Информационная безопасность: актуальные вызовы и перспективы

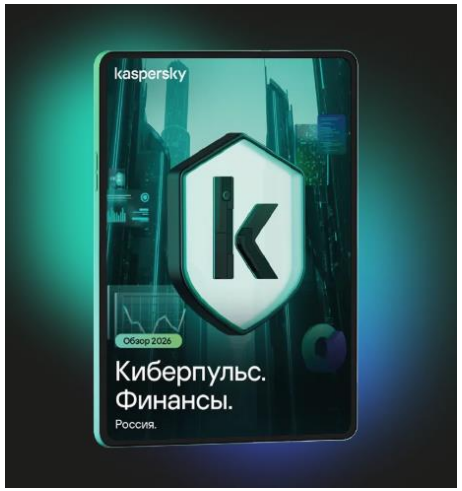
kaspersky

Анатомия ландшафта киберугроз

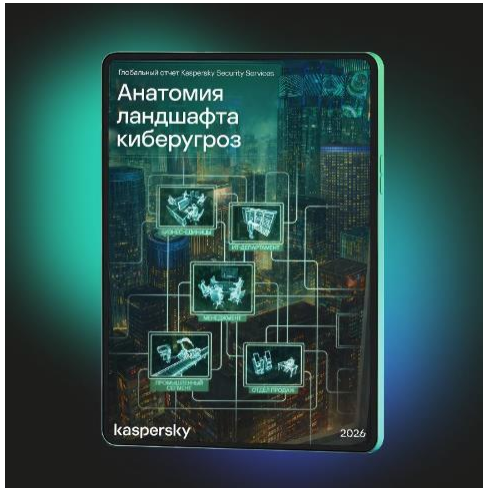
https://lp.kaspersky.com/ru/cyberpulse/











kaspersky

Анатомия ландшафта киберугроз



Исследование охватывает **глобальную** статистику инцидентов и позволяет увидеть, как злоумышленники выбирают **цели**, какие **инструменты** и **техники** применяют, а также какие **меры** наиболее эффективны для защиты организаций.

kaspersky

Анатомия ландшафта киберугроз

I. Введение
II. Критичность инцидентов
III. Выявление атак
IV. Характер инцидентов высокой критичности
V. Тактики атакующих
VI. Техники и процедуры злоумышленников
VII. Эффективность выявления угроз в SOC
VIII. Ограничения детектирования и скрытая компрометация

Ключевая статистика киберугроз для бизнеса в России

Количество кибератак на бизнес в России, 2025 vs 2024[1]

