VK Cloud

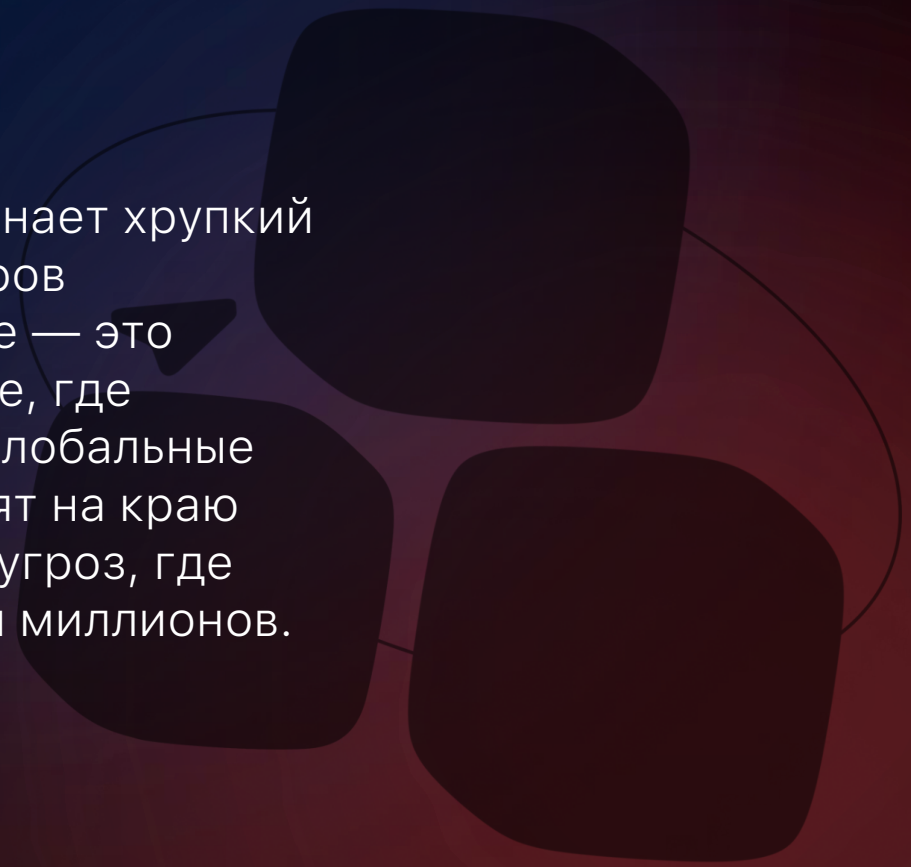
Кибербезопасность предприятия и защита инфраструктуры, информационных систем, данных и приложений от современных угроз

Станислав Погоржельский
Технологический евангелист VK Cloud

tech

Проблематика 2025 →

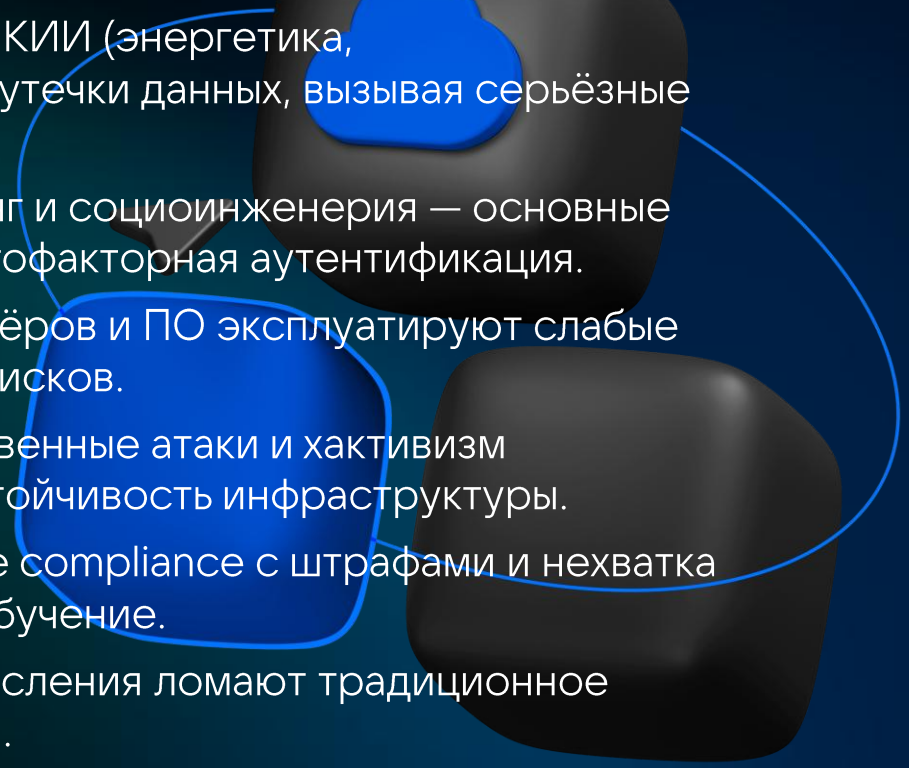
В 2025 году кибербезопасность предприятия напоминает хрупкий замок в бурю цифровой эпохи: невидимые тени хакеров проникают сквозь стены инфраструктуры, где данные — это сокровища, а приложения — уязвимые ворота. В мире, где искусственный интеллект плетет паутину обмана, а глобальные конфликты разжигают кибервойны, предприятия стоят на краю пропасти, балансируя между инновациями и хаосом угроз, где каждая ошибка может обернуться потерей доверия и миллионов.



