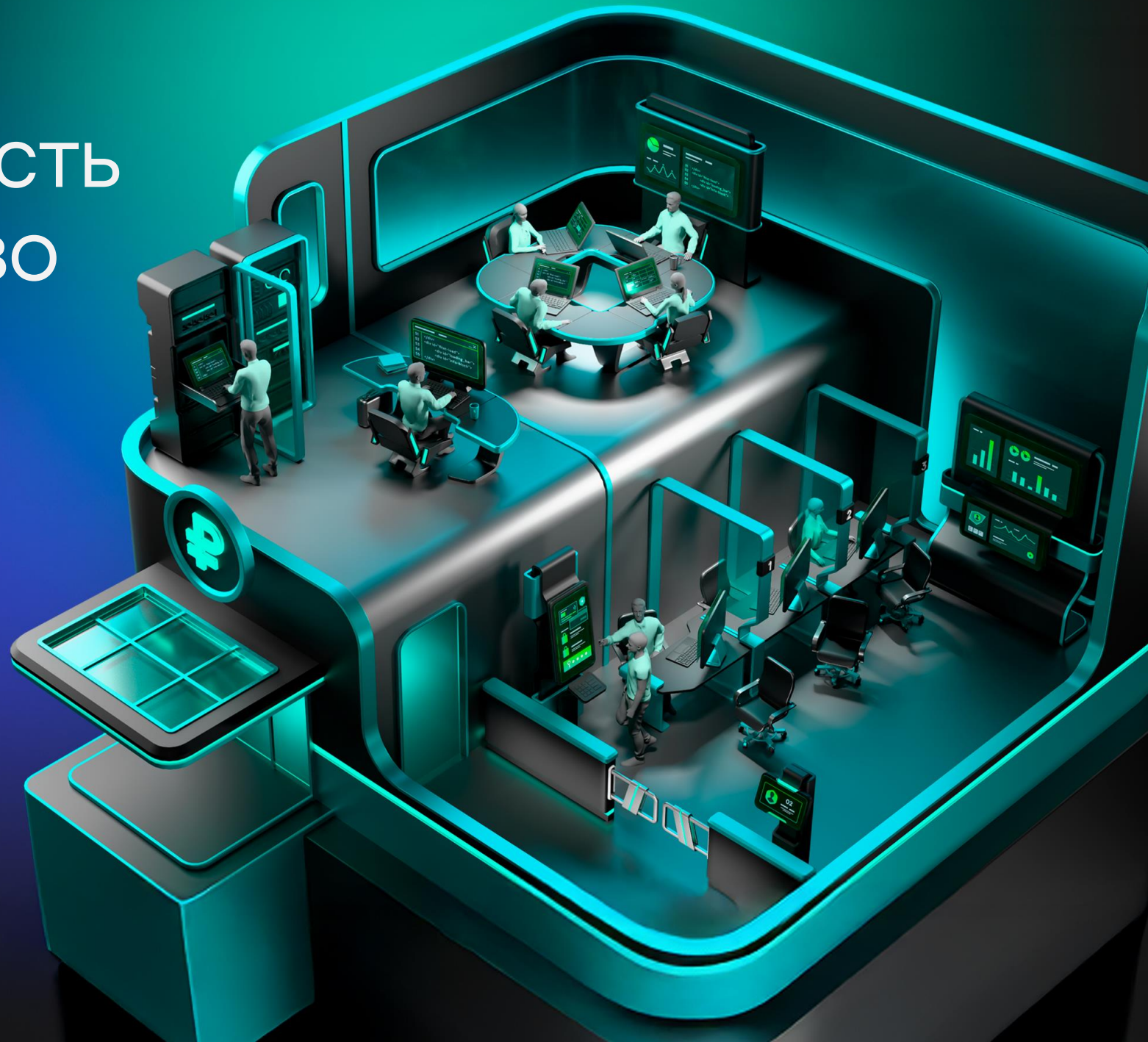
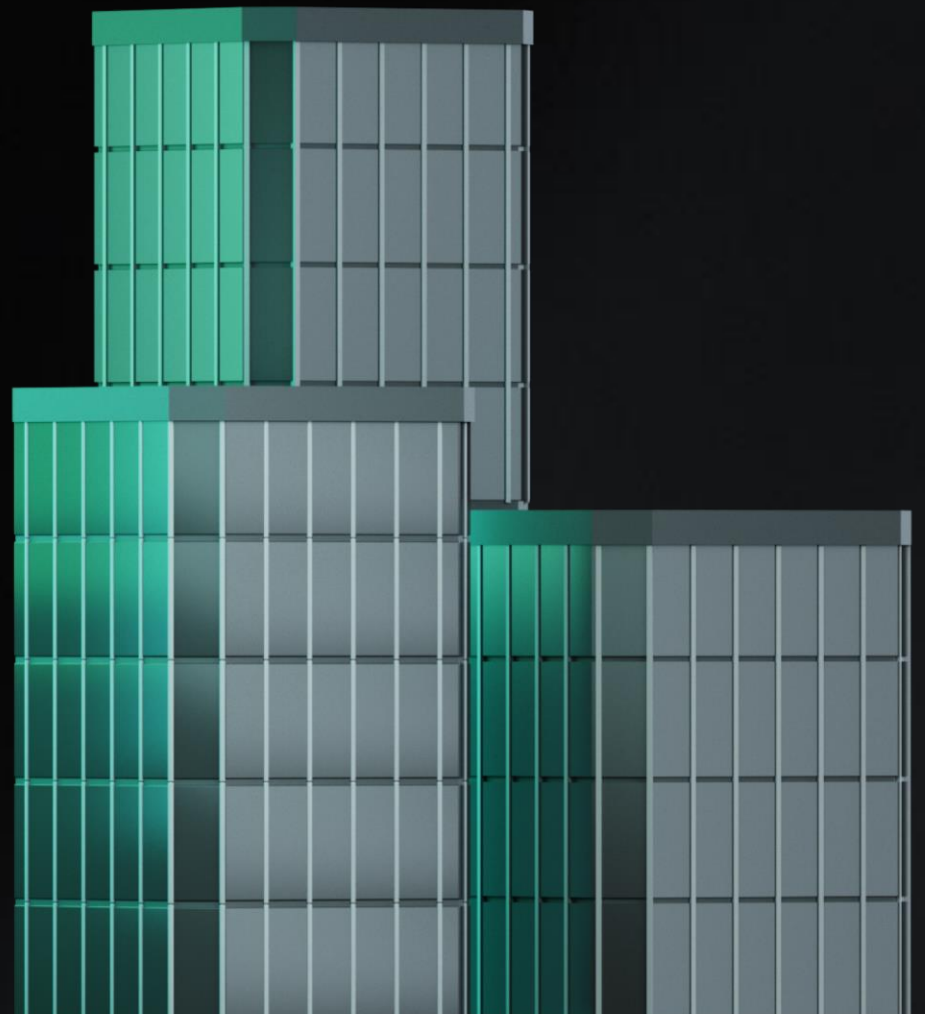
Кибербезопасность как преимущество финансовых организаций



kaspersky

Содержание



01

Обзор приоритетов отрасли, главных трендов и вызовов цифровизации

Обзор финансовой отрасли

Основные участники финансового сектора

Обзор приоритетов отрасли

Финансовые технологии становятся неотъемлемой частью всех видов финансовых услуг, они трансформируют бизнес-модели и повышают их клиентоориентированность

3 основных приоритета финансовых организаций:

Привлечение и удержание клиентов

Реализация проектов по сокращению барьеров в процессе взаимодействия клиентов с банком, внедрение бесшовного клиентского опыта

Информационная устойчивость

Увеличение технологической гибкости и масштабируемости для оптимальной поддержки бизнес-задач

Цифровое доверие и контроль

Защита клиентских данных и развитие перспективных бизнес-моделей на базе защищенной инфраструктуры, соответствующей требованиям регулятора

Привлечение и удержание клиентов

Реализация проектов по сокращению барьеров в процессе взаимодействия клиентов с финансовой организацией, внедрение бесшовного клиентского опыта

Цели:

1. Развитие цифровых каналов
2. Персонализированный подход
3. Повышение удобства пользователей

Краткосрочные планы

- Улучшение мобильного банка или приложения и продвижение омниканального опыта
- Таргетированные клиентские уведомления
- Персонализированные цифровые предложения продуктов и сервисов

Среднесрочные планы

- Виртуальные ассистенты и управление контактным центром
- Развитие сервисов на базе информации о транзакциях
- Оптимизация ценности, генерируемой одним клиентом

Долгосрочные планы

- Финансовая экосистема
- Финансовые операции, встроенные в повседневный образ жизни клиента
- Стратегическая оптимизация ценообразования с использованием больших данных

Информационная устойчивость

Увеличение технологической гибкости и масштабируемости для оптимальной поддержки бизнес-задач

Цели:

1. Устойчивая платформа цифрового банкинга
2. Активное использование облачных сервисов
3. Создание гибкой и масштабируемой IT-архитектуры

Краткосрочные планы

- Постепенное перемещение бизнес-приложений в облако
- Подготовка фреймворка для адаптации облачных сервисов
- Декомпозиция монолитных приложений на микросервисы

Среднесрочные планы

- Приоритизация рабочих нагрузок для трансформации по новым методологиям
- Выбор рабочих нагрузок для миграции в облако
- Оптимизация рабочих процессов для ускорения вывода приложений

Долгосрочные планы

- Мониторинг всех приложений и рабочих нагрузок в режиме реального времени
- Использование ИИ для мониторинга инфраструктуры и проактивного разрешения инцидентов
- Управление API для связанности между всеми устройствами, приложениями и данными

Цифровое доверие и контроль

Защита клиентских данных и развитие перспективных бизнес-моделей на базе защищенной инфраструктуры, соответствующей требованиям регулятора

Цели:

1. Современные технологии идентификации клиентов
2. Усиленная кибербезопасность
3. Комплексное управление рисками

Краткосрочные планы

- Оптимизация цифровых процессов идентификации клиентов
- Отслеживание и отчетность по инцидентам в режиме реального времени
- Управление операционными рисками и устойчивостью

Среднесрочные планы

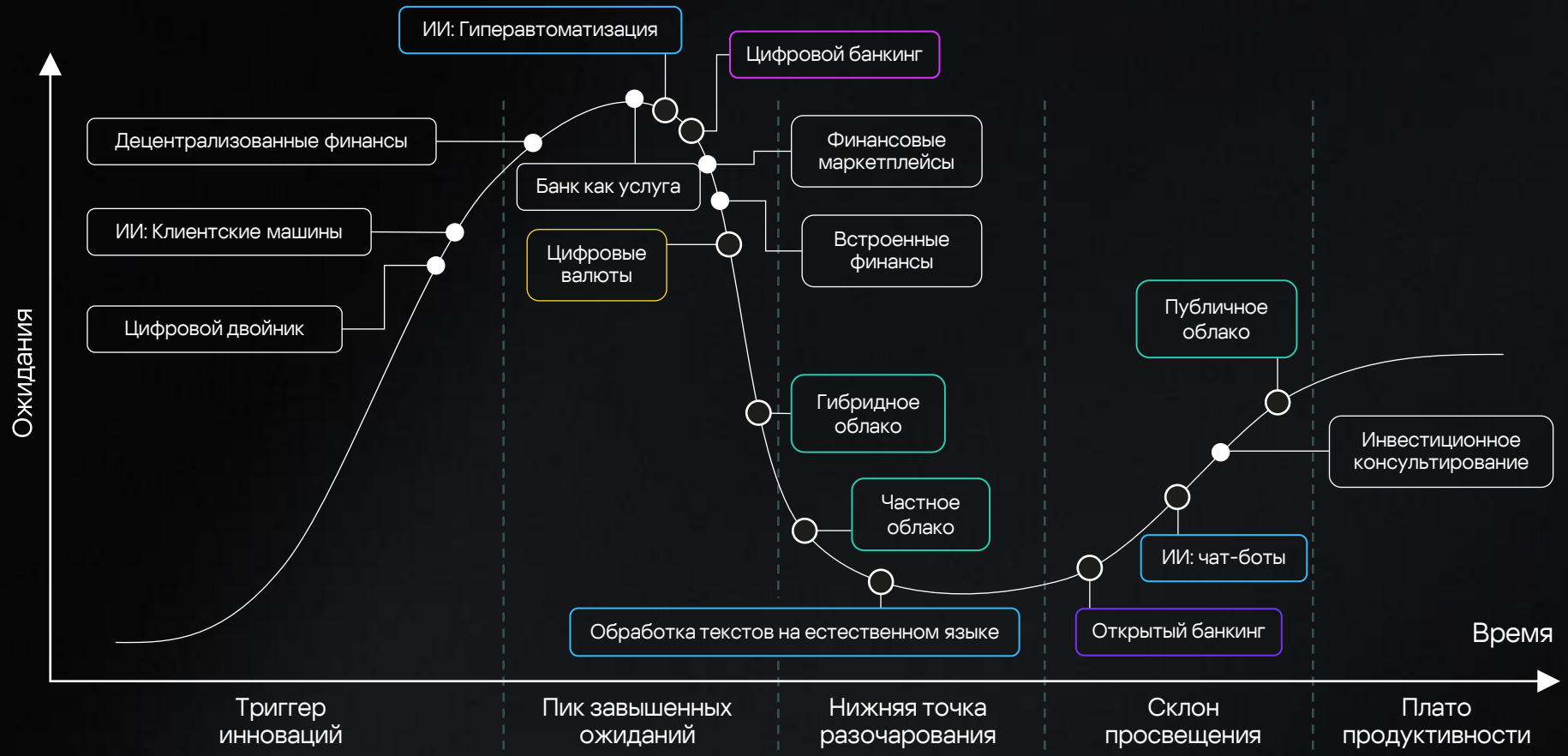
- Продвинутые процедуры проверки клиентов (Know Your Customer, KYC) / (Customer Due Diligence, CDD)
- Интеллектуальная система мониторинга для противодействия отмыванию доходов
- Управление рисками со стороны третьих лиц

Долгосрочные планы

- Скоринговые модели для оценки рисков идентификации клиентов
- Облачные сервисы информационной безопасности
- Анализ здоровья кредитного портфеля и его соответствия требованиям регулятора

Тренды в финансовой отрасли

Большинство трендов неразрывно связано с информационными технологиями



Облачные сервисы

- Гибридное облако
- Частное облако
- Публичное облако

Искусственный интеллект

- Гипераватоматизация
- Чат-боты
- Обработка текстов на естественном языке

Многие обозначенные тренды уже давно существуют на рынках, однако они продолжают масштабироваться и все больше становятся «новой реальностью»

* Цикл зрелости (Gartner Hype Cycle) трендов в финансовой отрасли

Главные тренды в финансовой индустрии

Новые технологии — один из способов поддержать приоритеты финансовых организаций, но они несут в себе новые риски.

