разработка стандарта повышения осведомлённости работников в области ИБ



- По направлениям
- По ролям

# Соответствие требованиям



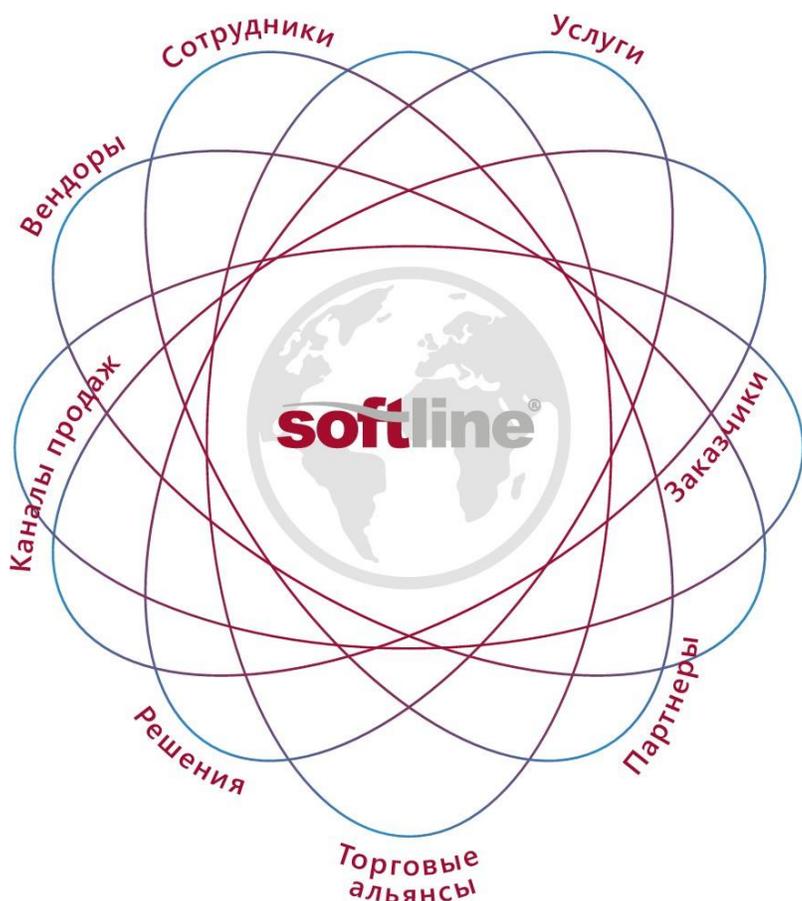
## Соответствие требованиям

- Приведение в соответствие 187-ФЗ; (235 и 239 приказ ФСТЭК)
- Приведение в соответствие 152-ФЗ (21 приказ ФСТЭК);
- Приведение в соответствие требованиям ГИС/МИС (17 приказ ФСТЭК);
- Специальные проверки и специальные исследования;
- Аттестация объектов автоматизации.



# Почему Softline

# Глобальный лидер в цифровой трансформации и информационной безопасности



## Краеугольный камень цифровой трансформации

**30 лет**  
На IT рынке

**3000+**  
Реализованных проектов

**3600+**  
Сотрудников

**1000+**  
Менеджеров

**800+**  
Инженеров

## Лидер информационной безопасности

**380**  
Инженеров по направлению ИБ

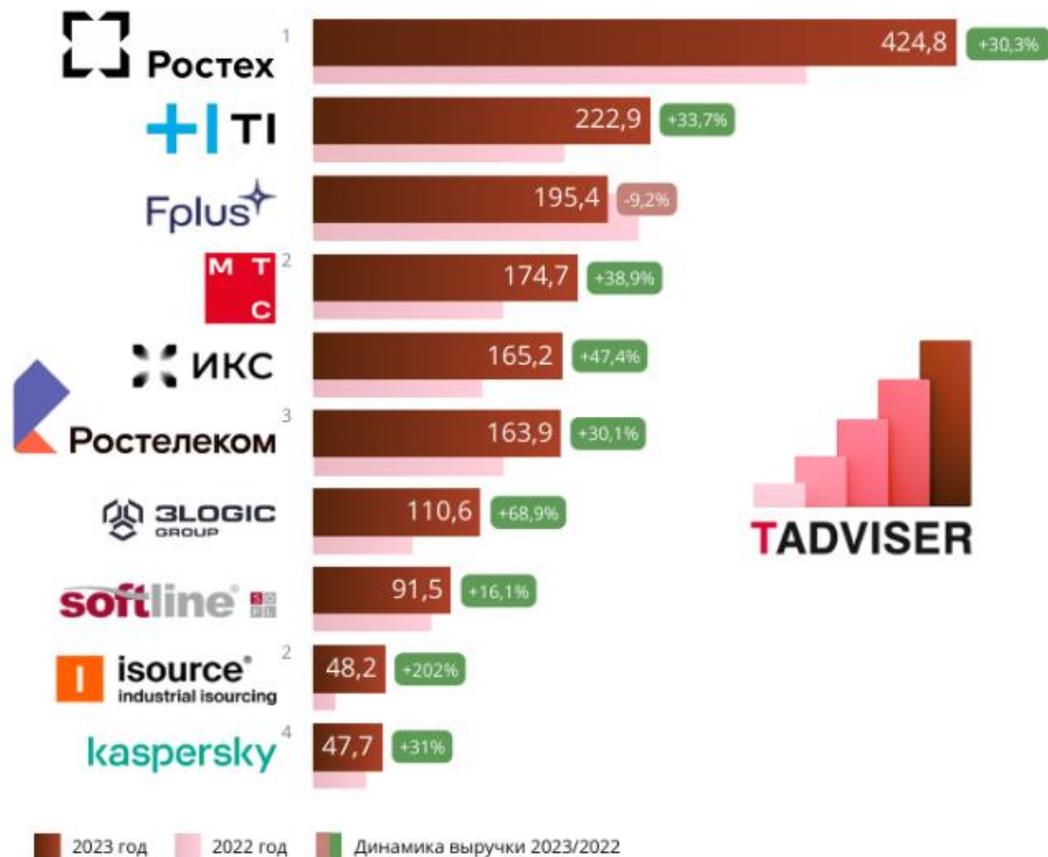
**ТОП-3**  
[Крупнейших в РФ компаний в сфере ИБ по рейтингу Cnews](#)