Веб-угрозы

2024

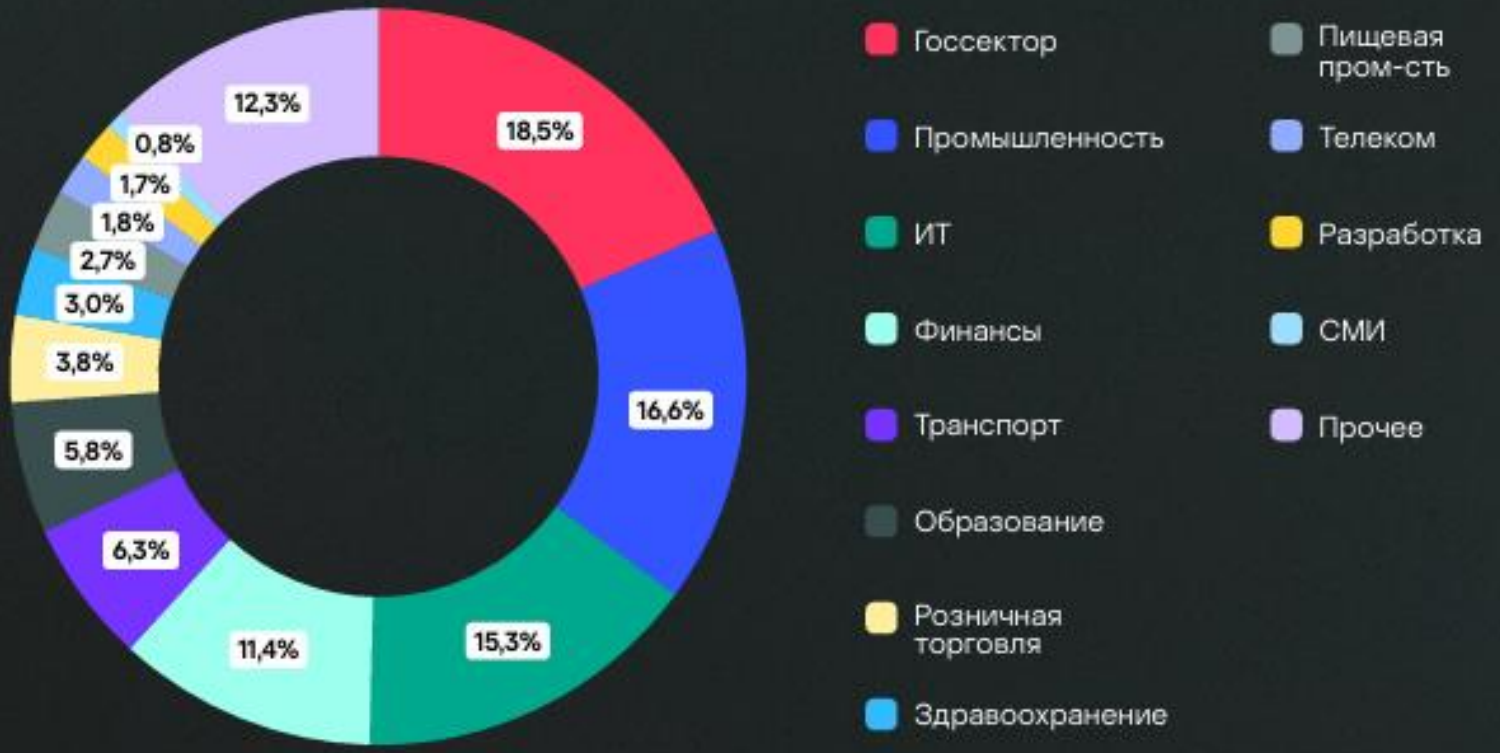
2025 -31%

Угрозы на устройстве

2024

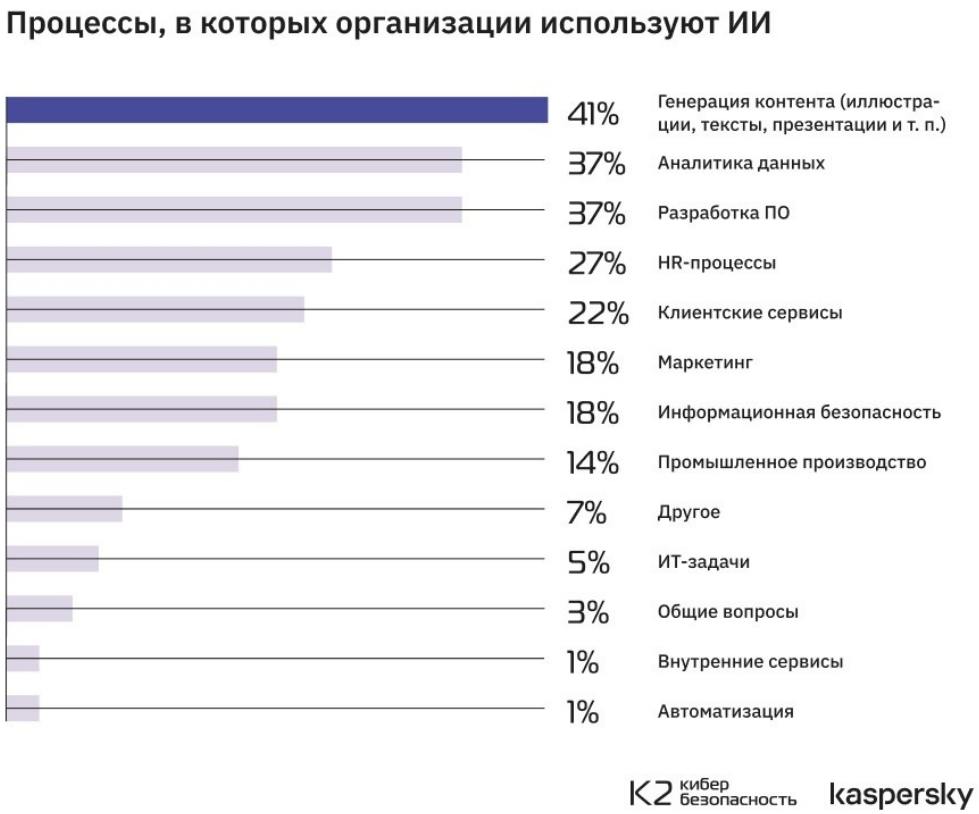
2025 +23%

Распределение инцидентов высокой критичности по отраслевым секторам. Глобальная статистика[2]