1	Открытый банкинг	Открытый банкинг позволяет повысить качество клиентского обслуживания и дать возможность компаниям-партнерам использовать данные банка. Внедрение стандартов открытых API требует соблюдения повышенных мер информационной безопасности, в том числе проведения аудита квалифицированными специалистами.
2	Облачные сервисы	Облачные сервисы помогают масштабировать бизнес и быстро запускать новые проекты без существенных капитальных вложений.
3	Цифровой банкинг	Банки продолжают развивать дистанционный доступ, цифровизацию продуктов и онлайн-сервисы.
4	Искусственный интеллект	Искусственный интеллект все активнее используется для обработки данных и автоматизации рутинных операций. IDC прогнозирует, что к 2026 году 85% организаций по всему миру будут использовать искусственный интеллект и компьютерное зрение.
5	Цифровые валюты	Цифровые валюты нацелены на повышение эффективности платежей и финансовой доступности, а также на снижение рисков, связанных с использованием наличных денег.

+

Другие тренды

- Встроенные финансы
- Банк как услуга (BaaS)
- Децентрализованные финансы (DeFi)
- Финансовые маркетплейсы
- Цифровые двойники
- Инвестиционное консультирование

Приоритеты	Затрагиваемые тренды
Привлечение и удержание клиентов	1, 3, 4, 5
Информационная устойчивость	2, 3, 5
Цифровое доверие и контроль	1, 2, 3, 4, 5

Тренды	Преимущества
1 Открытый банкинг	• Повышенная доступность финансовых сервисов • Конкурентоспособность и развитие инноваций • Улучшенный клиентский опыт
2 Облачные сервисы	• Более масштабируемая и устойчивая инфраструктура • Сокращение затрат на инфраструктуру • Быстрая обработка платежей
3 Цифровой банкинг	• Большая клиентская база • Улучшенный клиентский опыт • Сокращенное время вывода новых услуг на рынок
4 Искусственный интеллект	• Оптимизация рутинных задач • Конкурентоспособность и развитие инноваций • Улучшенный клиентский опыт
5 Цифровые валюты	• Повышенная доступность финансовых сервисов • Конкурентоспособность и развитие инноваций • Улучшенный клиентский опыт

Сегодня цифровизация помогает финансовым организациям расширять спектр услуг, автоматизировать рутинные процессы и экономить ресурсы, но при этом увеличиваются киберриски.

Вызовы, связанные с ключевыми трендами

- Защита инфраструктуры и данных клиентов
- Соответствие требованиям регуляторов

Ситуационные тренды для России

- Импортозамещение в ИТ и ИБ
- Усиление регуляторных требований
- Слияния-поглощения

- Внутренняя разработка
- Рост объема трансграничных переводов

Финансовые организации

Работают
с «живыми» деньгами

Обрабатывают огромное
количество транзакций

Привлекают наиболее
продвинутых киберпреступников

Опрос руководителей и директоров по ИБ (CISO)*

Что в настоящее время влияет на кибербезопасность банков **больше всего**?

Быстрая цифровизация отрасли

Расширение и усложнение инфраструктуры, которая требует защиты.

Строгое регулирование отрасли

Построение систем информационной безопасности с учетом требований регуляторов.

Цифровая трансформация должна учитывать риски кибербезопасности.

Кибербезопасность должна строиться с учетом требований регуляторов.

* Ответы на основе глубинных интервью, которые проводила «Лаборатория Касперского»

Цифровизация финансового сектора

Быстрая цифровизация → Необходима защита более сложной инфраструктуры

Вызовы кибербезопасности

- Расширение поверхности атаки
- Новые уязвимости и угрозы
- Наличие устаревших (legacy) систем
- Управление и защита сложной инфраструктуры
- Недостаток знаний
- Нехватка специалистов
- Ограничения бюджета
- Строгие регуляторные требования

Риски

- Ваша система может подвергаться атаке прямо сейчас
- Частая проблема — злоумышленники внутри компании
- Атаки на ЦОД могут причинить серьезный ущерб
- Шифровальщики могут заблокировать важные данные и устройства
- Утечка конфиденциальных данных влечет не только денежные, но и репутационные потери
- Необходимо полностью соблюдать сложные требования регулирующих органов

Примеры необходимых действий

- Общая защита инфраструктуры
- Защита платформы онлайн-банкинга и ее клиентов
- Защита финансовых операций, проводимых через различные каналы – банкоматы, платежные терминалы и онлайн-банкинг
- Защита данных клиентов от взлома и кражи
- Устранение рисков, связанных со сторонними поставщиками и провайдерами
- Обеспечение соответствия нормативным требованиям

Задачи финансовой организации

Понимаем важность регуляторных требований для финансовой отрасли

Соответствие ГОСТ Р 57580

Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер.

Перечень документов соответствия

Стандарты

- ГОСТ Р 57580.1-2017
- ГОСТ Р 57580.2-2018
- И другие

Нормативные акты Банка России

- ФЗ № 86
- ФЗ № 161
- Положение 821-П
- Положение 757-П
- Положение 683-П

Задачи финансовой организации

Понимаем важность регуляторных требований для финансовой отрасли

Создание системы информационной безопасности

Соблюдение требований при построении системы киберзащиты позволяет обеспечить высокий уровень защиты информации, нейтрализовать актуальные угрозы.

Перечень документов соответствия

ГИС

- ФЗ № 149
- Приказ ФСТЭК России № 17
- Приказ ФСБ России № 524

ИСПДн

- ФЗ № 152
- ПП № 1119
- Приказ ФСТЭК России № 21
- Приказ ФСБ России № 378

КИИ

- ФЗ № 187
- ПП № 127
- Приказ ФСТЭК России №239
- Приказ ФСТЭК России № 235

Задачи финансовой организации

Понимаем важность регуляторных требований для финансовой отрасли

Подготовка к аттестации

Целью аттестации является проверка соответствия объекта информатизации установленным требованиям, выявление возможных уязвимостей и рисков.

Перечень документов соответствия

ГИС

- Приказ ФСТЭК России № 17
- Приказ ФСБ России № 524

Аттестация

- Приказ ФСБ России № 77

Задачи финансовой организации

Понимаем важность регуляторных требований для финансовой отрасли

Подготовка к категорированию

Целью категорирования является определение уровня значимости объекта КИИ, что позволяет применить необходимые меры защиты информации.

Перечень документов соответствия

КИИ

- ФЗ N°187
- Приказ ФСТЭК России № 239
- Приказ ФСТЭК России № 235

Категорирование

- ПП № 127

Задачи финансовой организации

Понимаем важность регуляторных требований для финансовой отрасли

Интеграция с ГосСОПКА

Требуется при необходимости взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы РФ. Для финансовой отрасли также важно обеспечить возможность передачи информации об инцидентах через ФинЦЕРТ.

Перечень документов соответствия

КИИ

- ФЗ №167
- ФЗ №187
- Приказ ФСБ России № 367
- Приказ ФСБ России № 282
- Приказ ФСБ России № 196

Операторы персональных данных

- ФЗ №152
- Приказ ФСБ России № 77

02

Угрозы кибербезопасности

Распространенные угрозы в финансовой отрасли

42%
всех инцидентов в 2024 году было связано с использованием шифровальщиков*

Шифровальщики

Каждое 14-е
заражение устройства пользователя инфостилером может привести к краже банковской карты*

Инфостилеры

13%
рост атак с целью кражи денежных средств в России

Фрод

В 6 раз
выросло количество DDoS-атак в России зимой 2023-2024 года по сравнению с аналогичным периодом годом ранее*

DDoS

* По данным «Лаборатории Касперского» за 2024 г.

Распространенные угрозы в финансовой отрасли

24%
всех киберинцидентов в 2024 году произошло с использованием фишинга*

17%
всех киберинцидентов в 2022–2023 годах были вызваны злонамеренными действиями сотрудников*

Фишинг

Инсайдеры

Распространенные угрозы могут стать первым шагом для реализации более продвинутой атаки

Продвинутые угрозы

* По данным «Лаборатории Касперского» за 2024 г.

Основные продвинутые угрозы в финансовой отрасли

Комплексные целевые атаки (APT)

2023

- LoneZerda
- BlindEagle
- Dark Caracal

2024

- Zanubis
- SideWinder

1 млрд долларов США

Carbanak — масштабная кампания по краже денег, общий ущерб от которой достиг 1 млрд долларов США

За последние 2 года «Лаборатория Касперского» обнаружила 5 крупных APT-кампаний , у которых одной из главных целей были финансовые организации

Основные продвинутые угрозы в финансовой отрасли

Атаки
с использованием
уязвимостей
«нулевого дня»

Google Chrome

в 2024 году эксперты «Лаборатории Касперского» обнаружили уязвимость «нулевого дня» в самом популярном браузере*

Атаки на цепочки
поставок

Бэкдор XZ

потенциально самая опасная атака на цепочку поставок в 2024 году и за все время существования Linux-систем*

* По данным «Лаборатории Касперского» за 2024 г.

Основные продвинутые угрозы в финансовой отрасли

Банковские трояны

Coyote

многоэтапный банковский троянец, нацеленный на клиентов более чем 60 банковских учреждений, с особо сложной цепочкой заражения*

Mamont

>31 тыс.

атак Mamont отразили наши защитные решения за октябрь и ноябрь 2024 года

Grandoreiro

1 700

финансовых институтов и их пользователей стали целью Grandoreiro в 2024 году по миру

* По данным «Лаборатории Касперского» за 2024 г.

Известное вредоносное ПО, нацеленное на финансовые организации

Банковский троян QBot

Также известен как QuackBot и Pinkslipbot. Впервые обнаружен в 2007 году и с тех пор постоянно развивается. В настоящее время банкер доставляется потенциальным жертвам через уже присутствующее на их компьютерах вредоносное ПО, а также при помощи социальной инженерии и спам-рассылок.
Решения «Лаборатории Касперского» для дома и бизнеса используют многоуровневый подход, в том числе поведенческий анализ, для обнаружения и блокировки этой угрозы.

Вредоносное ПО Prilex

Prilex – группировка киберпреступников, которая охотится за данными банковских карт с 2014 года. В последнее время они сосредоточились на атаках через POS-терминалы.
Prilex продолжает эволюционировать. Среди усовершенствований — возможность блокировать транзакции через NFC.
Мошенники устанавливают в POS-терминал вредоносное ПО, прибегая к методам социальной инженерии.
Чаще всего активность Prilex наблюдается в регионе Латинской Америки. Также зловред был использован в Германии.

* APK (Android Package Kit) – формат файлов, используемый операционной системой Android для установки и распространения приложений.

Известное вредоносное ПО, нацеленное на финансовые организации

Банковский троян PixPirate

Поскольку PixPirate относится к последнему поколению банковских троянцев для устройств на базе Android, он может задействовать функции системы автоматизации денежных переводов (ATS). Эта возможность позволяет злоумышленникам автоматизировать процесс вредоносных денежных переводов через платформу мгновенных платежей Pix, активно используемую несколькими бразильскими банками. Приложения-дропперы, используемые для доставки PixPirate, маскируются под приложения-аутентификаторы, обычно распространяемые в виде файлов APK* на фишинговых сайтах.

Троян Emotet

С помощью Emotet злоумышленники получают доступ к конфиденциальным данным на чужих устройствах.
Emotet известен тем, что умеет обманывать базовые антивирусы так, что те не могут его распознать. После загрузки программа ведет себя, как компьютерный червь, стремясь проникнуть на другие устройства сети.
В основном троянец распространяется через фишинговые письма. В электронном письме содержится вредоносная ссылка или зараженный документ.
Emotet впервые обнаружили в 2014 году – троянец атаковал клиентов немецких и австрийских банков. Сейчас Emotet распространился по всему мир и может атаковать компании любой отрасли, также государственные учреждения.

* APK (Android Package Kit) – формат файлов, используемый операционной системой Android для установки и распространения приложений.

Crimeware и финансовые киберугрозы в 2024 году

1. Выросло число атак с использованием ИИ
2. Мошенники чаще атаковали системы мгновенных платежей
3. Вымогатели тщательнее выбирали цели
4. Бразильские банковские троянцы снова были в тренде
5. Было больше бэкдоров в пакетах программ с открытым исходным кодом
6. Преступники чаще использовали ошибки в конфигурации устройств и сервисов
7. Структура преступных групп стала более гибкой
8. Злоумышленники писали зловреды на непопулярных или кроссплатформенных языках
9. Хактивисты стали активнее

https://securelist.ru/ksb-financial-and-crimeware-predictions-2025/114565/

Прогнозы по crimeware и финансовым киберугрозам на 2025 год

1. Всплеск активности стилеров
2. Атаки на центральные банки и механизмы открытого банкинга
3. Рост атак на цепочку поставок в проектах с открытым исходным кодом
4. Новые угрозы на основе блокчейна
5. Искусственная порча данных с помощью шифровальщиков
6. «Нормативный» шантаж в атаках шифровальщиков
7. Распространение модели «шифровальщик как услуга» (RaaS)
8. Больше искусственного интеллекта и машинного обучения в системах безопасности
9. Рост числа финансовых кибератак через смартфоны

https://securelist.ru/ksb-financial-and-crimeware-predictions-2025/114565/

Кибериндиденты в финансовой отрасли

2 место

по стандартным инцидентам

3 место

по критическим инцидентам

Стандартные

Доля зарегистрированных инцидентов в конкретной отрасли от общего числа инцидентов во всех отраслях

Критические

Доля зарегистрированных инцидентов высокой степени тяжести в конкретной отрасли от общего числа инцидентов высокой степени тяжести во всех отраслях

* По данным «Лаборатории Касперского», отчет MDR 2025 г.