tech

Конкретнее, пожалуйста

1. **AI-усиленные атаки и дипфейки:** Злоумышленники применяют ИИ для адаптивного malware, фишинга и дипфейков, затрудняя детекцию; нужны проактивные меры защиты.
2. **Эволюция с двойным вымогательством:** Атаки на КИИ (энергетика, здравоохранение) сочетают шифрование и угрозу утечки данных, вызывая серьёзные финансовые и операционные убытки.
3. **Утечки данных от человеческого фактора:** Фишинг и социоинженерия — основные причины; необходимо регулярное обучение и многофакторная аутентификация.
4. **Уязвимости цепочек поставок:** Атаки через партнёров и ПО эксплуатируют слабые места; требуется аудит и zero trust для снижения рисков.
5. **Геополитические угрозы и хактивизм:** Государственные атаки и хактивизм усиливаются из-за напряжений; повысить киберустойчивость инфраструктуры.
6. **Регуляторные вызовы и дефицит кадров:** Строгие compliance с штрафами и нехватка экспертов нагружают бюджеты; инвестировать в обучение.
7. **Квантовые угрозы криптографии:** Квантовые вычисления ломают традиционное шифрование; перейти на постквантовые стандарты.

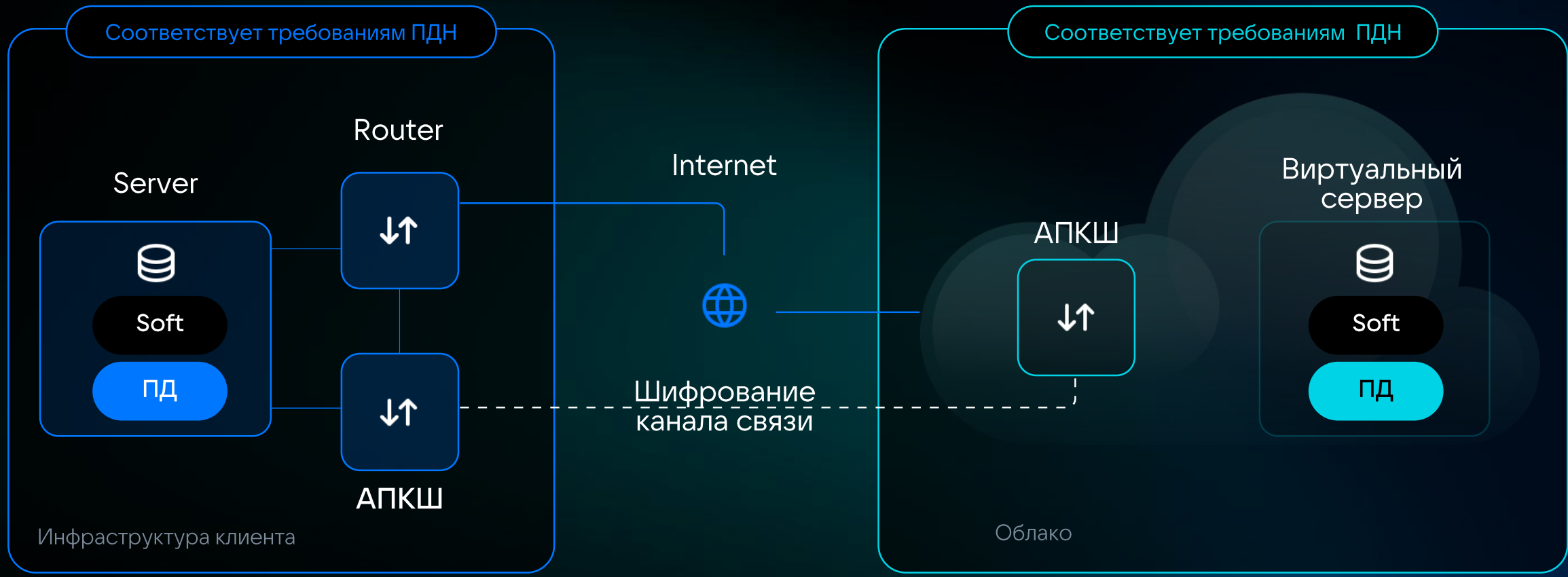


Есть решение?

В 2025 году гибридная инфраструктура выступает как надежный щит в цифровой буре, сочетая on-premise контроль с облачной гибкостью, чтобы развеять тени угроз и укрепить крепость предприятия, где данные остаются неприкосновенными, а инновации — защищенными от хаоса.

- **Повышенная устойчивость:** Распределение ресурсов минимизирует риски отказа, противостоит геоугрозам через бэкап.
- **Улучшенный контроль:** Хранение данных в приватной инфраструктуре обеспечивает доступ, упрощает compliance и снижает уязвимости цепочек.
- **Интеграция Zero Trust:** Автоматизирует детекцию AI-атак/дипфейков, фокус на проактивной защите от человеческого фактора.
- **Масштабируемость и экономия:** Elastic scaling снижает затраты ИБ и упрощает постквантовую крипто в облаке.