**ФСБ, ФСТЭК**  
Лицензии

**Инфосекьюрити, ТЦ Инженер**  
Входят в ГК Софтлайн

# Рейтинг

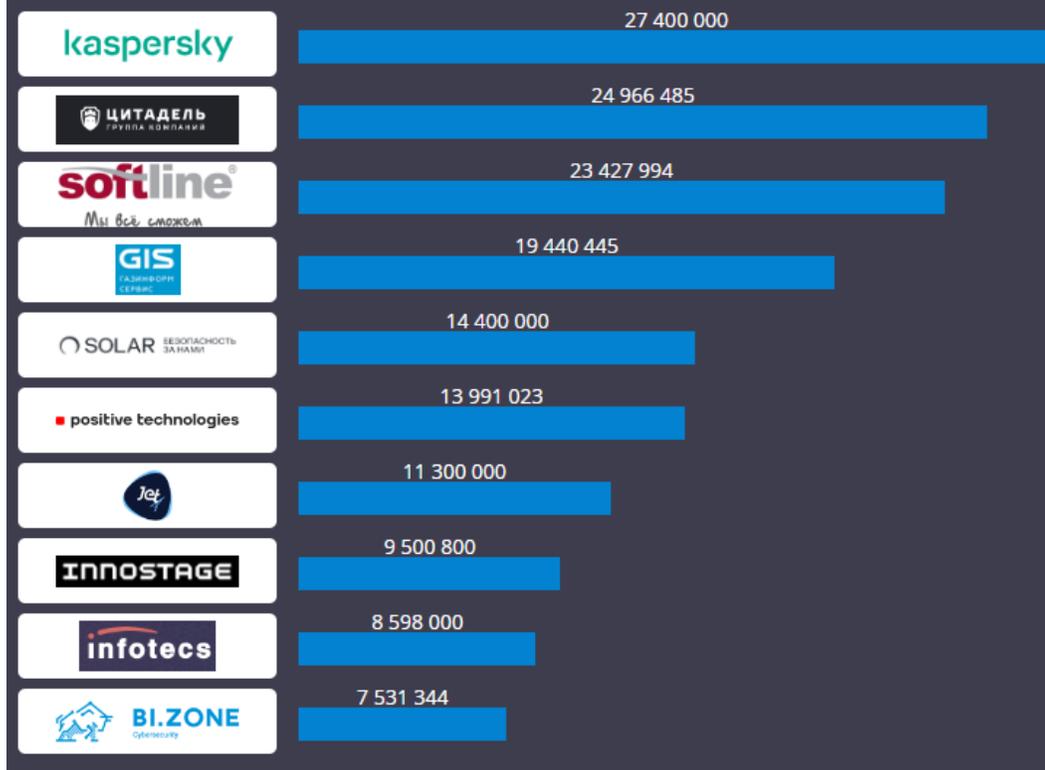
## Крупнейшие ИТ-компании в России по выручке за 2023 год (в млрд рублей)



## Топ-10 игроков рынка информационной безопасности



■ Выручка в 2022 г. в Ртыс. с НДС



1. Выручка Радиозлектронного комплекса  
2. Без НДС  
3. Выручка от цифровых сервисов  
4. Выручка российского юр.лица

# Пилотное тестирование

Практическая проверка функциональных возможностей и требований к решению

- **Устав** пилотного проекта
- **Программа** и методика испытаний
- **Детализированный отчёт** по результатам тестирования
- **Выдача рекомендаций** по покрытию векторов угроз
- **Демонстрация** функциональных возможностей
- **Качественный переход и реализация** проекта по внедрению





Цифровая Трансформация.  
Успешная. Эффективная.

**Шкатов Александр**

**Ведущий менеджер группы развития продаж решений  
информационной безопасности в ЦФО**

**T +79601171278**

[Alexander.Shkatov@softline.com](mailto:Alexander.Shkatov@softline.com)