Кибериндиденты в финансовой отрасли

В 2024 году финансовый сектор чаще остальных сталкивался с киберугрозами**

~ 270 000

предупреждений безопасности зафиксировано в 2024 году по всему миру*

~ 80 млн ₽

средний размер ущерба от целевой атаки для финансовой организации

> 50%

успешных атак произошло вследствие эксплуатации уязвимостей в инфраструктуре финансовых организаций в 2023 году

16,19%

доля зарегистрированных инцидентов в 2024 году в финансовой отрасли в России*

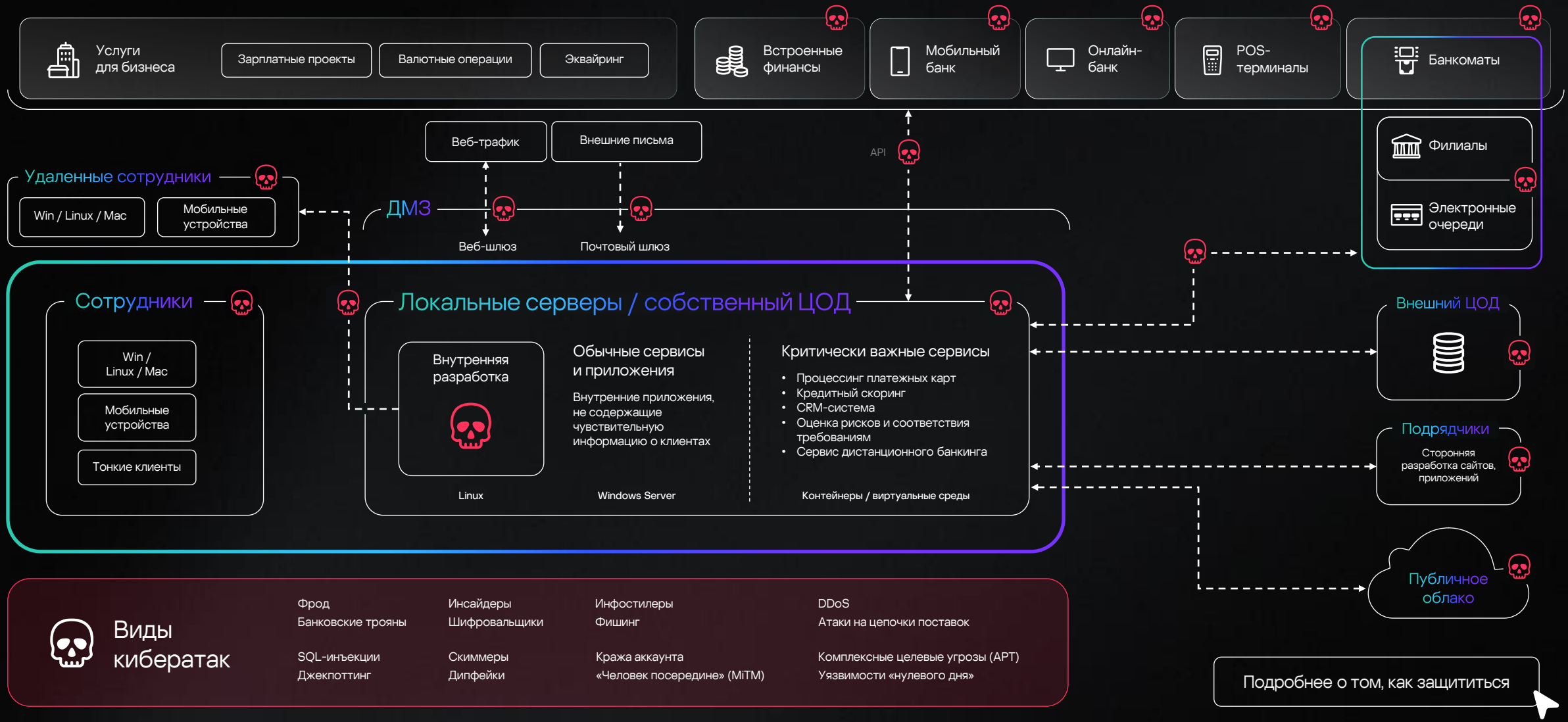
14,52%

доля зарегистрированных критических инцидентов в 2024 году в финансовой отрасли в России*

* По данным «Лаборатории Касперского», отчет MDR 2025 г.

** По данным аналитического отчета «Лаборатории Касперского» Ландшафт угроз для России и СНГ в 2024 году

Пример инфраструктуры клиента с точками входа атак и возможными угрозами



Последствия кибератак для финансовых организаций

- Шифровальщики
- Инфостилеры
- Фрод
- Фишинг
- Инсайдеры
- DDoS
- Комплексные целевые угрозы (APT)
- Атаки с использованием уязвимостей «нулевого дня»
- Атаки на цепочки поставок
- Банковские трояны

Утечка данных

Нарушение бизнес-процессов

Кража денег

Репутационный ущерб

03

Всеобъемлющий подход к защите

Как финансовой отрасли защититься от современных кибератак?

Внедрите целостную стратегию, которая поможет вооружить, проинформировать и подготовить к борьбе со всем спектром современных угроз и атак штатных специалистов или своевременно привлечь наших экспертов.

0

Подготовка

Аудит

Оптимизируйте процессы и актуализируйте информационные активы с помощью инвентаризации всей финансовой инфраструктуры компании (выполняется внутренними специалистами компании или внешними экспертами)

1

Инструменты

Решения

Обеспечьте необходимым инструментарием ваших штатных ИБ-экспертов для устранения киберинцидентов

2

Знания

Аналитика и тренинги

Будьте в курсе современных угроз и повышайте квалификацию своих экспертов, чтобы справиться с киберинцидентами

3

Поддержка

Сервисы

Положитесь на внешних экспертов для анализа защищенности, оперативной помощи и получения дополнительной защиты и рекомендаций

Всеобъемлющий подход к защите*

Нажмите на иконки продуктов, чтобы узнать больше

1. Инструменты
2. Знания
3. Поддержка

1 Инструменты

Комплексная защита от угроз разной степени сложности

Базовая защита от массовых угроз

- Kaspersky Security для бизнеса
- Kaspersky Security для почтовых серверов
- Kaspersky Secure Mobility Management
- Kaspersky Security для виртуальных и облачных сред
- Kaspersky Security для интернет-шлюзов
- Kaspersky NGFW

Расширенная защита от сложных угроз

- Kaspersky EDR Expert
- Kaspersky Anti Targeted Attack
- Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Symphony Security

Kaspersky Symphony EDR

Kaspersky Symphony XDR

Фокусные решения

- Kaspersky Embedded System Security
- Kaspersky Mobile Security SDK
- Kaspersky Fraud Prevention
- Kaspersky Who Calls SDK / REST API
- Kaspersky DDoS Protection
- Kaspersky Scan Engine

За пределами традиционной ИБ

- Kaspersky Container Security
- Kaspersky SD-WAN
- Kaspersky Thin Client

2 Знания

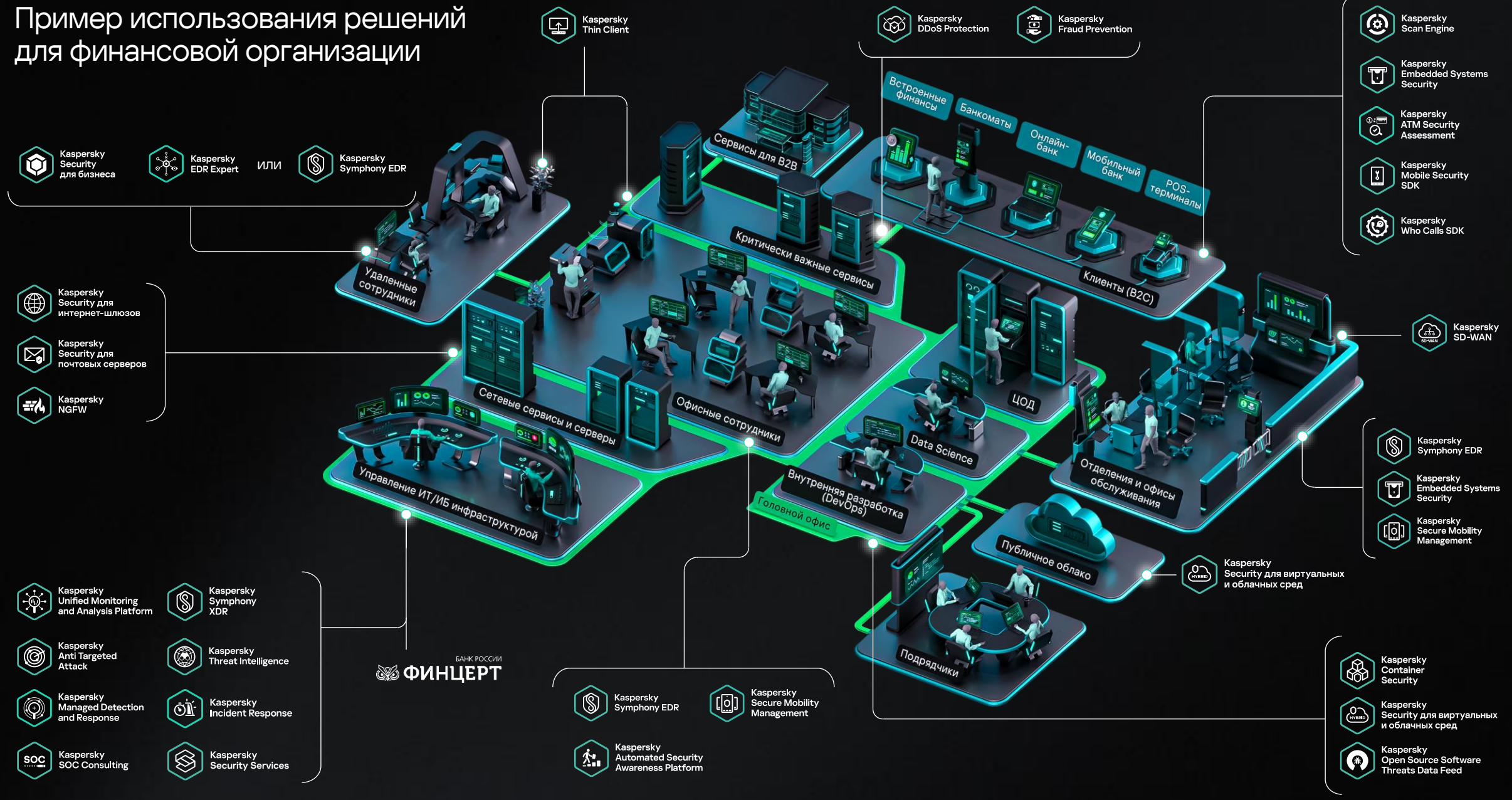
- Осведомленность: Kaspersky Security Awareness
- Аналитика угроз: Kaspersky Threat Intelligence
- Тренинги: Kaspersky Cybersecurity Training

3 Поддержка

- Анализ защищенности: Kaspersky Security Assessment
- Анализ защищенности: Kaspersky ATM Security Assessment
- Управляемая защита: Kaspersky Managed Detection and Response
- Реагирование на инциденты: Kaspersky Incident Response
- Оценка компрометации: Kaspersky Compromise Assessment
- SOC-консалтинг: Kaspersky SOC Consulting
- Профессиональные сервисы: Kaspersky Professional Services

* Представлены основные группы продуктов и сервисов

Пример использования решений для финансовой организации



Результаты внедрения комплексного подхода

- Отказоустойчивая инфраструктура
- Конфиденциальные данные в безопасности
- Низкий риск финансовых потерь
- Соответствие требованиям регуляторов

- Непрерывность бизнеса и доступность сервисов
- Доверие клиентов и партнеров
- Фокус на целевых задачах бизнеса

04

Карточки продуктов и сервисов

Эффективная стратегия кибербезопасности: инструменты

Комплексная защита от угроз разной степени сложности

Киберконтроль всех возможных векторов атак, защита всех активов финансовой организации и охват всех сценариев безопасности

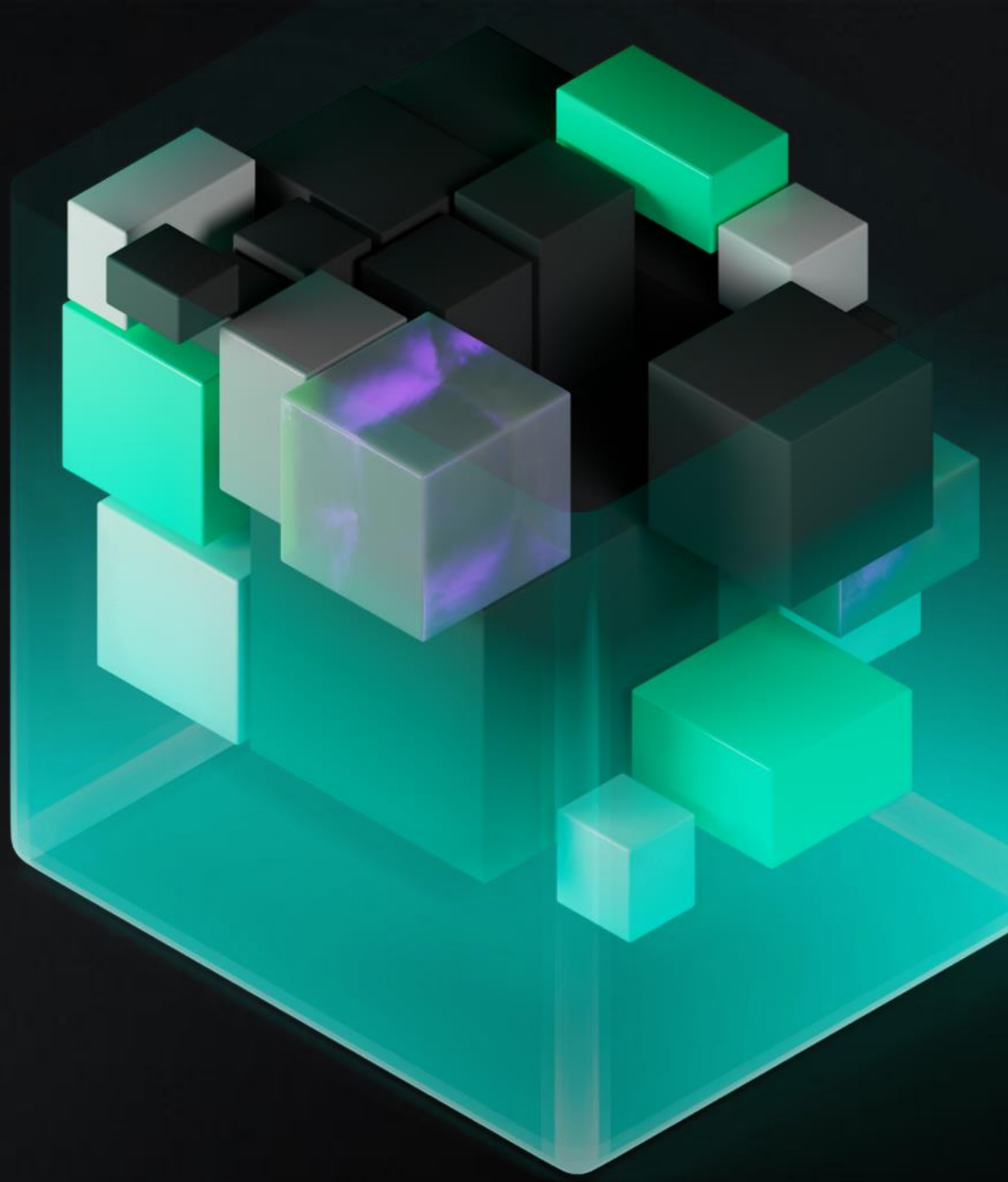
Фокусные решения для нужд отрасли

Действие с учетом специфики и нормативных требований финансовой отрасли, а также особенностей ландшафта угроз