Передача ПДн в облачную инфраструктуру



tech

Гибридная инфраструктура

Гибридная инфраструктура сочетает локальный ЦОД с облачными ресурсами, обеспечивая географическое распределение данных и приложений, а также дополнительные уровни защиты через облачные сервисы

Преимущества

Повышенная отказоустойчивость: георепликация данных между локальным ЦОДом и облаком обеспечивает непрерывность бизнеса даже при сбоях в одном из центров обработки данных

Гибкость и масштабируемость: облачные ресурсы позволяют оперативно адаптироваться к изменяющимся нагрузкам и требованиям, обеспечивая быстрое расширение или сокращение ресурсов по мере необходимости

Дополнительная защита данных: использование облачных решений для резервного копирования и восстановления данных обеспечивает дополнительный уровень безопасности и защиты от потери информации

tech

Исследования

tech

Переход от IaaS к PaaS

В 2025 году кибербезопасность становится не только щитом, но и катализатором трансформации: угрозы, подобно шторму, вынуждают предприятия переосмыслить инфраструктуру, переходя от уязвимых IaaS к более защищённым PaaS, где безопасность встроена, а данные остаются под контролем.

- **Стимул перехода от IaaS к PaaS:** Усиление атак (AI, мисконфигурации в 99% сбоев) вынуждает отказ от сложного управления IaaS в пользу PaaS с встроенными средствами безопасности (CSPM, CNAPP) и автоматизацией.
- **Выгоды PaaS для кибербезопасности:** PaaS обеспечивает встроенную защиту (Zero Trust, шифрование), минимизирует человеческий фактор и упрощает compliance, снижая риски утечек и цепочек поставок.
- **Операционная эффективность:** PaaS автоматизирует управление инфраструктурой, сокращает затраты на ИБ и поддерживает масштабируемость, позволяя фокусироваться на защите от AI-атак и квантовых угроз.

*Исследование выполнялось компанией Apple Hills Digital с 2022 по июнь 2025 года

Apple Hills Digital 2025

Отрасль	Рост затрат на ИТ в 2025 г.	Рост затрат на ИТ в 2026-2028 гг.
Банки и финансы	🟢	🟡
Госбюджет	🟢	🟡
Телеком, медиа, ИТ	🟢	🟢
Ритейл	🟢	🟢
Энергетика и ресурсы	🟡	🟡
Обрабатывающая промышленность	🟡	🔴
Транспорт	🟡	🟡
Строительство и недвижимость	🔴	🔴

Обозначения:

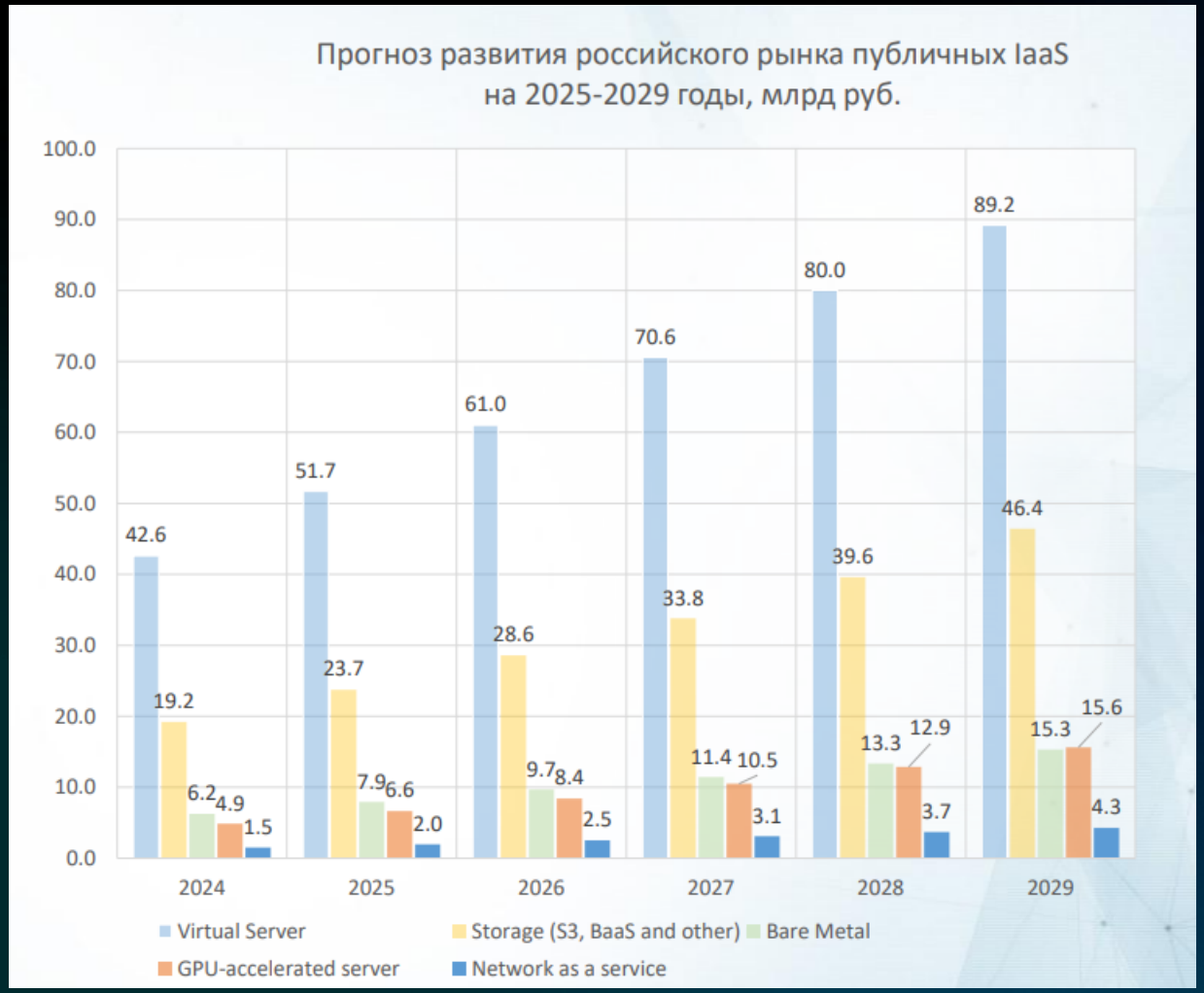
- 🟢 - *темп роста затрат на ИТ выше среднего*
- 🟡 - *средний темп роста затрат на ИТ*
- 🔴 - *низкий темп роста / сокращение затрат на ИТ*