Доля критичных инцидентов в ИТ отражает тренд на атаки на цепочки поставок. Инциденты в госсекторе — следствие геополитической напряженности. Потенциально высокая цена ИБ-инцидента для организаций в таких отраслях как финансы, промышленность и транспорт традиционно вызывает повышенный интерес злоумышленников к этим отраслям.

Безопасность ИИ входит в ТОП-5 приоритетов четверти российских корпораций

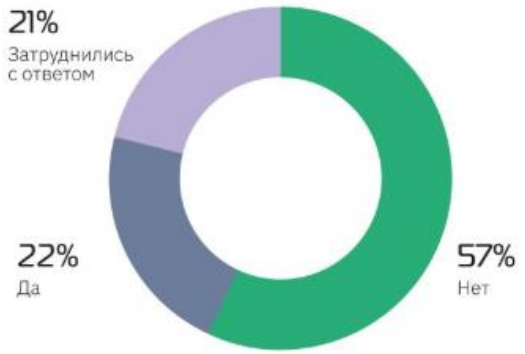


K2 кибер безопасность kaspersky

«Лаборатория Касперского» и К2 Кибербезопасность провели исследование* подходов российского бизнеса к безопасному использованию технологий искусственного интеллекта. Респондентами выступили специалисты из более **200 крупных российских организаций** из следующих отраслей экономики: **ИТ, финансы, торговля, телекоммуникации, строительство, фармацевтика.** Компании представили результаты в преддверии Петербургского международного экономического форума (ПМЭФ).

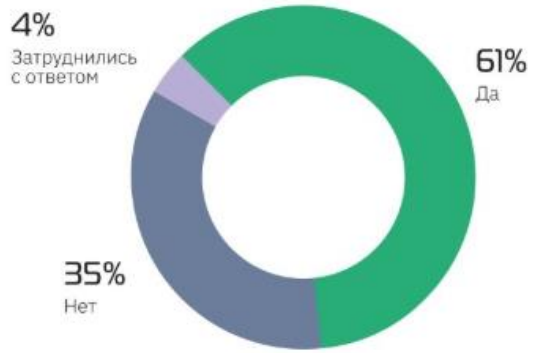
Безопасность ИИ входит в ТОП-5 приоритетов четверти российских корпораций

Выделен бюджет на ИИ-безопасность?

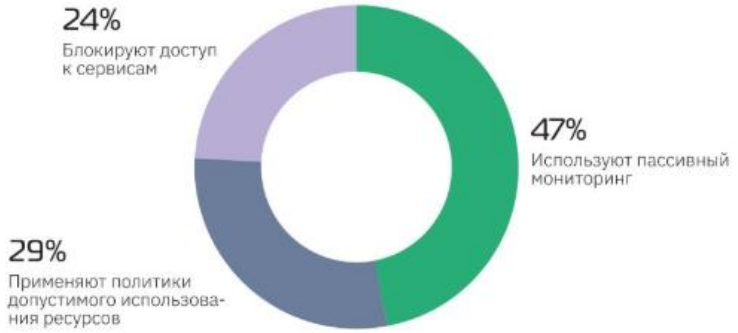


K2 кибер безопасность kaspersky

Руководство компаний стремится к контролю использования внешних ИИ-сервисов?

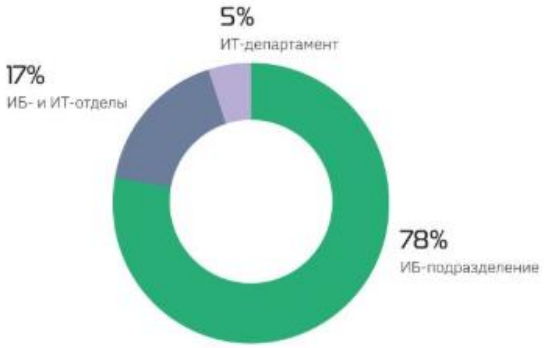


Какие подходы применяются для управления доступом к внешним моделям?