За пределами традиционной ИБ

Мы не только защищаем IT-технологии и процессы финансовых организаций, но и обеспечиваем целостность и защиту сети, гарантируем кибербезопасность и развиваем другие направления

Комплексная защита от угроз разной степени сложности



Kaspersky Security для бизнеса

Страница продукта

Вернуться к схеме

1 Инструменты

Фундаментальная многоуровневая защита конечных точек с фокусом на автоматическую блокировку массовых угроз разной степени сложности, в том числе шифровальщиков и бесфайловых атак. Включает гибкие инструменты контроля конечных точек и позволяет управлять безопасностью из единой консоли.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Новые уязвимости и угрозы
- Нехватка специалистов
- Строгие регуляторные требования
- Ограничения бюджета

Как решение помогает отрасли

Обеспечивает безопасность каждой отдельной конечной точки финансовой инфраструктуры

Предоставляет единую консоль для централизованного управления конечными точками

Защищает от эксплойтов и шифровальщиков, оцениваем и устраняем уязвимости на уровне конечных точек

Помогает контролировать программы, устройства и работу приложений, запущенных на серверах

Поддерживает все основные ОС и средства виртуализации, включая популярные российские операционные системы

Поддерживает полноценную работу на российских ОС и базах данных

Вернуться к схеме

1 Инструменты

Kaspersky Security для виртуальных и облачных сред

Страница продукта

Решение снижает риски безопасности, характерные для облачных сред, включая вредоносное ПО, фишинг и сетевые угрозы и сокращает потребление ресурсов виртуализации. Продукт повышает устойчивость бизнеса и обеспечивает эффективную защиту гибридной среды вне зависимости от используемых типов облаков.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Увеличение поверхности атаки
- Новые уязвимости и угрозы
- Нехватка специалистов
- Строгие регуляторные требования

Как решение помогает отрасли

Защищает гибридные среды вне зависимости от типа рабочей нагрузки и используемых облаков

Поддерживает широкий спектр облачных платформ и сред виртуализации, в т.ч. российские

Повышает прозрачность гибридных инфраструктур и сокращает количество ИТ-инцидентов

Предоставляет единую точку управления всей облачной инфраструктурой

Экономит инвестиции в гибридную инфраструктуру за счет использования оптимизированных легких агентов

Помогает соответствовать требованиям регуляторов на постоянной основе

Вернуться к схеме

1 Инструменты

Kaspersky Security для почтовых серверов

Страница продукта

Решение обеспечивает безопасное использование основного канала бизнес-коммуникации – электронной почты. Защищает от спама, вредоносных писем, любых форм фишинга и других угроз. Оно также контролирует безопасность передачи информации, снижая риски финансовых потерь из-за мошенничества и утечек данных.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Увеличение поверхности атаки
- Новые уязвимости и угрозы
- Ограничения бюджета
- Наличие устаревших (legacy) систем

Как решение помогает отрасли

Обеспечивает надежный и защищенный обмен корпоративной почтой без потерь в скорости коммуникаций

Сокращает риски заражения и утечки данных благодаря расширенным возможностям фильтрации контента

Защищает от всех актуальных угроз - спама, фишинга, BEC, APT, атак через QR-коды и др. – с помощью технологий на базе ML

Использует надежные внешние источники аналитических данных об угрозах, а также собственные передовые исследования и данные TI

Позволяет анализировать объекты в изолированной среде и выявлять даже тщательно замаскированное вредоносное ПО за счет интеграции с KATA

Легко интегрируется с существующей инфраструктурой, почтовыми платформами и уже используемыми решениями для защиты почты

Kaspersky Security для интернет-шлюзов

Страница продукта

Вернуться к схеме

1 Инструменты

Решение надежно защищает от массовых сетевых угроз, включая вредоносное ПО, программы-шифровальщики и майнеры. Обеспечивает контроль доступа к веб-ресурсам, что позволяет минимизировать риск возникновения киберинцидентов по вине сотрудников, а также повысить производительность труда.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Увеличение поверхности атаки
- Новые уязвимости и угрозы
- Ограничения бюджета
- Нехватка специалистов

Как решение помогает отрасли

Обеспечивает полноценную защиту пользователей и рабочих мест от всех видов онлайн-угроз

Эффективно выявляет, анализирует и блокирует вредоносное ПО, включая шифровальщики, майнеры, фишинг и др.

Тщательно контролирует доступ пользователей к веб-ресурсам в соответствии с политиками безопасности компании

Минимизирует последствия применения социальной инженерии в отношении сотрудников за счет контроля сетевых подключений

Обнаруживает и фильтрует вредоносные URL с помощью собственной глобальной репутационной базы

Позволяет обеспечить соответствие требованиям регуляторов за счет проверки веб-трафика

Kaspersky Secure Mobility Management

Страница продукта

Решение для управления парком мобильных устройств, сочетающее в себе технологии защиты и передовые практики управления жизненным циклом мобильных устройств. Оно поддерживает все основные платформы, а полная интеграция в экосистему «Лаборатории Касперского» превращает мобильные устройства в безопасный компонент IT-инфраструктуры, оптимизирует рабочие процессы и повышает общую эффективность работы.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Расширение поверхности атаки
- Новые уязвимости и угрозы
- Ограничения бюджета
- Нехватка специалистов
- Наличие устаревших (legacy) систем
- Строгие регуляторные требования

Вернуться к схеме

1 Инструменты

Как решение помогает отрасли

Обеспечивает безопасность и управление различными видами мобильных устройств с помощью единого интегрированного решения

Позволяет управлять мобильными устройствами как неотъемлемой частью IT-инфраструктуры с централизованной регистрацией событий

Сокращает операционные расходы и нагрузку на сотрудников благодаря автоматизации повторяющихся задач, связанных с жизненным циклом мобильных устройств

Позволяет безопасно использовать в бизнесе разнородный парк мобильных устройств (включая основанные на отечественной AuroraOS)

Помогает обеспечить соответствия нормативным требованиям благодаря широкому спектру средств управления, защиты и предотвращения нарушения политик безопасности

Обеспечивает полноценное импортозамещение покинувших рынок зарубежных решений класса EMM / UEM

Вернуться к схеме

1 Инструменты

Kaspersky NGFW

Страница продукта

Межсетевой экран нового поколения на основе лидерских технологий предоставляет защиту финансовых компаний от широкого спектра киберугроз, контролирует активность приложений и сервисов, позволяет эффективно управлять трафиком и оптимизирует производительность инфраструктуры. Это полностью российский продукт с собственной архитектурой и движками безопасности, который соответствует стратегии движения к импортонезависимости.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Управление и защита сложной инфраструктуры
- Новые уязвимости и угрозы
- Расширение поверхности атаки
- Строгие регуляторные требования
- Нехватка специалистов

Как решение помогает отрасли

Защищает финансовые организации от актуальных сетевых угроз благодаря продвинутым движкам безопасности и регулярно обновляющимся базам

Обеспечивает полный контроль сетевого трафика и активности приложений для управления доступом к интернет-ресурсам и митигации целого спектра угроз

Предоставляет единую точку управления всеми развернутыми NGFW и другими продуктами Kaspersky

Помогает реализовать комплексный подход к защите инфраструктуры благодаря интеграции с решениями класса XDR, SIEM, Sandbox

Оптимизирует рутинные процессы мониторинга и администрирования сети, высвобождая ресурсы профильных специалистов

Помогает соблюдать требования регуляторов и соответствовать стратегии импортозамещения

Вернуться к схеме

1 Инструменты

Kaspersky EDR Expert

Страница продукта

Мощное решение класса EDR, которое предоставляет специалистам ИБ полную картину событий в инфраструктуре рабочих мест и серверов и эффективно защищает их от сложных угроз и APT-атак. Kaspersky EDR Expert обеспечивает визуализацию конечных точек, эффективное обнаружение угроз и реагирование на инциденты, а также предоставляет инструменты для проактивного поиска угроз и анализа первопричин.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Новые уязвимости и угрозы
- Нехватка специалистов
- Строгие регуляторные требования

Как решение помогает отрасли

Обеспечивает усиление классической защиты рабочих мест передовыми технологиям по противодействию сложным угрозам

Усиливает контроль и повышает видимость инфраструктуры рабочих мест финансовой организации

Автоматизирует процессы по сбору данных, выявлению угроз и реагированию на них

Сокращает трудозатраты на процесс обработки сложных инцидентов на уровне конечных точек

Повышает эффективность показателей среднего времени обнаружения и реагирования на инциденты

Обеспечивает централизованное реагирование в распределенной инфраструктуре рабочих мест и серверов

Предоставляет инструментарий для проактивного поиска угроз и сопоставления с матрицей MITRE

Помогает соответствовать требованиям действующего законодательства

Kaspersky Anti Targeted Attack

Страница продукта

Комплексное решение для защиты от APT-атак и других сложных киберугроз, включающее возможности сетевой песочницы, NDR и дополнительно EDR. Решение контролирует безопасность как на уровне сети, так и на уровне рабочих мест, предоставляя полную картину IT-инфраструктуры и защиту от целевых атак.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Увеличение поверхности атаки
- Новые уязвимости и угрозы
- Ограничения бюджета
- Строгие регуляторные требования
- Нехватка специалистов

Как решение помогает отрасли

Обеспечивает продвинутую защиту от целевых атак на уровне сетевого трафика, почты и рабочих мест

Минимизирует риски утечек и финансовые потери благодаря проактивному выявлению рисков, поиску угроз и аномалий

Выявляет атаки, направленные на инфраструктуру, благодаря современным технологиям детектирования и проактивного поиска угроз

Анализирует трафик и выявляет как внешние, так и внутренние сетевые угрозы

Дает полное представление обо всех устройствах в сети, связанных с ними угрозах и объектах, требующих внимания в первую очередь

Использует данные глобальной аналитики об актуальных APT и угрозах для финансового сектора

Kaspersky Unified Monitoring and Analysis Platform

Страница продукта

Высокопроизводительное решение класса SIEM, предназначенное для централизованного сбора, анализа и корреляции ИБ-событий из различных источников для выявления киберинцидентов и своевременной их нейтрализации. Является ключевой технологией для построения SOC в финансовой организации.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Новые уязвимости и угрозы
- Расширение поверхности атаки
- Недостаток знаний
- Ограничения бюджета
- Нехватка специалистов
- Строгие регуляторные требования

Как решение помогает отрасли

Обнаруживает атаки на инфраструктуру банков, осуществляя сбор, нормализацию, хранение и корреляцию событий из массива разных источников

Минимизирует потери от мошеннических транзакций путем своевременного их выявления и приостановления их обработки, а также противодействует другим действиям киберпреступников

Оптимизирует рутинные процессы мониторинга, приоритизации алертов, проактивного поиска за счет использования ИИ

Предоставляет решение для надежного и экономичного хранения логов с удобным поиском по хранящимся данным

Улучшает временные показатели по обнаружению сложных атак на инфраструктуру финансовых организаций

Помогает соответствовать требованиям регуляторов в области безопасности КИИ, в том числе взаимодействовать с НКЦКИ – получать и отправлять данные об инцидентах

Линейка решений Kaspersky Symphony. 4 уровня защиты

1 Инструменты

Kaspersky Symphony — это линейка решений, которая дает организациям все необходимое для постепенной или одночастной реализации подхода к построению надежной и адаптивной системы кибербезопасности. Все элементы этой экосистемы дополняют и усиливают друг друга.

Гибкий выбор

- Kaspersky Symphony XDR
  - XDR Core
- Kaspersky Symphony MDR
- Kaspersky Symphony EDR
- Kaspersky Symphony Security

Функциональное сравнение уровней Kaspersky Symphony

Kaspersky Symphony	Security	MDR	EDR	XDR
Уровень защиты	Базовая собственная защита	Передовая управляемая защита	Передовая собственная защита	Расширенная собственная защита
Автоматическая защита конечных точек (физических, мобильных и виртуальных) от массовых угроз	•	•	•	•
Передовое обнаружение сложных угроз на уровне конечных точек и реагирование на них		•	•	•
Детектирование с помощью передовой песочницы и реагирование на обнаружения				•
Комплексный мониторинг и корреляция событий ИБ (SIEM), встроенный модуль ГосСОПКА, интеграция с различными ИБ-системами				•
Единый граф расследования, плейбуки, управление инцидентами благодаря платформе управления Open Single Management Platform				•
Управление аналитическими данными о киберугрозах (TI Platform) и встроенные потоки данных (data feeds)				•
Защита электронной почты (SEG) и веб-трафика (SWG)				•
Глубокий анализ сетевого трафика (NTA) и реагирование на уровне шлюзов				•
Повышение киберграмотности				•

XDR Core

Kaspersky Symphony Security

Страница продукта

Решение для обеспечения фундаментальной безопасности всех типов конечных точек: компьютеры, серверы, мобильные устройства, виртуальные рабочие места, публичные облака. В основе решения — передовые технологии защиты данных от вредоносного ПО и вторжений, продвинутые инструменты контроля и администрирования и уникальная глобальная экспертиза «Лаборатории Касперского».