VK tech

*Исследование выполнялось компанией Apple Hills Digital с 2022 по июнь 2025 года. Компании РФ

Apple Hills Digital 2025

Сегмент публичных IaaS-сервисов: прогноз на 2025-2029 годы

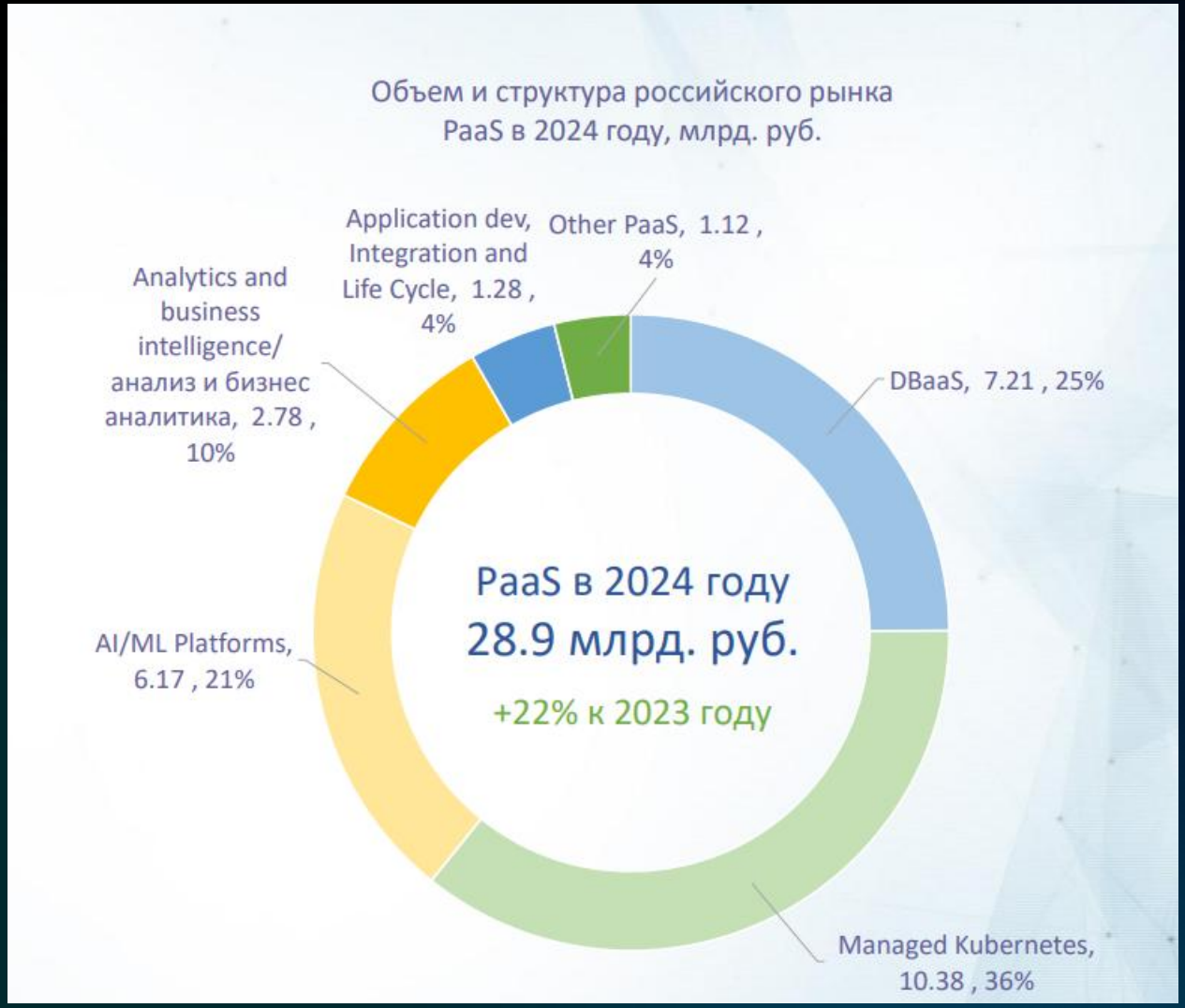


tech

*Исследование выполнялось компанией Apple Hills Digital с 2022 по июнь 2025 года. Компании РФ