K2 кибер безопасность kaspersky

Кто в компаниях, где отсутствует собственная разработка, несет ответственность за контроль использования ИИ?



K2 кибер безопасность kaspersky

Данные по основным типам угроз для бизнеса в России, 2025 vs 2024

+49%

рост количества атак с помощью шпионского ПО[1]

+55%

рост количества атак с помощью ВПО для кражи паролей[1]

Каждый десятый россиянин генерирует рабочие пароли с помощью ИИ. Чтобы снизить риски и не зависеть от сторонних сервисов, компаниям стоит внедрить корпоративный менеджер паролей: он безопасно создает и хранит уникальные пароли и помогает их вовремя менять[3].

+23% +39% рост в Q1 2026

рост количества атак с помощью банкеров (ВПО для кражи денежных средств через онлайн-доступ к банковским счетам)[1]

+61%

рост количества атак с помощью бэкдоров[1]

-0,5% +20% рост в Q1 2026

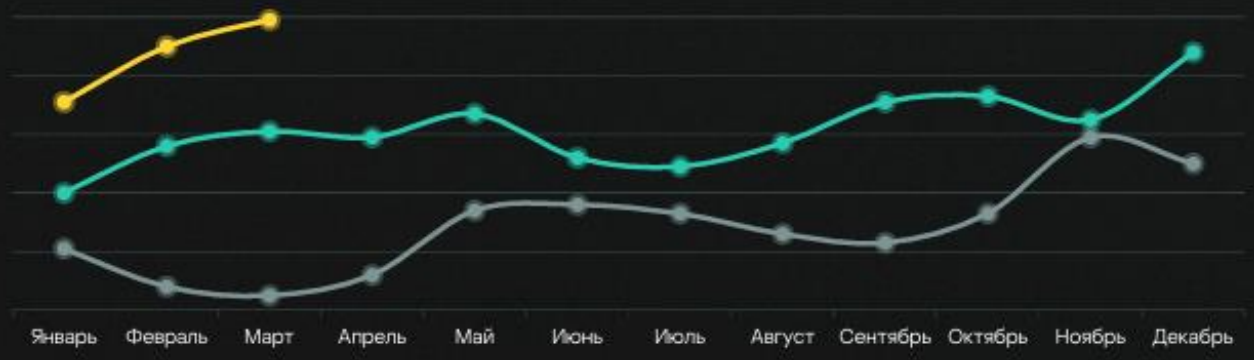
динамика количества атак с помощью программ-вымогателей (ransomware)[1]