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Новые уязвимости и угрозы
- Нехватка специалистов
- Ограничения бюджета
- Строгие регуляторные требования

Как решение помогает отрасли

Обеспечивает безопасность каждой отдельной конечной точки финансовой инфраструктуры, в т.ч. в виртуальных средах

Предоставляет единую консоль для централизованного управления конечными точками

Защищает от эксплойтов и шифровальщиков, оценивает и устраняет уязвимости на уровне конечных точек

Помогает контролировать программы, устройства и работу приложений, запущенных на серверах

Поддерживает все основные ОС и средства виртуализации, включая популярные российские операционные системы

Блокирует файловые, почтовые и веб-угрозы, предотвращает вторжения

Вернуться к схеме

1 Инструменты

Kaspersky Symphony EDR

Страница продукта

Решение, разработанное для экспертов в области ИБ, которое в синергии с включенной базовой защитой конечных точек позволяет блокировать массовые угрозы, автоматически и проактивно искать сложные киберугрозы, проводить расследования инцидентов и предоставляет ИБ-специалистам обширный инструментарий для реагирования на уровне конечных точек.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Новые уязвимости и угрозы
- Нехватка специалистов
- Строгие регуляторные требования

Как решение помогает отрасли

Эффективно блокирует массовые угрозы, обнаруживает и помогает расследовать сложные угрозы в рамках всей инфраструктуры конечных точек

Повышает качество обнаружения сложных угроз и целевых атак, объединяя в одном решении технологии EPP и EDR

Обеспечивает всесторонний обзор всех рабочих мест в инфраструктуре финансовой организации

Оптимизирует затраты на процесс обработки инцидентов на уровне конечных точек

Предоставляет инструменты для проактивного поиска угроз и ретроспективного анализа

Поддерживает различные меры по реагированию

Вернуться к схеме

1 Инструменты

Kaspersky Symphony MDR

Страница продукта

Решение для круглосуточной защиты бизнеса силами экспертов SOC Kaspersky, в том числе включающее в себя решение класса EPP. Команда MDR расследует события безопасности, осуществляет непрерывный мониторинг инфраструктуры организации и анализирует телеметрию на предмет инцидентов. Уникальные индикаторы атак позволяют обнаружить скрытые угрозы, а встроенные механизмы ИИ помогают ускорить процесс обработки событий безопасности.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Увеличение поверхности атаки
- Новые уязвимости и угрозы
- Нехватка специалистов
- Ограничения бюджета
- Строгие требования регуляторов

Как решение помогает отрасли

Мониторит и обнаруживает угрозы 24/7, даже если до подключения решения компрометация уже случилась

Предоставляет возможность пользоваться ключевыми преимуществами SOC, не имея его внутри компании

Защищает все виды хостов – физические, мобильные и виртуальные

Обеспечивает обзор всех защищаемых ресурсов с их текущим статусом

Снижает время реагирования на инциденты с помощью автоматизированных сценариев

Повышает эффективность использования временных, человеческих и других ресурсов вашей команды ИБ

Вернуться к схеме

1 Инструменты

Kaspersky Symphony XDR

Страница продукта

Самое продвинутое решение линейки Kaspersky Symphony по выстраиванию комплексной защиты всей инфраструктуры организации. Решение позволяет централизованно управлять всей ИБ-инфраструктурой и защищать многочисленные точки входа от потенциальных угроз. С Kaspersky Symphony XDR эксперты по ИБ получают полный набор инструментов, которые позволяют выявлять кибератаки на всех этапах их развития, проводить анализ первопричин и оперативно реагировать на сложные инциденты.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Новые уязвимости и угрозы
- Расширение поверхности атаки
- Недостаток знаний
- Ограничения бюджета
- Нехватка специалистов
- Наличие устаревших (legacy) систем
- Строгие регуляторные требования

Как решение помогает отрасли

Комплексно защищает всю ИТ-инфраструктуру и все потенциальные «точки проникновения» от киберугроз любого уровня сложности

Обеспечивает централизованное управление безопасностью всей ИТ-инфраструктуры финансовой компании

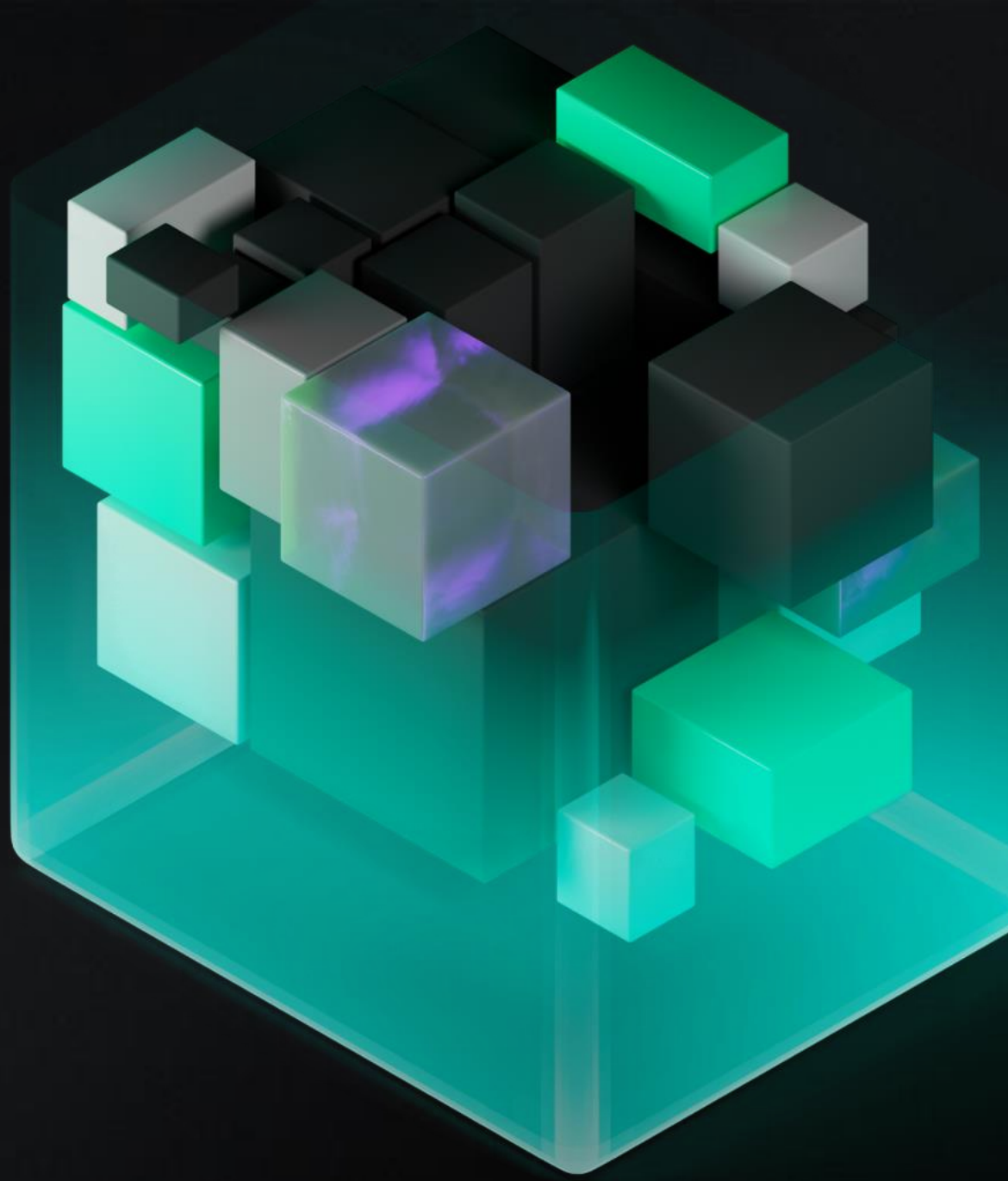
Помогает сэкономить ресурсы за счёт автоматизации рутинных процессов ИБ и снижения потенциальных потерь от кибератак

Помогает тесно интегрировать инструменты ИБ в ваши процессы с поддержкой различных кросс-продуктовых сценариев

Предоставляет встроенную передовую аналитику, повышая эффективность работы с инцидентами

Способствует обеспечению соответствия регуляторным требованиям в вопросах ИБ

Фокусные решения для нужд отрасли



Вернуться к схеме

1 Инструменты

Kaspersky Embedded Systems Security

Страница продукта

Специализированное решение для защиты банкоматов, POS-терминалов и других встраиваемых устройств базе Windows и Linux, а также рабочих станций под управлением уже не поддерживаемых операционных систем. Решение предлагает контроль приложений в сочетании с опциональной защитой от вредоносного ПО и сетевых угроз, контролем целостности и другими технологиями обеспечения безопасности.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Расширение поверхности атаки
- Новые уязвимости и угрозы
- Нехватка специалистов
- Наличие устаревших (legacy) систем

Как решение помогает отрасли

Защищает банкоматы, платежные терминалы и другие встраиваемые системы

Защищает низкопроизводительные устройства со слабым интернет-подключением

Поддерживает широкий спектр встраиваемых платформ и совместимость с устройствами разных типов

Обеспечивает высокую устойчивость к вмешательству извне и атакам инсайдеров

Позволяет оптимизировать безопасность инфраструктуры встраиваемых устройств на базе устаревших операционных систем и оборудования

Kaspersky Fraud Prevention

Страница продукта

Сессионный антифрод, позволяющий выявлять даже самые сложные схемы мошенничества на ранней стадии в режиме реального времени в цифровых каналах – на вебсайтах и мобильных приложениях. За счет комбинации целого спектра технологий Kaspersky Fraud Prevention повышает безопасность клиентов финансовой организации и улучшает их клиентский опыт.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Новые уязвимости и угрозы
- Расширение поверхности атаки
- Недостаток знаний
- Ограничения бюджета
- Строгие регуляторные требования

Как решение помогает отрасли

Обнаруживает кражу учетных записей пользователей, несанкционированный доступ и мошеннические аккаунты

Позволяет обнаружить отмывание денежных средств и финансирование терроризма

Выявляет мошенничество с использованием социальной инженерии

Снижает количество мошеннических событий и улучшает клиентский опыт

Снижает затраты на претензионную работу и расходы на второй фактор (СМС, пуш-уведомления и пр.)

Повышает эффективность фродмониторинга при помощи обогащения дополнительными данными

Обнаруживает злоупотребление маркетинговыми акциями и бонусными программами

Помогает соответствовать требованиям в области противодействия отмыванию денег и выявления фрода в системе быстрых платежей

Kaspersky DDoS Protection

Страница продукта

Вернуться к схеме

1 Инструменты

Решение минимизирует влияние DDoS-атак, обеспечивая постоянную доступность всей инфраструктуры и важнейших онлайн-ресурсов, например клиентских сервисов. Решение включает все необходимое для защиты от любых видов DDoS-атак и уменьшения их последствий – непрерывный анализ трафика, оповещения о возможных атаках, перенаправление трафика в центры очистки и возврат очищенного трафика в сеть.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Новые уязвимости и угрозы
- Расширение поверхности атаки
- Ограничения бюджета
- Нехватка специалистов
- Строгие регуляторные требования

Как решение помогает отрасли

Детектирует и фильтрует DDoS-атаки с первого пакета

Обеспечивает доступность инфраструктуры и сервисов на высоком уровне (99,95%)

Обеспечивает безопасность веб-ресурсов финансовых организаций и митигирует атаки ботов

Защищает шифрованный трафик без раскрытия TLS-сертификата

Предоставляет возможности интеграции с решениями класса WAF для защиты от угроз

Помогает соответствовать требованиям регуляторов

Kaspersky Scan Engine

Страница продукта

Вернуться к схеме

1 Инструменты

Решение для обнаружения и борьбы с киберугрозами, которое с легкостью интегрируется почти с любыми приложениями. Работает через протоколы HTTP и ICAP, позволяя сканировать проходящий трафик и передаваемые объекты. Решение интегрируется с информационными системами, веб-приложениями, прокси-серверами, сетевыми хранилищами данных и почтовыми шлюзами.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Новые уязвимости и угрозы
- Расширение поверхности атаки
- Управление и защита сложной инфраструктуры
- Строгие регуляторные требования

Как решение помогает отрасли

Защищает финансовые системы от угроз из файлов, которые загружают клиенты

Фильтрует вредоносные, фишинговые и рекламные URL-адреса

Обезвреживает зараженные файлы, архивы и зашифрованные объекты

Защищает файловые и резервные хранилища финансовых организаций

Предоставляет широкие возможности интеграции решения с целым рядом платформ и корпоративных систем

Вернуться к схеме

1 Инструменты

Kaspersky Mobile Security SDK

Страница продукта

Набор библиотек, которые позволяют быстро создавать безопасные приложения и интегрировать средства защиты непосредственно в приложение прямо на этапе разработки. Kaspersky Mobile Security SDK позволяет создать на мобильном устройстве безопасную для банковского приложения среду, обеспечивает безопасный доступ к серверам финансовой организации, обнаруживает и блокирует широкий спектр распространенных киберугроз.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Новые уязвимости и угрозы
- Расширение поверхности атаки
- Строгие регуляторные требования

Как решение помогает отрасли

Гарантирует, что мобильные устройства клиентов финансовой организации под надёжной защитой

Обеспечивает надежную передачу финансовой информации только указанным адресатам

Блокирует доступ к вредоносным и фишинговым сайтам и SMS

Обеспечивает соответствие правилам и политикам безопасности

Снижает количество успешных попыток фрода в отношении клиентов

Помогает поддерживать лояльность клиентов в отношении компании за счет минимизации мошеннической активности

Kaspersky Who Calls SDK

Страница продукта

Набор библиотек, которые встраиваются в мобильные приложения финансовой организации для защиты клиентов от мошеннических и нежелательных спам-звонков. Приложение со встроенными библиотеками Kaspersky Who Calls SDK с помощью ИИ-алгоритмов позволяет определять номера телефонов по обширной базе, распознавать опасные звонки и блокировать их. Функции также доступны в рамках веб-сервиса Kaspersky Who Calls REST API, который интегрируется в АТС финансовой организации.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