Apple Hills Digital 2025

Сегмент публичных PaaS-сервисов: объем и структура в 2024 году

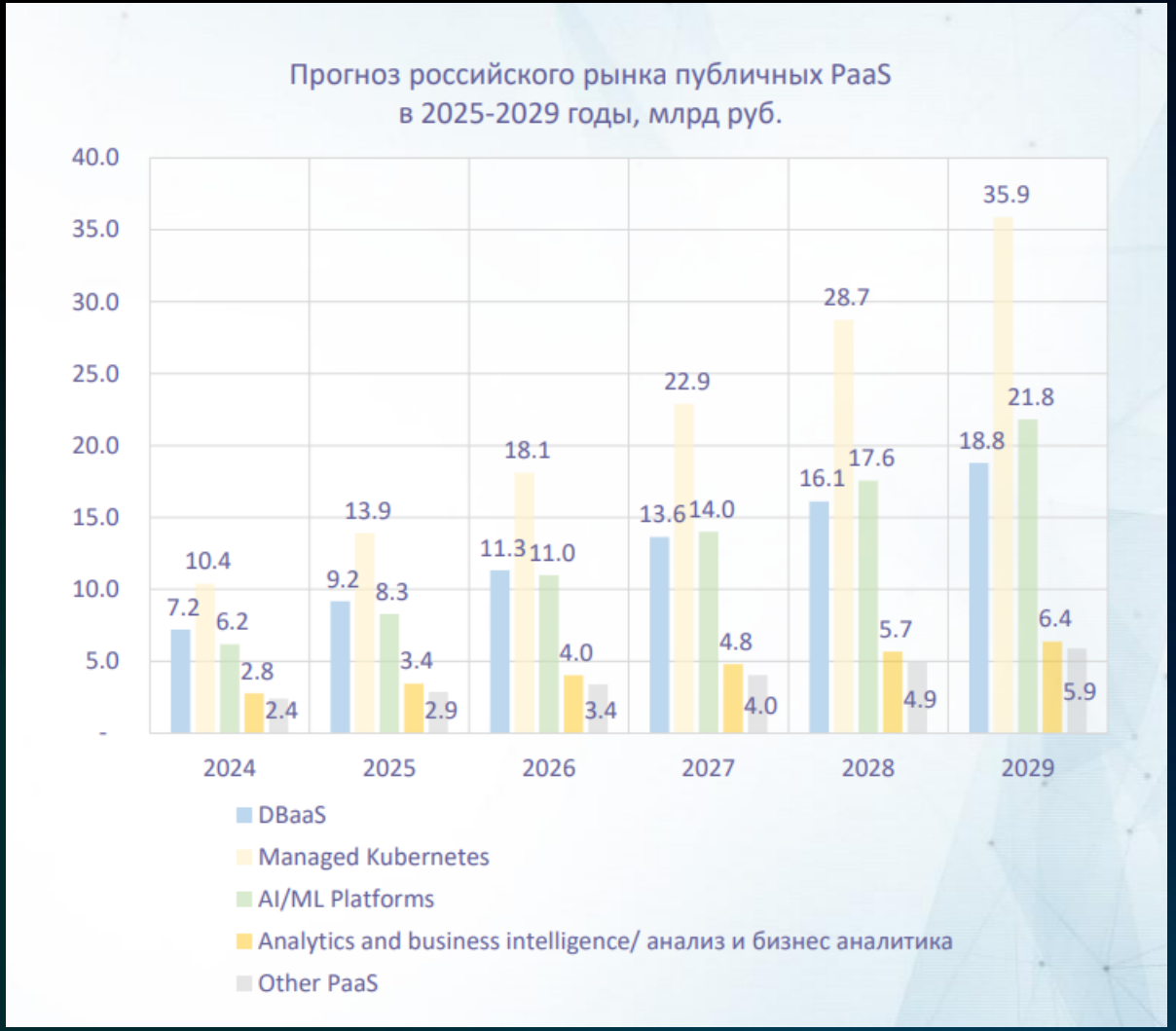


tech

*Исследование выполнялось компанией Apple Hills Digital с 2022 по июнь 2025 года. Компании РФ

Apple Hills Digital 2025

Сегмент публичных PaaS-сервисов: прогноз на 2025-2029 годы



tech

*Исследование выполнялось компанией Apple Hills Digital с 2022 по июнь 2025 года. Компании РФ

Исследования

Генеративный ИИ

Генеративный ИИ меняет фокус программ защиты данных с структурированных на неструктурированные данные, такие как текст, изображения и видео.

Рост инвестиций в защиту неструктурированных данных влияет на обучение больших языковых моделей (LLM), развертывание данных и процессы вывода.