-3% +39% рост в Q1 2026

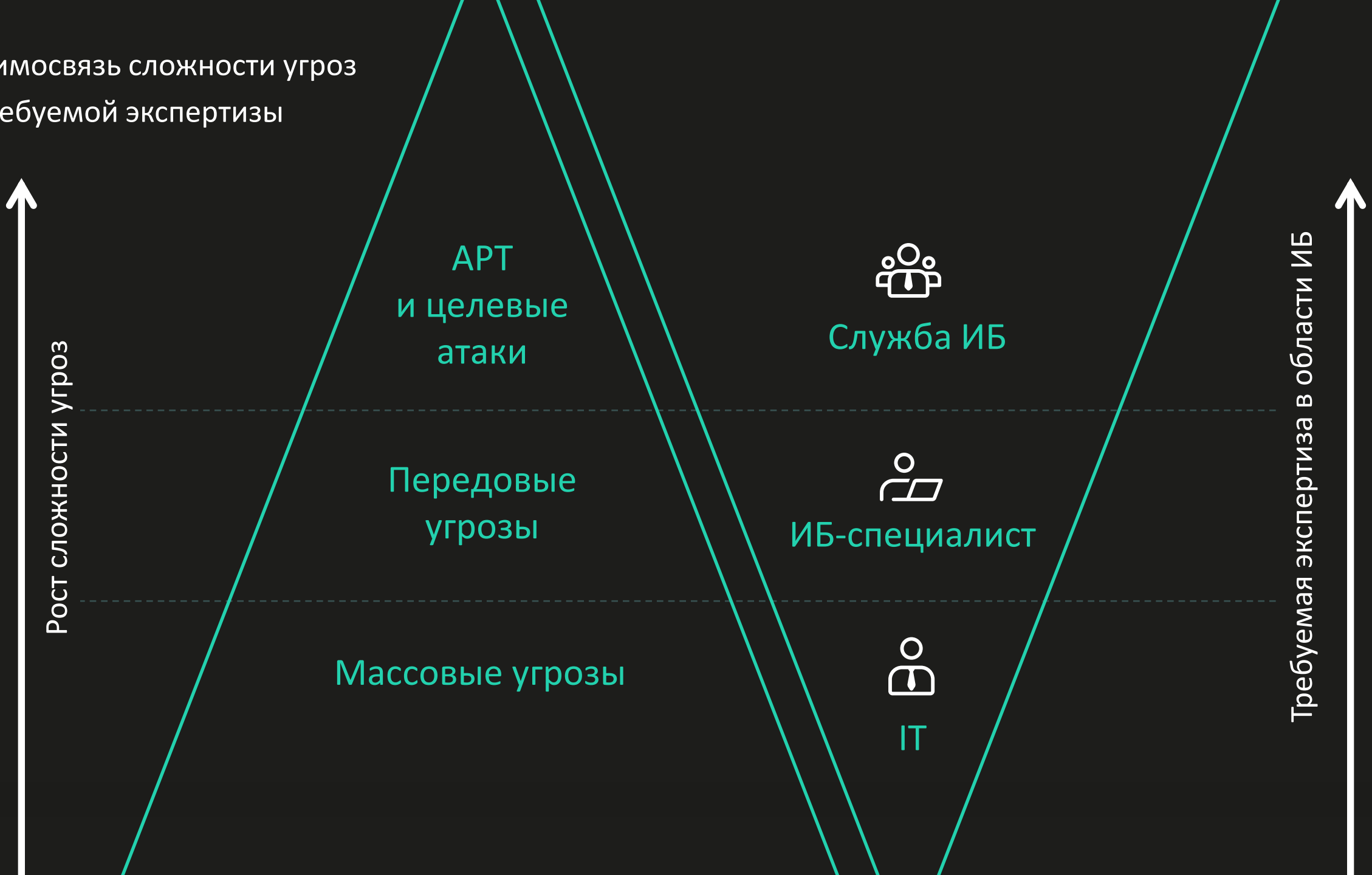
динамика количества атак с помощью эксплойтов[1]

Сезонность атак с использованием программ-вымогателей на бизнес в России[4]

Традиционные всплески атак шифровальщиков в целом совпадают с наиболее активными периодами делового сезона. Примечательно, что показатели начала 2026 уже превышают пиковые значения предыдущих лет.



Взаимосвязь сложности угроз и требуемой экспертизы



Решения «Лаборатории Касперского»

Растущая сложность угроз

3 Сложные кибертаки

2 Передовые угрозы

1 Массовые угрозы

Ресурсы

Kaspersky Expert Security
Команда ИБ или SOC

Kaspersky Optimum Security
ИБ-специалист

Kaspersky Security Foundations
IT-специалист

Требуемый инструментарий для отражения

Мощный EDR	SIEM	NTA с сетевой песочницей	Для изолированных сред
Kaspersky Endpoint Detection and Response	Kaspersky Unified Monitoring and Analysis Platform	Kaspersky Anti Targeted Attack	Kaspersky Private Security Network

Базовый EDR	Хостовая песочница	Платформа киберграмотности
Kaspersky EDR для бизнеса Оптимальный	Kaspersky Sandbox	Kaspersky Automated Security Awareness Platform

Фокусные решения

Для территориально-распределенных сетей	Защита контейнеров
Kaspersky SD-WAN	Kaspersky Container Security
Защита онлайн-ресурсов от DDoS атак	**Защита внутренних систем от угроз из файлов**
Kaspersky DDoS Protection	Kaspersky Scan Engine
Защита гражданских объектов от дронов	**Решения на базе микроядерной ОС**
Kaspersky Antidrone	KasperskyOS

Малый бизнес		Средний и крупный бизнес					
Kaspersky Endpoint Security Cloud	Kaspersky Small Office Security	Kaspersky Security для бизнеса	Kaspersky Security для виртуальных и облачных сред	Kaspersky Secure Mobility Management	Kaspersky Embedded System Security	Kaspersky Security для почтовых серверов	Kaspersky Security для интернет-шлюзов
Защита конечных устройств						Защита сети и почты	

НОВОСТИ

Kaspersky NGFW





kaspersky

Линейка KX (Kaspersky Extension)

семейство сетевых аппаратных платформ, разработанных специально для решения Kaspersky NGFW. Эти устройства обеспечивают высокую производительность, надежную защиту от киберугроз и масштабируемость для различных сценариев использования.