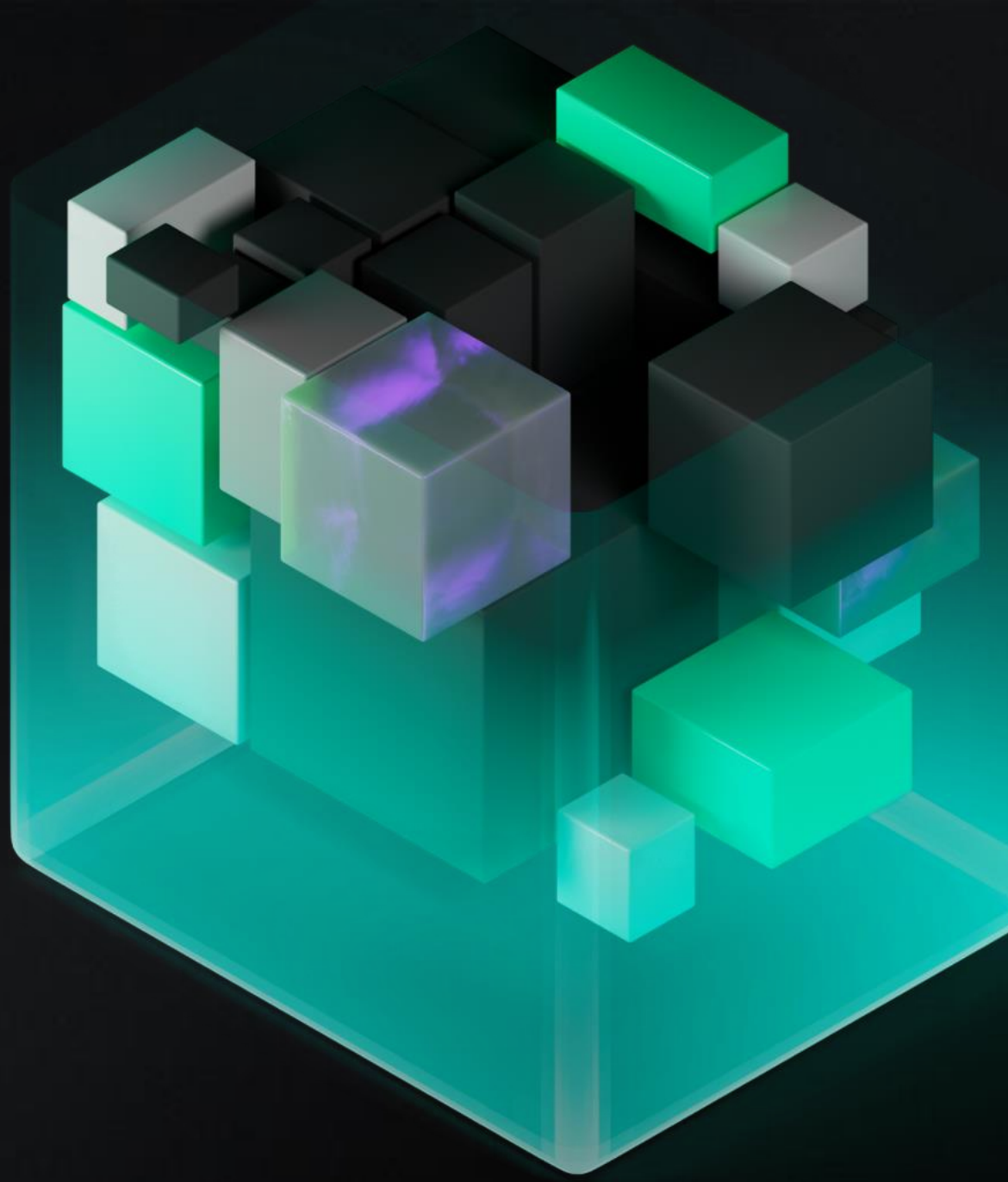
Решаемые проблемы

- Строгие регуляторные требования
- Расширение поверхности атаки
- Недостаток знаний

Как решение помогает отрасли

- Определяет звонки как с телефонных номеров, так и из мессенджеров
- Распознает мошеннические и рекламные звонки и блокирует их
- Предоставляет детальную информацию о номере телефона, включая его репутацию
- Обогащает данными внутренние анти-фрод системы финансовых организаций
- Снижает количество успешных попыток фрода в отношении клиентов
- Помогает поддерживать лояльность клиентов в отношении финансовой организации

За пределами традиционной ИБ



Kaspersky Container Security

Страница продукта

Вернуться к схеме

1 Инструменты

Решение обеспечивает безопасность контейнерных приложений на всех этапах жизненного цикла. Бесшовно встраивается в процесс разработки ПО, учитывает специфику контейнерных сред и защищает каждый компонент: от реестра образов контейнеров до оркестратора. Наглядные и понятные виджеты помогают отслеживать состояние продукта и обнаруживать инциденты безопасности.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Увеличение поверхности атаки
- Новые уязвимости и угрозы
- Недостаток знаний
- Строгие регуляторные требования

Как решение помогает отрасли

Обеспечивает безопасность контейнеризованных приложений, как внутренних, так и клиентских

Повышает прозрачность среды и процессов разработки

Защищает приложения на каждом этапе создания и эксплуатации

Поддерживает широкий спектр популярных оркестраторов, CI/CD-платформ и реестров образов

Проверяет инфраструктуру и приложения на соответствие нормативным требованиям

Ускоряет выход клиентских приложений и сервисов

Вернуться к схеме

1 Инструменты

Kaspersky SD-WAN

Страница продукта

Решение для построения отказоустойчивых распределенных филиальных сетей с централизованным управлением. Позволяет быстро подключать сетевое оборудование и удобно управлять им, обеспечивает необходимое качество работы приложений, повышает уровень безопасности и скорость внедрения новых сервисов, а также сокращает расходы на инфраструктуру. В составе решения используются сертифицированные отечественные аппаратные платформы.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Управление и защита сложной инфраструктуры
- Ограничения бюджета
- Наличие устаревших (legacy) систем
- Строгие регуляторные требования
- Нехватка специалистов

Как решение помогает отрасли

Обеспечивает простое и быстрое подключение отделений, банкоматов и ЦОД	Предоставляет единую точку управления всей сетью, настройками оборудования и политиками ИБ
Обеспечивает максимальное качество сетевого обслуживания для финансовых приложений	Предоставляет возможности для простой интеграции средств защиты и облачных сервисов
Сокращает затраты на каналы связи и обслуживание инфраструктуры	Сокращает количество ИТ-инцидентов и среднее время восстановления
Оптимизирует рутинные задачи и процессы мониторинга сети	Снимает потребность в ИТ/ИБ-специалистах в филиалах

Kaspersky Thin Client

Страница продукта

Кибериммунная инфраструктура тонких клиентов на базе KasperskyOS. Такие тонкие клиенты предназначены для предоставления пользователю доступа к удаленному рабочему столу и служат заменой локальной рабочей станции. Благодаря кибериммунному подходу тонкие клиенты на базе KasperskyOS безопасны по умолчанию. Решение быстро интегрируется в инфраструктуру и получает настройки в автоматическом режиме.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Управление и защита сложной инфраструктуры
- Расширение поверхности атаки
- Строгие регуляторные требования

Как решение помогает отрасли

Предоставляет безопасные кибериммунные рабочие места сотрудникам

Контролирует сетевые подключения пользователей к удаленным рабочим столам

Обеспечивает безопасность данных, передаваемых между сотрудниками и финансовой инфраструктурой

Предоставляет централизованную систему управления для ИБ- и ИТ-специалистов

Обеспечивает гибкое управление и контроль всей инфраструктуры тонких клиентов, которая может содержать до 100 000 узлов

Эффективная стратегия кибербезопасности: знания

Знания о киберугрозах

Предоставляем достоверные и релевантные данные об угрозах в различных форматах. Уникальные аналитические данные укрепляют систему безопасности и помогают принимать конкретные меры

Знания о важности киберграмотности

Тренинги по повышению осведомленности помогают выработать у сотрудников навыки кибербезопасного поведения и мотивируют их применять эти навыки в повседневной работе

Практические знания о работе с инцидентами

В ходе тренингов эксперты оттачивают навыки работы с цифровыми уликами, узнают, как обнаруживать и анализировать вредоносное ПО, а также как эффективно реагировать на инциденты

Kaspersky Security Awareness

Страница продукта

Гибкий подход к формированию навыков кибербезопасного поведения помогает снизить количество инцидентов, вызванных человеческим фактором. Наши отраслевые тренинги в игровой форме помогают руководителям и менеджерам внедрять эффективные стратегии киберзащиты, а автоматизированная платформа позволяет повысить осведомленность об угрозах рядовых сотрудников.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Новые уязвимости и угрозы
- Недостаток знаний
- Строгие регуляторные требования
- Расширение поверхности атаки

Как решение помогает отрасли

Предотвращает инциденты безопасности, вызванные человеческим фактором

Укрепляет общую защищенность финансовых организаций и развивает культуру безопасности на всех уровнях

Повышает осведомленность и прививает навыки безопасного поведения

Повышает вовлеченность сотрудников в процесс защиты конфиденциальных данных

Предоставляет возможность управления настройками защитных решений с учетом результатов обучения сотрудников

Формирует навыки распознавания признаков атак и правильного поведения в случае инцидента

Kaspersky Threat Intelligence Portal

Страница продукта

Портал предоставляет доступ ко всем человекочитаемым аналитическим данным об угрозах через единый веб-интерфейс, где сервисы работают взаимосвязанно, усиливая друг друга. Сводя воедино все знания и опыт, используя технологии обработки и анализа данных, портал помогает финансовым организациям эффективно противостоять современному ландшафту киберугроз.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Новые уязвимости и угрозы
- Расширение поверхности атаки
- Недостаток знаний
- Нехватка специалистов

Как решение помогает отрасли

Обеспечивает единую точку доступа к актуальным и достоверным знаниям об угрозах для предотвращения атак на ранних стадиях	Повышает уровень знаний штатных специалистов об угрозах и улучшает эффективность процесса работы с инцидентами
Предоставляет гибкий сервис поиска угроза и их взаимосвязей для ускорения процесса расследования инцидентов	Помогает защитить бренд, отслеживать цифровые активы и угрозы в даркнет-ресурсах
Усиливает процесс анализа файлов с помощью «песочницы», атрибуции атак и выявления схожести файлов	Предоставляет актуальный ландшафт угроз с учетом отраслевой и региональной специфики
Предоставляет отчёты об угрозах, связанных с APT и финансово мотивированными группировками	Помогает аналитикам отслеживать инфраструктуры кибергруппировок

Kaspersky Threat Data Feeds

Страница продукта

Более 30 готовых потоков данных об угрозах для решения разных ИБ-задач финансовых организаций. Потоки данных предоставляют информацию об известных вредоносных программах, фишинговых веб-сайтах, последних уязвимостях, эксплойтах и пр., усиливая различные решения ИБ. Kaspersky Threat Data Feeds позволяют командам безопасности не только обнаруживать угрозы, но и эффективно определять приоритет инцидентов, которые требуют немедленного устранения, предоставляя дополнительный ценный контекст из разнообразных источников Kaspersky.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Новые уязвимости и угрозы
- Расширение поверхности атаки
- Недостаток знаний
- Нехватка специалистов

Как решение помогает отрасли

Усиливает ИБ-решения, включая SIEM, XDR, межсетевые экраны, IPS/IDS, Security Proxy и пр., постоянно обновляемыми индикаторами компрометации и действенным контекстом

Обогащает SIEM-системы высококачественными данными об угрозах с полезным контекстом для повышения качества детектирования и снижения нагрузки на них

Интегрируется с TI-платформами, в том числе Kaspersky CyberTrace, для эффективного управления потоками данных об угрозах и создания проактивной системы защиты от киберугроз

Предоставляет возможность интеграции индикаторов с высоким уровнем доверия в периметровые СЗИ для блокировки угроз, в том числе в NGFW иностранного производства

Помогает быстрее выявлять критические уведомления и передавать их в приоритетном порядке группам реагирования на инциденты

Позволяет защитить процесс разработки программного обеспечения от угроз в компонентах с открытым исходным кодом

Kaspersky Digital Footprint Intelligence

Страница продукта

Комплексный сервис для защиты от цифровых угроз, который помогает клиентам отслеживать свои цифровые активы и обнаруживать угрозы в даркнете и видимой части интернета. Благодаря оповещениям в режиме реального времени Kaspersky Digital Footprint Intelligence позволяет организациям быстро и эффективно реагировать на потенциальные угрозы.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Новые уязвимости и угрозы
- Расширение поверхности атаки
- Недостаток знаний
- Нехватка специалистов

Как решение помогает отрасли

Обеспечивает комплексный мониторинг всех активов финансовой организации, которые могут подвергнуться атаке или компрометации

Определяет сетевые ресурсы и службы, являющиеся потенциальными векторами атаки

Осуществляет мониторинг мошеннических действий, которые могут нанести ущерб репутации компании и/или обмануть клиентов

Обнаруживает скомпрометированные данных сотрудников, партнеров и клиентов, включая номера банковских карт

Осуществляет непрерывный мониторинг даркнета на предмет любых упоминаний финансовой организации клиента

Предотвращает негативное влияние на работоспособность бизнеса

Kaspersky Cybersecurity Training

Страница продукта

Тренинги для укрепления навыков в области анализа вредоносных программ, реверс-инжиниринга, активного поиска угроз и реагирования на инциденты. Программы обучения повышают уровень знаний и квалификацию штатных специалистов, решая проблему нехватки профессионалов в области кибербезопасности. Развивая эти навыки, организации могут снизить существующие риски и эффективно реагировать на инциденты.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Увеличение поверхности атаки
- Строгие регуляторные требования
- Недостаток знаний
- Нехватка специалистов

Как решение помогает отрасли

Развивает специализированные навыки и повышает квалификацию в области ИБ

Решает проблему нехватки квалифицированных специалистов

Повышает эффективность обнаружения угроз и скорость реагирования на инциденты

Обученные сотрудники обеспечат полный контроль над защитой инфраструктуры без привлечения специалистов со стороны