Пример: Компания вроде Target обнаруживает утечку конфиденциальных видеоматериалов из корпоративной системы, что требует усиления ИИ-защиты неструктурированных данных для предотвращения репутационных потерь.

Управление машинными идентичностями

Увеличение машинных учетных записей от GenAI, облачных сервисов и автоматизации расширяет поверхность атаки, требуя координации IAM.

Команды IAM управляют только 44% машинных идентичностей в организации (опрос Gartner среди 335 лидеров, 2024).

Пример: В атаке на SolarWinds хакеры эксплуатировали неуправляемые машинные учетные записи для доступа к правительственным системам США, что привело к глобальному скандалу и миллиардным убыткам.

Исследования

Тактический ИИ и оптимизация технологий

Лидеры фокусируются на узких, измеримых применениях ИИ, интегрируя их в существующие инициативы для повышения эффективности кибербезопасности.

Тактические внедрения ИИ минимизируют риски и демонстрируют ценность инвестиций через интеграцию с существующими метриками.

Пример: Банк JPMorgan Chase применяет ИИ для анализа фишинговых email в реальном времени, что снижает успешность атак на 30% и интегрируется с их системой мониторинга угроз

Организации используют в среднем 45 инструментов ИБ, что требует консолидации и валидации для повышения эффективности программ безопасности.

Свыше 3000 вендоров; фокус на переносимости данных и моделировании угроз для баланса нужд и затрат.

Пример: После нарушения данных в Equifax компания сократила инструменты с 50 до 30, объединив их в единую платформу, что снизило время реагирования на угрозы и операционные расходы на 20%.

Безопасность поведения и борьба с выгоранием

Расширение ценности программ безопасности поведения и культуры

Программы SBCP становятся критическими с интеграцией GenAI для снижения инцидентов от сотрудников и повышения осведомленности.

С GenAI и интегрированной архитектурой организации сократят инциденты от сотрудников на 40% к 2026 году.

Пример: Microsoft внедряет ИИ-тренинги для симуляции фишинга среди сотрудников, что уменьшило утечки данных на 25% после инцидентов вроде SolarWinds

Выгорание лидеров и команд от нехватки навыков и эволюционирующих угроз требует инвестиций в личную устойчивость.

Эффективные лидеры фокусируются на управлении стрессом для повышения эффективности программ ИБ.

Пример: В Maersk после кибератаки NotPetya команда ввела программы ментального здоровья, что снизило текучесть кадров на 15% и улучшило реакцию на будущие угрозы.

Рост атак без вредоносного ПО

В 2025 году доминируют атаки, не использующие malware, фокусируясь на социальной инженерии и краже идентичностей.

79% обнаружений в 2024 году были malware-free, с ростом vishing-атак на 442% во второй половине года.

Пример: Группа CHATTY SPIDER использовала социальную инженерию для быстрого доступа к системам, обходя традиционные антивирусы, что привело к утечкам в финансовом секторе

Ускорение времени прорыва киберпреступников

Киберпреступники сокращают время от обнаружения до атаки, используя автоматизацию для быстрого проникновения.

Рекордное время прорыва — 51 секунда, среднее — 48 минут в 2024 году.

Пример: Организованные группы вроде LIMINAL PANDA применяли автоматизированные инструменты для шпионажа, быстро компрометируя правительственные сети в Азии

CrowdStrike 2025 Global Threat Report

Примеры

1. В 2024 году группа JACKPOT PANDA атаковала финансовую компанию в Европе, украв $10 млн через компрометацию облачной платформы. Инструменты: Использовали украденные учетные данные и автоматизированные скрипты для эксплуатации API. Вывод: Необходимы усиленные меры защиты API и мониторинг учетных записей.
2. Группа CRIMSON SQUID скомпрометировала медицинскую сеть, зашифровав данные пациентов и потребовав выкуп. Инструменты: Тактики ransomware с двойным вымогательством и фишинговые email с ИИ-генерируемым контентом. Вывод: Требуется интеграция ИИ-детекции для борьбы с продвинутым фишингом и бэкапы для восстановления.
3. Неизвестный атаковал производственную фирму, используя уязвимости в цепочке поставок ПО. Инструменты: Троянизированные обновления легитимного софта для внедрения бэкдоров. Вывод: Аудит цепочек поставок и внедрение Zero Trust минимизируют риски стороннего ПО.
4. В 2024 году хакеры провели атаку на транспортную инфраструктуру, используя cloud-native уязвимости. Инструменты: Эксплуатация неправильно настроенных S3-бакетов для кражи данных. Вывод: CSPM-инструменты и регулярные проверки конфигураций облаков критически важны.
5. Группа SHADOW ORACLE атаковала энергетическую компанию, используя автоматизированные инструменты для быстрого латерального движения. Инструменты: Боты для сканирования сети и эксплуатации слабых паролей. Вывод: Регулярное обновление паролей и EDR-решения помогут замедлить такие атаки.