Внешний вид модели

KX-100

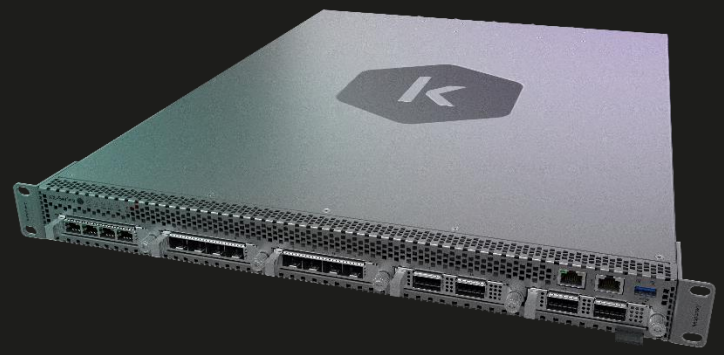


Внешний вид модели

KX-400

KX-1000

KX-3500



Аппаратные и виртуальные платформы

	KX-100	KX-400	KX-1000	KX-3500
Производительность в режиме L4 FW + Application Control**	10 Гбит/с	40 Гбит/с	100 Гбит/с	180 Гбит/с
Производительность в режиме NGFW (L4 FW + Application Control + IDPS)**	3 Гбит/с	10 Гбит/с	20 Гбит/с	50 Гбит/с
Интерфейсы	• 6 × 10/100/1000 Ethernet RJ45 • 2 × SFP+	• 4 × 10/100/1000 Ethernet RJ45 • 8 × 25G SFP28 • 4 × 100G QSFP28	• 4 × 10/100/1000 Ethernet RJ45 • 8 × 25G SFP28 • 4 × 100G QSFP28	• 4 × 10/100/1000 Ethernet RJ45 • 8 × 25G SFP28 • 4 × QSFP28

Виртуальные платформы

Подробнее о методике тестирования производительности

Подробнее о модели

vKX



Виртуальные исполнения, предназначенные для развертывания Kaspersky NGFW на собственных ресурсах заказчика без необходимости использования аппаратных платформ.

В данный момент доступно виртуальное исполнение Kaspersky NGFW vKX-8.

Параметры оборудования	vKX-8
Производительность в режиме L4 FW + Application Control*	1,5 Гбит/с
Производительность в режиме NGFW (L4 FW + Application Control + IDPS)*	800 Мбит/с
Гипервизоры	KVM или VMware ESXi
Интерфейсы	10 шт.
Формат поставки	QCOW2 + XML файл