Способствует снижению рисков и повышению эффективности работы команды

Сокращает время расследования и реагирования благодаря имеющимся знаниям и оперативным действиям команды

Эффективная стратегия кибербезопасности: поддержка

Управляемая защита

Круглосуточная управляемая защита силами экспертов «Лаборатории Касперского» от растущего числа киберугроз

Консалтинг и анализ защищённости

Всесторонняя проверка ваших систем и средств защиты на устойчивость к киберугрозам

Профессиональные сервисы

Развертывание, обслуживание и оптимизация продуктов «Лаборатории Касперского» для получения максимума преимуществ

Kaspersky Application Security Assessment

Страница продукта

Анализ защищенности приложений помогает выявлять уязвимости в веб- и мобильных приложениях, включая онлайн-банкинг. Сочетание экспертного анализа и передовых инструментов позволяют обнаружить слабые места в архитектуре приложений и бизнес-логике. По итогам тестирования предоставляются рекомендации по усилению безопасности приложений.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Недостаток знаний
- Новые уязвимости и угрозы
- Нехватка специалистов
- Расширение поверхности атаки

Как решение помогает отрасли

Оценивает устойчивость критически важных приложений к реальным кибератакам

Обнаруживает уязвимости и логические ошибки в критически важных приложениях

Предоставляет экспертные рекомендации по повышению безопасности приложений

Минимизирует финансовые потери за счет раннего выявления уязвимостей в приложениях

Помогает снизить риски утечки данных и мошеннических действий, выявляя слабые места в приложениях

Помогает защитить репутацию благодаря выявлению слабых мест и уязвимостей в приложениях

Kaspersky Penetration Testing

Страница продукта

Тестирование на проникновение имитирует реальные атаки, чтобы выявить уязвимости внутри сети и на периметре. Сочетание передовых инструментов и ручного анализа позволяет экспертам Kaspersky выявлять угрозы, которые остаются незамеченными автоматическими системами защиты. Это повышает устойчивость инфраструктуры финансовой организации.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Наличие устаревших (legacy) систем
- Новые уязвимости и угрозы
- Нехватка специалистов
- Увеличение поверхности атаки

Как решение помогает отрасли

Обнаруживает критичные уязвимости внутри сети и на периметре

Минимизирует финансовые потери за счет раннего обнаружения уязвимостей

Оценивает устойчивость финансовой организации к реальным кибератакам на инфраструктуру

Помогает оптимизировать меры безопасности с учетом их влияния на уровень защиты

Помогает усилить защиту данных и снизить риски мошенничества, выявляя слабые места в инфраструктуре

Предоставляет экспертные рекомендации по повышению устойчивости инфраструктуры

Kaspersky Red Teaming

Страница продукта

Тестирование с участием Red Team моделирует реальную атаку, чтобы оценить, насколько эффективно команда кибербезопасности обнаруживает и реагирует на угрозы. Эксперты Kaspersky проводят тестирование с учетом принципов конфиденциальности, целостности и доступности данных в соответствии с международными стандартами и лучшими практиками.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Недостаток знаний
- Новые уязвимости и угрозы
- Нехватка специалистов
- Увеличение поверхности атаки

Как решение помогает отрасли

Оценивает эффективность blue team по навыкам обнаружения кибератак и реагирования на них

Оценивает устойчивость к реальным атакам на критические бизнес-процессы

Предоставляет рекомендации по укреплению системы безопасности

Помогает повысить устойчивость к целевым атакам за счет моделирования реальных угроз

Помогает снизить риск сбоев в критически важных процессах, выявляя слабые места

Минимизирует финансовые потери за счет раннего обнаружения критичных уязвимостей

Kaspersky ATM Security Assessment

Страница продукта

Анализ защищенности платежных систем помогает выявить уязвимости в системах банкоматов (ATM) и POS-терминалов. Эксперты моделируют реальные атаки, анализируют потенциальные угрозы и предоставляют рекомендации по усилению защиты платежной инфраструктуры.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Наличие устаревших (legacy) систем
- Новые уязвимости и угрозы
- Нехватка специалистов
- Увеличение поверхности атаки

Как решение помогает отрасли

Оценивает устойчивость платежной инфраструктуры к реальным кибератакам

Выявляет уязвимости в инфраструктуре банкоматов и POS-терминалов

Предоставляет рекомендации по усилению защиты банкоматов и POS-терминалов

Анализирует потенциальные сценарии взлома и последствий кибератак

Помогает предотвратить мошенничество и сбои за счет раннего выявления уязвимостей в банкоматах и POS-терминалах

Помогает приоритизировать меры безопасности для повышения устойчивости платежной системы

Вернуться к схеме

3 Поддержка

Kaspersky Managed Detection and Response

Страница продукта

Круглосуточная управляемая защита от растущего числа киберугроз, обходящих автоматические средства безопасности. Команда MDR расследует события безопасности, осуществляет непрерывный мониторинг инфраструктуры организации и анализирует телеметрию на предмет инцидентов. Сервис подходит как небольшим банкам или филиалам, у которых нет достаточного количества ИБ-специалистов, так и более крупным финансовым организациям, ИБ-эксперты которых перегружены.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Увеличение поверхности атаки
- Новые уязвимости и угрозы
- Нехватка специалистов
- Ограничения бюджета
- Строгие требования регуляторов

Как решение помогает отрасли

Осуществляет круглосуточный мониторинг и проактивный поиск угроз силами экспертов

Выявляет угрозы на ранней стадии и оперативно реагирует на них с использованием ИИ-аналитики

Высвобождает ресурсы ИБ для решения критически важных задач бизнеса

Предоставляет отчеты с практическими рекомендациями по усилению безопасности

Оптимизирует расходы на безопасность, устраняя необходимости найма и обучения дорогостоящих ИБ-специалистов

Снижает риски простоев и финансовых потерь за счет выявления угроз и сложных атак на ранней стадии

Вернуться к схеме

3 Поддержка

Kaspersky Incident Response

Страница продукта

Сервис позволяет восстановить полную картину инцидента. Kaspersky Incident Response охватывает весь цикл расследования и реагирования: от первичного анализа и сбора данных до определения основного вектора атаки и подготовки плана по устранению последствий.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Нехватка специалистов
- Новые уязвимости и угрозы
- Строгие регуляторные требования
- Ограничения бюджета
- Недостаток знаний

Как решение помогает отрасли

Оперативно локализует угрозы во избежание дальнейших потерь

Проводит глубокий анализ инцидента, выявляя причины и векторы атаки

Восстанавливает хронологию и логику инцидента

Обеспечивает оперативное восстановление после инцидента

Помогает минимизировать риски утечки данных и штрафов, оперативно локализуя угрозы

Предоставляет экспертные рекомендации по повышению устойчивости системы безопасности

Kaspersky Compromise Assessment

Страница продукта

Вернуться к схеме

3 Поддержка

Сервис для выявления активных кибератак, а также ранее незамеченных угроз, которые не удалось обнаружить с помощью существующих инструментов и процессов ИБ.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Нехватка специалистов
- Недостаток знаний
- Новые уязвимости и угрозы
- Строгие регуляторные требования
- Ограничения бюджета
- Увеличение поверхности атаки

Как решение помогает отрасли

Выявляет скрытые атаки и следы компрометации инфраструктуры

Анализирует поведение и функционал отдельных вредоносных файлов

Предоставляет подробные отчеты о выявленных угрозах и индикаторах компрометации

Предоставляет экспертные рекомендации по устранению угроз и укреплению защиты

Предоставляет независимую экспертную оценку вероятности компрометации инфраструктуры

Снижает риски утечки данных и финансовых потерь за счет выявления скрытых угроз

Kaspersky SOC Consulting

Страница продукта

Сервис помогает создать и оптимизировать Центры мониторинга безопасности (SOC). Kaspersky SOC Consulting охватывает все этапы — от разработки архитектуры до оптимизации процессов, помогая эффективно обнаруживать и реагировать на современные киберугрозы.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Нехватка специалистов
- Недостаток знаний
- Новые уязвимости и угрозы
- Строгие регуляторные требования
- Ограничения бюджета

Как решение помогает отрасли

- Разрабатывает и оптимизирует архитектуру SOC
- Помогает внедрять лучшие практики построения SOC
- Оценивает уровень зрелости SOC и помогает его развивать
- Проводит тренинги повышения квалификации команды SOC
- Помогает снизить операционные расходы за счет оптимизации процессов
- Повышает эффективность выявления и реагирования на угрозы

Kaspersky Professional Services

Страница продукта

Профессиональные сервисы помогают укрепить защиту и оптимизировать работу IT-инфраструктуры на базе решений Kaspersky. Наши эксперты предоставляют профессиональную поддержку, чтобы повысить уровень безопасности и обеспечить устойчивость к современным киберугрозам.

Поддерживаемые приоритеты

- Привлечение и удержание клиентов
- Информационная устойчивость
- Цифровое доверие и контроль

Решаемые проблемы

- Недостаток знаний
- Наличие устаревших (legacy) систем
- Нехватка специалистов

Как решение помогает отрасли

Помогает внедрить решения безопасности с учетом специфики финансовых организаций

Обеспечивает техническую и экспертную поддержку систем безопасности

Снижает нагрузку на внутреннюю команду информационной безопасности

Повышает эффективность систем безопасности в вашей инфраструктуре

Повышает устойчивость инфраструктуры к новым и сложным киберугрозам

Оптимизирует расходы и повышает отдачу от инвестиций в кибербезопасность

05

Опыт, наши клиенты и истории успеха

Опыт Kaspersky в финансовой отрасли

> 15 лет

> 100 стран

>3 400 финансовых организаций в мире

Наши технологии и опыт позволяют эффективно свести к минимуму риски для финансовых организаций. Возможности решений соответствуют передовым мировым практикам в области защиты.

~1900
в России и СНГ

~430
в Азиатско-Тихоокеанском регионе

~530
в Европе

~360
в странах Южной и Северной Америки

~230
в странах Ближнего Востока, Турции и Африке

Преимущества «Лаборатории Касперского» для финансовых организаций

1. Отечественное ПО и понимание важности регуляторных требований
2. Технологическое лидерство благодаря опыту мирового уровня
3. Международное признание и вклад в индустрию

Истории успеха

Среди наших клиентов — **крупнейшие банки и финансовые организации** по всему миру

РСХБ Россельхозбанк

В рамках стратегии цифровой трансформации Россельхозбанк осуществляет развитие своих сервисов, уделяя особое внимание вопросам информационной безопасности и следования политике импортозамещения.

Решение от «Лаборатории Касперского» стало центральным элементом системы безопасности компании, повышая степень защищённости от кибератак.

Банк Русский Стандарт

Миграция на отечественное ПО и взаимодействие с российскими производителями повысило надёжность и стабильность IT-систем банка.

Решение от «Лаборатории Касперского» даёт возможность автоматизировать многие рутинные действия, централизованно собирать, анализировать и проводить корреляцию событий из различных источников данных для выявления и предотвращения инцидентов.

Истории успеха

Среди наших клиентов — **крупнейшие банки и финансовые организации** по всему миру

KICB
KYRGYZ INVESTMENT AND CREDIT BANK

Кыргызский Инвестиционно-Кредитный Банк (KICB)

KICB, как динамично развивающийся во все сферах банк, делает упор на надежности и защите своих и клиентских данных, на бесперебойной работе всех сервисов и предоставлении своим клиентам безопасных, качественных услуг.

Современные технологии, постоянные исследования кибератак и системный подход «Лаборатории Касперского» позволяют Банку опережать возникающие угрозы и поддерживать высочайший уровень защиты.

KICB ставит в приоритет безопасность и бесперебойную работу банка для удобства клиентов и оказания им качественных и надежных услуг, в чем банку помогают решения «Лаборатории Касперского» в области информационной безопасности. «Лаборатория Касперского» на протяжении многих лет поддерживает статус надёжного партнёра по эффективной защите от киберугроз. Наше сотрудничество началось с внедрения базовых мер защиты на конечных точках, а впоследствии мы добавили решения по обнаружению и реагированию на целевые атаки и обеспечили комплексную безопасность инфраструктуры банка.

Чынгыз Мендекеев

Руководитель команды Управления информационной безопасности «Кыргызского Инвестиционно-Кредитного Банка»

Истории успеха

Ссылка на документ

Итальянский банк

Banca Popolare di Sondrio

Предпосылки / проблемы:

- Неудовлетворенность имеющейся системой кибербезопасности
- Отсутствие четкого роадмапа у предыдущего вендора
- Неуверенность в том, что вендор будет идти «в ногу со временем»
- Банк хотел в короткие сроки найти решения, которые способны обеспечить эффективную защиту от атак и при этом будут легкими в управлении

Банк начал знакомство с «Лабораторией Касперского» с продукта KES. Успешное внедрение решения обеспечило лояльность нового клиента, и в дальнейшем были куплены KATA и KEDR

Наши решения в банке

- Kaspersky Anti Targeted Attack
- Kaspersky EDR Expert
- Kaspersky Security для бизнеса

> 2600
сотрудников

330
филиалов

2
дата-центра

Истории успеха

Ссылка на документ

Банк в Доминикане

Предпосылки / проблемы:

- Рост количества кибератак на финансовую отрасль в стране
- Развитие компании, расширение спектра предлагаемых услуг, что влечет за собой необходимость внедрения надежных решений по кибербезопасности
- Отсутствие в банке современных решений, которые помогали бы контролировать весь периметр

> Директор по ИТ и цифровой стратегии банка: «Бизнес и стратегия компании ориентированы на технологии, для которых важнее всего безопасность. Чтобы уверенно продвигаться в выбранном направлении, нам требуется множество финансовых инструментов с повышенным уровнем безопасности. Мы должны быть в авангарде».

«Лаборатория Касперского» предоставила комплексное решение, включающее не только продукты, но и сервисы

Наши решения в банке

- Kaspersky Anti Targeted Attack
- Kaspersky Managed Detection and Response
- Kaspersky Security для бизнеса
- Kaspersky Professional Services

\+ Расширенная поддержка и технический менеджер по работе с клиентами

500 сотрудников

31 филиал

Истории успеха

Ссылка на документ

Исламский банк в Бангладеш

aib
Al-Arafah Islami Bank PLC.