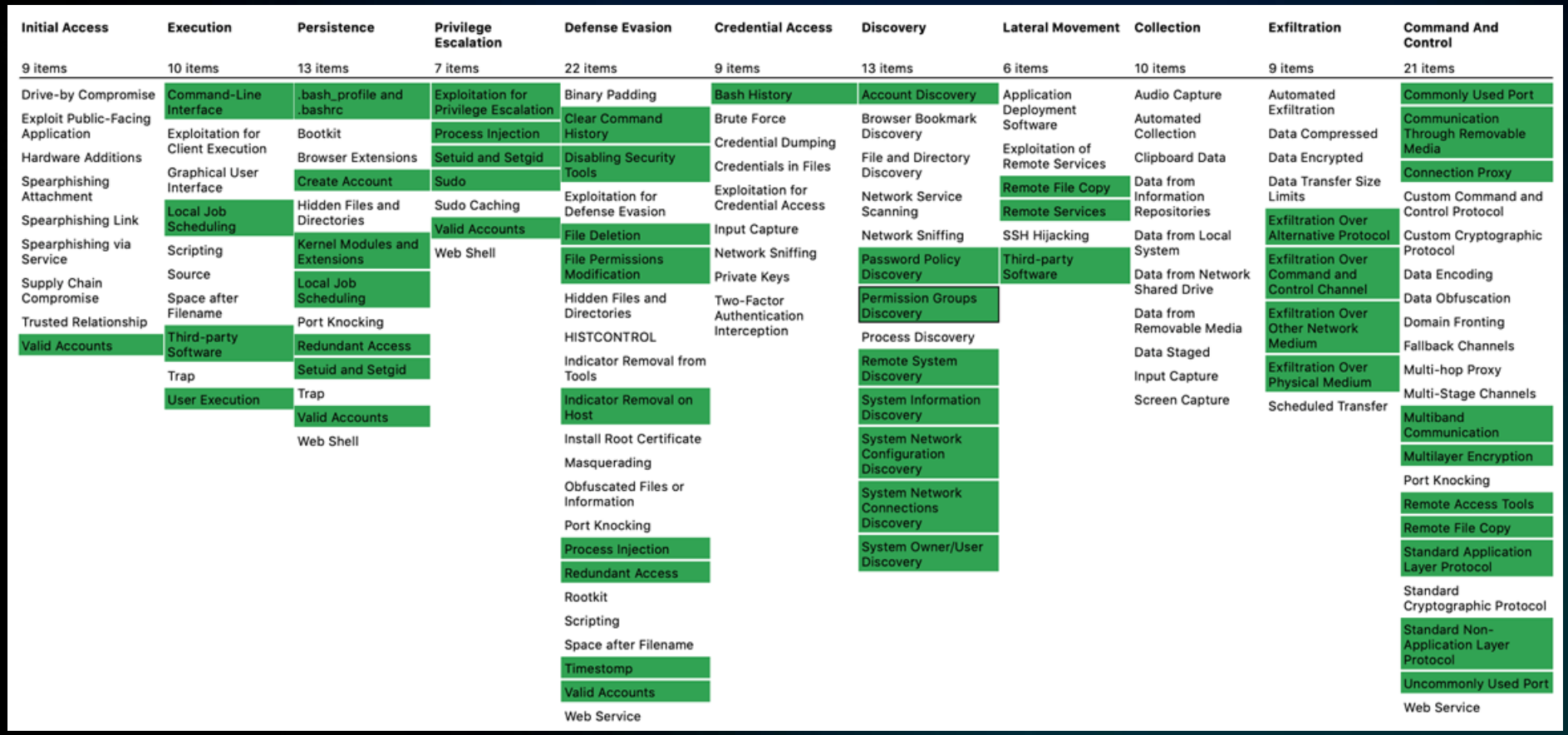
Примеры

1. Организация в здравоохранении столкнулась с дефицитом киберспециалистов, что привело к задержкам в реагировании на фишинговые атаки. Инструменты: Автоматизация задач с помощью AI для анализа угроз и базовые инструменты обучения персонала. Вывод: Инвестиции в развитие навыков и AI помогут закрыть пробелы в талантах и повысить эффективность защиты от человеческих ошибок.
2. Компания в финансовом секторе ввела AI для оптимизации процессов, но столкнулась с рисками утечек данных из-за недостаточного обучения. Инструменты: Интеграция AI в мониторинг, но без адекватных политик доверия и этических рамок. Вывод: Необходим баланс между скоростью внедрения AI и механизмами доверия для минимизации новых рисков и обеспечения безопасного использования.
3. Глобальная корпорация консолидировала свои инструменты ИБ на одной платформе, что упростило управление, но увеличило уязвимости от единой точки отказа. Инструменты: Платформенные решения для унификации, такие как облачные сервисы с встроенной безопасностью. Вывод: Консолидация требует тщательной оценки рисков и диверсификации для снижения зависимости и повышения устойчивости.
4. Предприятие в энергетике внедрило цифровые идентичности, но столкнулось с проблемами от deepfake-атак на аутентификацию. Инструменты: Биометрические системы и многофакторная аутентификация, уязвимые к подделкам. Вывод: Улучшение интероперабельности и регуляторного соответствия поможет противостоять deepfake-рискам и укрепить доверие к цифровым идентичностям.
5. Бизнес в производстве развил культуру устойчивости, интегрируя безопасность во все процессы после инцидента с умными устройствами. Инструменты: Регуляторные фреймворки для IoT и корпоративные политики "resilience by design". Вывод: Холистический подход к культуре безопасности обеспечит защиту от эволюционирующих угроз и повысит общую устойчивость организации