* Тестирование проводилось с 20 000 правил Firewall и включенным логированием

Решение для управления паролями организации

Kaspersky Password Manager for Business

Технический релиз

Июль 2026

Ключевые фичи

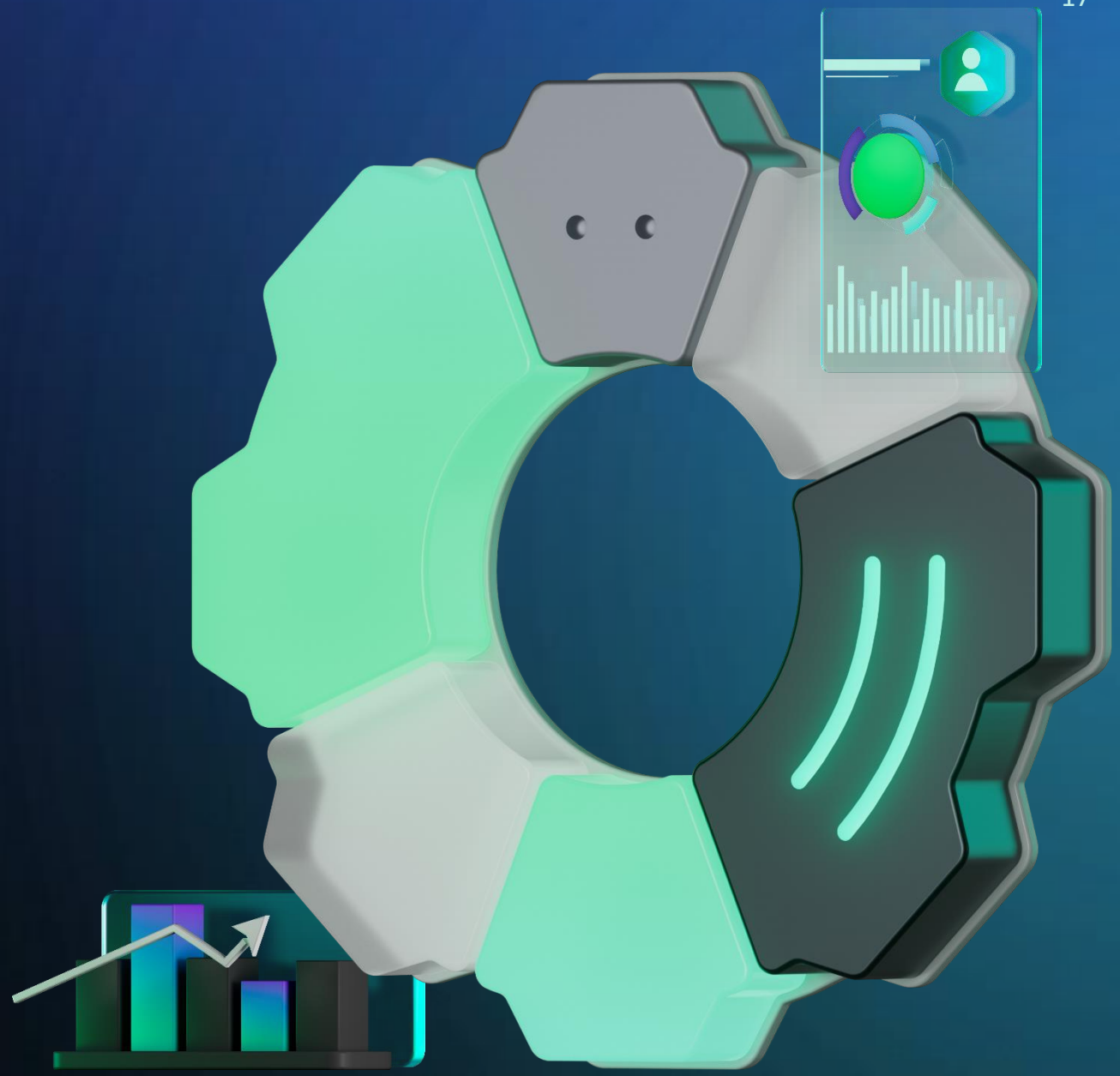
- Централизованное управление: управление лицензиями, развертывание продукта, парольные политики, управление пользователями
- Хранение паролей
- Проверка скомпрометированных паролей
- Генератор паролей
- Проверка безопасности паролей
- Поддержка одноразовых паролей (TOTP) и Passkey

Поддержка ОС

- Серверы: Windows и Linux
- Клиенты: Windows, Linux in 2027

Kaspersky Vulnerability Management

Новое решение корпоративного уровня для централизованного управления уязвимостями и мисконфигурациями



KSMS vs KSMS Plus

KSMS Plus – новая лицензия с расширенными возможностями для защиты почты. Будет доступна в конце ноября 2025.

Ключевые возможности	KSMS	KSMS Plus (NEW)
Антивирус, антиспам, антифишинг	•	•
Проверка подлинности отправителя (SPF, DKIM, DMARC, сопоставление домена отправителя)	•	•
Интеграция с песочницей KATA Sandbox, с глобальной репутационной базой Kaspersky Security Network (KSN / KPSN)	•	•
Фильтрация контента	•	•
Проверка зашифрованных архивов		•
Content disarm and reconstruction (CDR)		•
TBD в 2026 г.: Ретроспективное обнаружение угроз, защита от атак conversation hijacking (перехват диалога) и другие новые возможности продукта		•

KEDR Expert Plus

kaspersky

Новый бандл:
KL4711 Kaspersky EDR Expert Plus

Что внутри?