Предпосылки / проблемы:

- Отсутствие налаженной системы регулирования вопросов безопасности со стороны государства
- Отсутствие в банке централизованного контроля за ежедневными активностями
- Отсутствие решений по защите сетей и систем

Последствия:

- Многочисленные атаки вирусов, червей и троянцев как на локальную сеть головного офиса, так и на сеть филиалов
- Неконтролируемый доступ к зараженным вирусами веб-страницам и широкое использование незащищенных USB-носителей

Многочисленные заражения вирусными ПО, риск закрытия филиалов, трудности при внедрении онлайн-банкинга

Результат:

- Централизованный контроль использования устройств
- Предотвращение локального заражения в сети филиала

Для решения текущих и предотвращения потенциальных проблем банк внедрил KESB «Лаборатории Касперского»

Наши решения в банке

Kaspersky Security для бизнеса

> 2600 сотрудников

119 филиалов

> 1000 пользователей

06

Почему «Лаборатория Касперского»

Почему «Лаборатория Касперского»

Наша уникальная команда экспертов по информационной безопасности защищает мир от самых сложных и опасных киберугроз. Накопленная база знаний обогащает наши решения и сервисы, выводя их качество на несравненный уровень

>27 лет

строим безопасный мир

>467 тыс.

новых вредоносных файлов обнаруживаем ежедневно

>4,9 млрд

атак остановлено нашими решениями в 2024 году

>220 тыс.

корпоративных клиентов по всему миру

>900

активных групп и операций, связанных с APT, отслеживается нами

5

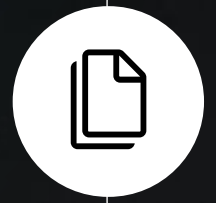
уникальных центров экспертизы

Регуляторный хаб

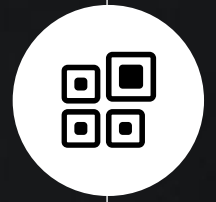
Как помогаем?

Регуляторный хаб поможет финансовым организациям ориентироваться в законодательных требованиях в сфере ИБ и понимать, какими мерами можно закрыть большую часть из них

Помощь в понимании, что необходимо именно вашей организации для соответствия законодательству



Автоматизированный подбор необходимой информации устраняет необходимость в самостоятельном изучении десятков страниц законов, приказов и других документов



Подбор решения для обеспечения информационной безопасности с учетом требований законодательства

Технологическое лидерство благодаря опыту мирового уровня

Исследования и расследования

В основе наших решений лежит мировой опыт в области исследования угроз и расследования инцидентов

Портфель сервисов и решений по ИБ позволяет нашим клиентам всегда быть на шаг впереди злоумышленников и получать экспертную поддержку на протяжении всего цикла реагирования на инциденты.

Безопасный подход к ИИ

Безопасный подход к использованию искусственного интеллекта в наших решениях

От обнаружения угроз с помощью алгоритмов ИИ и сортировки предупреждений до использования генеративного ИИ в аналитике об угрозах и расследовании инцидентов — мы занимаемся этим уже много лет и являемся лидерами в этой области.

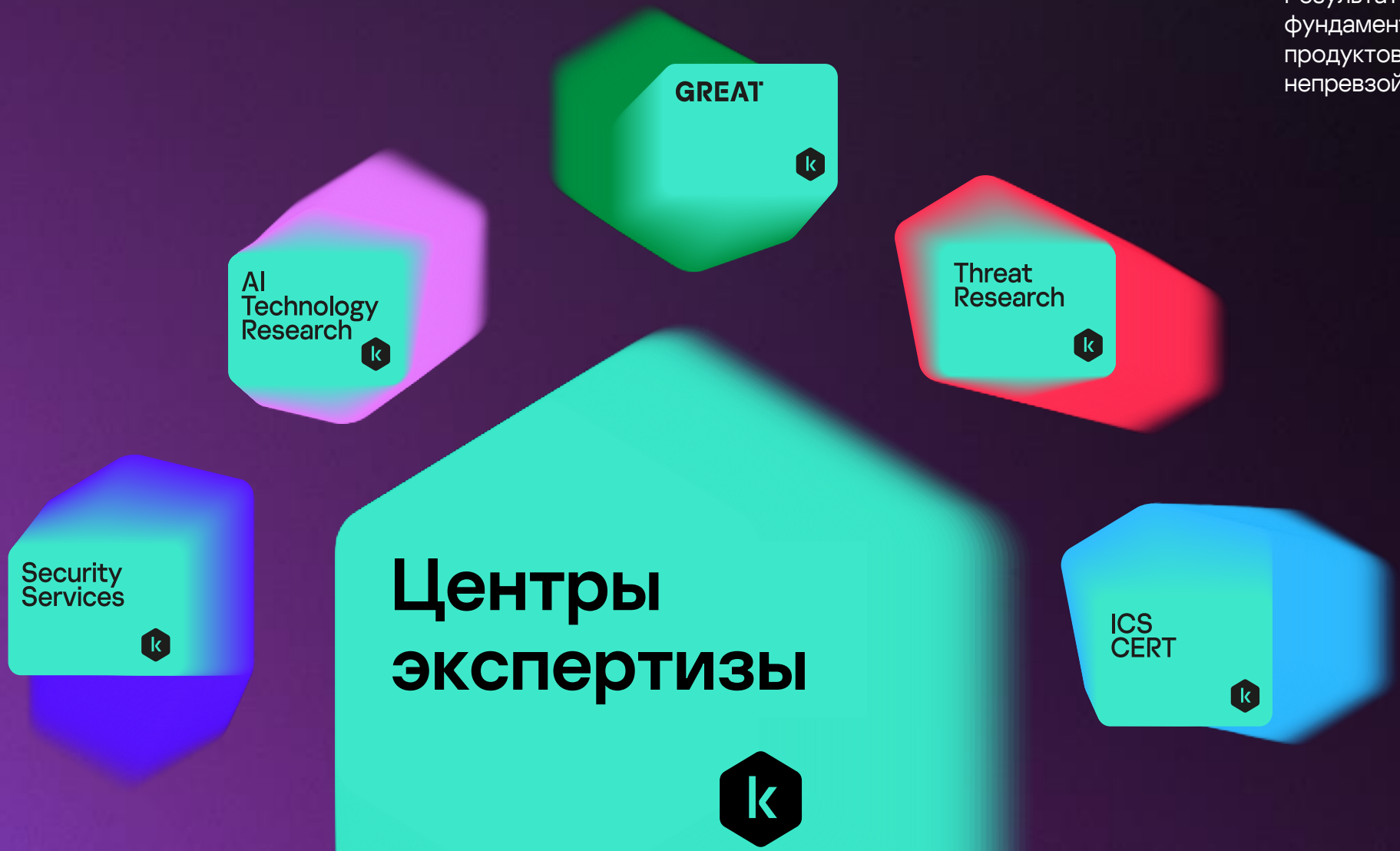
Безопасная разработка ПО

От безопасного жизненного цикла разработки программного обеспечения — к кибериммунным решениям

Безопасная разработка – один из главных принципов, лежащих в основе наших продуктов. Мы пользуемся самыми передовыми подходами к безопасной разработке, от SSDLC до Secure-by-Design.

Уникальная экспертиза

Наши эксперты работают в **пяти центрах экспертизы** и обладают уникальным опытом, глубокими знаниями и специальными навыками. Вносят огромный вклад в исследования киберугроз и расследования киберинцидентов. Результат их работы становится надежным фундаментом для всего портфеля наших продуктов и сервисов и обеспечивает непревзойденную защиту наших клиентов.



Подробнее

ИИ в основе наших решений

Более 20 лет

«Лаборатория Касперского» усиливает свои решения технологиями машинного обучения и искусственного интеллекта, которые позволяют ей быть на шаг впереди злоумышленников.

Основные направления деятельности нашего специализированного центра исследования технологий искусственного интеллекта Kaspersky AI Technology Research:

Интеграция ИИ и машинного обучения в наши решения по кибербезопасности

Проведение исследований по безопасности ИИ-алгоритмов и разработка принципов ответственного использования ИИ

Отслеживание угроз, связанных с использованием ИИ, для выявления новых потенциальных векторов атак

Разработка рекомендаций по безопасному использованию ИИ и участие в Альянсе в сфере ИИ

Исследование технологий генеративного ИИ на базе собственной инфраструктуры для запуска больших языковых моделей

Подробнее

Независимая оценка и прозрачность

Proven.
Transparent.
Independent.

В рамках **Инициативы глобальной прозрачности** «Лаборатория Касперского» предлагает всем заинтересованным лицам конкретные и эффективные инструменты для проверки надежности наших продуктов, внутренних процессов и бизнес-операций.

13

центров прозрачности по всему миру

Регулярные независимые тестирования

- Аудит SOC 2
- Сертификация ISO 27001

Программа Bug Bounty

Награды — знак качества

Продукты «Лаборатории Касперского» регулярно проходят независимую оценку ведущих исследовательских компаний, а наша компетентность в области киберзащиты признана ведущими отраслевыми аналитиками.

Больше тестов. Больше наград.

«Лаборатория Касперского» участвует в независимых тестах и обзорах уже более 10 лет: по результатам 1022 испытаний наши продукты заняли 771 первое место и 871 раз вошли в тройку лидеров, подтвердив свою высокую эффективность.

В 2024 г.

95	91	97%
тестов и обзоров	первое место	ТОП 3 мест

Подробнее

Активный вклад в индустрию

Являясь одним из ключевых мировых поставщиков аналитики о киберугрозах, мы тесно сотрудничаем с широким кругом ведущих международных экспертов в сфере цифровой безопасности и вместе боремся с киберпреступностью по всему миру.

INTERPOL

PARIS CALL FOR TRUST AND SECURITY IN CYBERSPACE 11 • 12 • 2018

industrial internet CONSORTIUM

AFRIPOL

Coalition Against Stalkerware

Мы расследуем киберинциденты и проводим операции по противодействию киберугрозам совместно с мировым ИБ-сообществом и международными организациями, такими как Интерпол, правоохранительными органами и подразделениями CERT по всему миру.

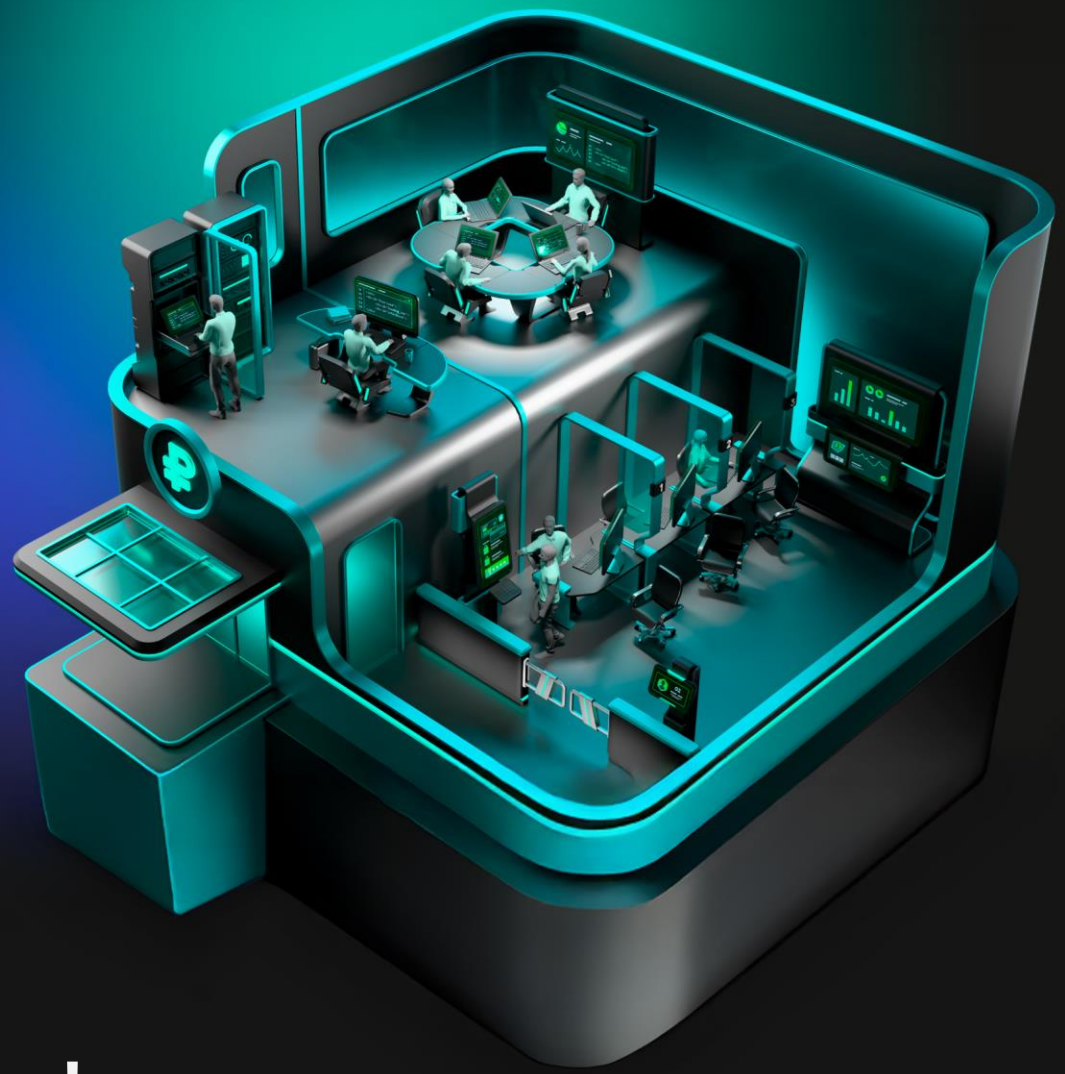
MITRE | ATT&CK®

Собранные нами аналитические данные об угрозах используются в международных проектах, в том числе дополняют матрицу MITRE ATT&CK.

Мы придерживаемся принципов этического раскрытия информации об уязвимостях.

«Лаборатория Касперского» повышает безопасность сторонних продуктов, выявляя и помогая устранять уязвимости нулевого дня в решениях таких крупных компаний, как **Adobe, Microsoft, Google, Apple и другие.**

kaspersky



Спасибо за внимание!

Свяжитесь с нами, чтобы узнать больше о кибербезопасности финансовых услуг

Подробнее