KES Расширенный
KEDR Expert (с Sandbox)

Тип и срок лицензии:
Base и Renewal Premium, Premium Plus
1, 2 или 3 года

От 100 устройств

Сервисы «Лаборатории Касперского»

Растущая сложность угроз

3 Сложные кибертаки

2 Передовые угрозы

1 Массовые угрозы

Ресурсы

Kaspersky Expert Security
Команда ИБ или SOC

Kaspersky Optimum Security
ИБ-специалист

Kaspersky Security Foundations
IT-специалист

Рекомендации по экспертным сервисам

Повышение экспертизы	Аналитика угроз	Анализ компрометации	Управляемая защита	Реагирование на угрозы	Анализ защищенности
Kaspersky Cybersecurity Training	Kaspersky Threat Intelligence	Kaspersky Compromise Assessment	Kaspersky MDR	Kaspersky Incident Response	Kaspersky Security Assessment

Системный подход к тренингам в сфере IT-безопасности

Обогащение данными	Оценка навыков сотрудников	Онлайн курс для IT-специалистов	Интерактивная командная игра	Управляемая защита
Kaspersky Threat Intelligence Portal (OpenTIP)	Kaspersky Gamified Assessment Tool	Kaspersky Cybersecurity for IT Online	Kaspersky Interactive Protection Simulation	Kaspersky MDR

Поддержка

- Сервисы расширенной технической поддержки (MSA)
- Kaspersky Professional Services

Формирование ИБ-процессов и построение SOC

- **Kaspersky SOC Consulting**
- **Kaspersky Tabletop Exercise**
- **Kaspersky Adversary Attack Emulation**

Комплексная защита корпоративного сегмента



Комплексная защита промышленных инфраструктур

Kaspersky Symphony

Всеобъемлющая киберзащита бизнеса
в виртуозном исполнении

Kaspersky OT CyberSecurity

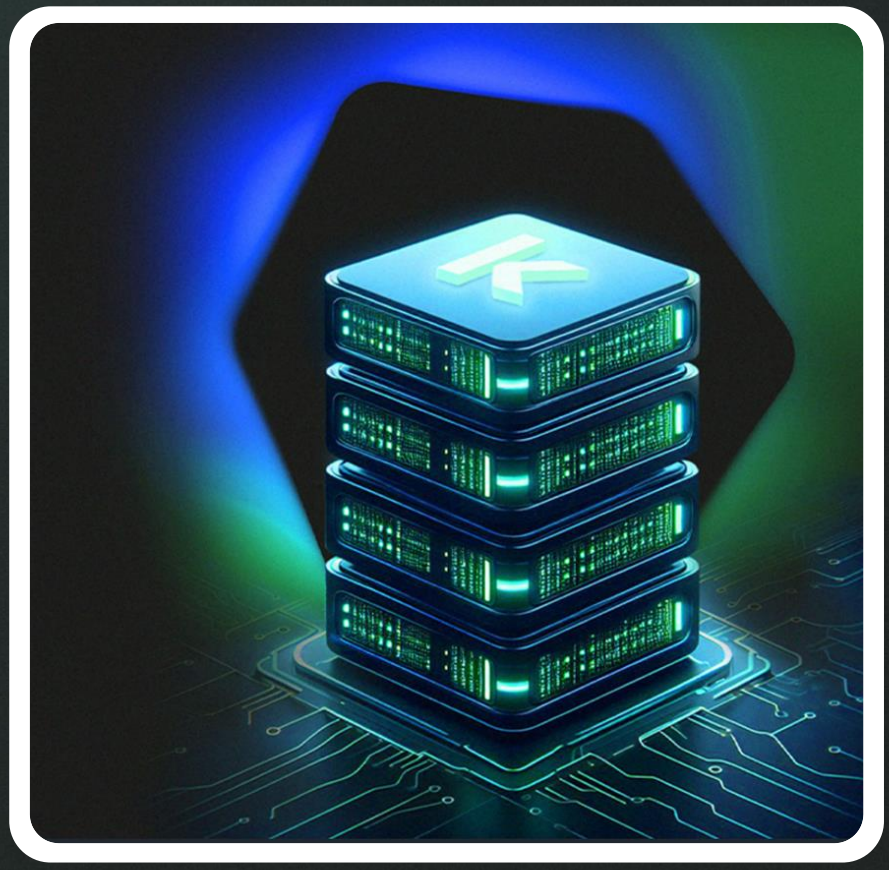
Сплав технологий и экспертизы
для промышленной кибербезопасности

Материалы



База материалов

для вашей продуктивной работы



Подробнее



Регуляторный хаб знаний в области ИБ

Это мощный инструмент, который помогает организациям разных отраслей оставаться в безопасности, учитывая последние изменения в законодательстве и регуляторной среде

regulhub.kaspersky.ru