Тренд на:
Сервисы защиты по подписке

tech

MITRE ATT&CK



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
9 items	10 items	13 items	7 items	22 items	9 items	13 items	6 items	10 items	9 items	21 items
Drive-by Compromise	Command-Line Interface	.bash_profile and .bashrc	Exploitation for Privilege Escalation	Binary Padding	Bash History	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Exploitation for Client Execution	Bootkit	Process Injection	Clear Command History	Brute Force	Browser Bookmark Discovery	Exploitation of Remote Services	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Graphical User Interface	Browser Extensions	Setuid and Setgid	Disabling Security Tools	Credential Dumping	File and Directory Discovery	Remote File Copy	Clipboard Data	Data Encrypted	Connection Proxy
Spearphishing Attachment	Local Job Scheduling	Create Account	Sudo	Exploitation for Defense Evasion	Credentials in Files	Network Service Scanning	Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Link	Scripting	Hidden Files and Directories	Sudo Caching	File Deletion	Exploitation for Credential Access	Network Sniffing	SSH Hijacking	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing via Service	Source	Kernel Modules and Extensions	Valid Accounts	File Permissions Modification	Input Capture	Password Policy Discovery	Third-party Software	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Supply Chain Compromise	Space after Filename	Local Job Scheduling	Web Shell	Hidden Files and Directories	Network Sniffing	Permission Groups Discovery		Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Trusted Relationship	Third-party Software	Port Knocking		HISTCONTROL	Private Keys	Process Discovery		Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Valid Accounts	Trap	Redundant Access		Indicator Removal from Tools	Two-Factor Authentication Interception	Remote System Discovery		Input Capture	Scheduled Transfer	Fallback Channels
	User Execution	Setuid and Setgid		Indicator Removal on Host		System Information Discovery		Screen Capture		Multi-hop Proxy
		Trap		Install Root Certificate		System Network Configuration Discovery				Multi-Stage Channels
		Valid Accounts		Masquerading		System Network Connections Discovery				Multiband Communication
		Web Shell		Obfuscated Files or Information		System Owner/User Discovery				Multilayer Encryption
				Port Knocking						Port Knocking
				Process Injection						Remote Access Tools
				Redundant Access						Remote File Copy
				Rootkit						Standard Application Layer Protocol
				Scripting						Standard Cryptographic Protocol
				Space after Filename						Standard Non-Application Layer Protocol
				Timestomp						Uncommonly Used Port
				Valid Accounts						Web Service
				Web Service						

VK Cloud

Вектора атак

Категория угроз/сценариев	Пассивная защита	Активная защита
DDoS-атаки	Гео- и IP-фильтрация, rate limiting	Анти-DDoS (scrubbing, mitigation на сетевом/транспортном уровне)
Веб-приложения	Статическая сигнатурная фильтрация	WAF с поведенческим анализом и автообновлением правил
Подозрительный трафик	Логи/алерты без реакции в реальном времени	NGFW с DPI и динамическим блокированием
Атаки нулевого дня	Ограничение экспонирования сервисов	IPS/IDS, NGFW с ML/AI детекцией аномалий
Неавторизованный доступ	ACL, сегментация сети	Интеграция NGFW с IAM, адаптивный контроль доступа
Сканирование и разведка (recon)	Скрывательство портов, фейковые ответы	Honeypots, активное реагирование и блокировка
Управление доступом и маршрутизацией	Встроенный облачный фаервол: SNAT/DNAT, открытие портов, статика	Динамическая настройка политик через API, автоприменение по контексту угроз
Правовое соответствие (РФ)	Облако с аттестацией по 152-ФЗ, К1, выполнение требований ФСТЭК и аттестованного гипервизора	Использование СКЗИ, сертифицированных ФСТЭК, настройка/управление на стороне клиента

Комплексная защита. Тренд на наличие SIEM

VK Cloud

Почему важна комплексная защита от атак и взломов?

Последствия для бизнеса могут измеряться значительным ущербом в виде потери позиций на рынке, прибыли и репутации

Финансовые потери:

↗ Gartner

Простой онлайн-сервиса на 1 час обходится компаниям в среднем в $300 000

Репутационный ущерб:

↗ Ponemon Institute

72% клиентов теряют доверие к компаниям после киберинцидентов

Потеря рыночных позиций:

Forbes ↗

В 2023 году 34% компаний малого бизнеса, подвергшихся DDoS-атакам, прекратили работу в течение года

VK Cloud

DDoS – главная угроза кибербезопасности

Немного статистики

Количество DDoS-атак в 2024 году в России увеличилось на 45%, а в сегменте L3/L4-атак — на 53% по сравнению с 2023 годом

Многовекторные атаки выросли на 118% в 2024 году

Средняя продолжительность DDoS-атак в 2024 году достигла 23 минут. Рекордные инциденты длились до 19 дней

Инструменты для организации DDoS-атак доступны в даркнете. Для некоторых из них есть тарифные планы с гарантией обхода конкретных систем защиты

VK Cloud

WAF | Облачный сервис защиты от атак и уязвимостей в веб-приложениях*

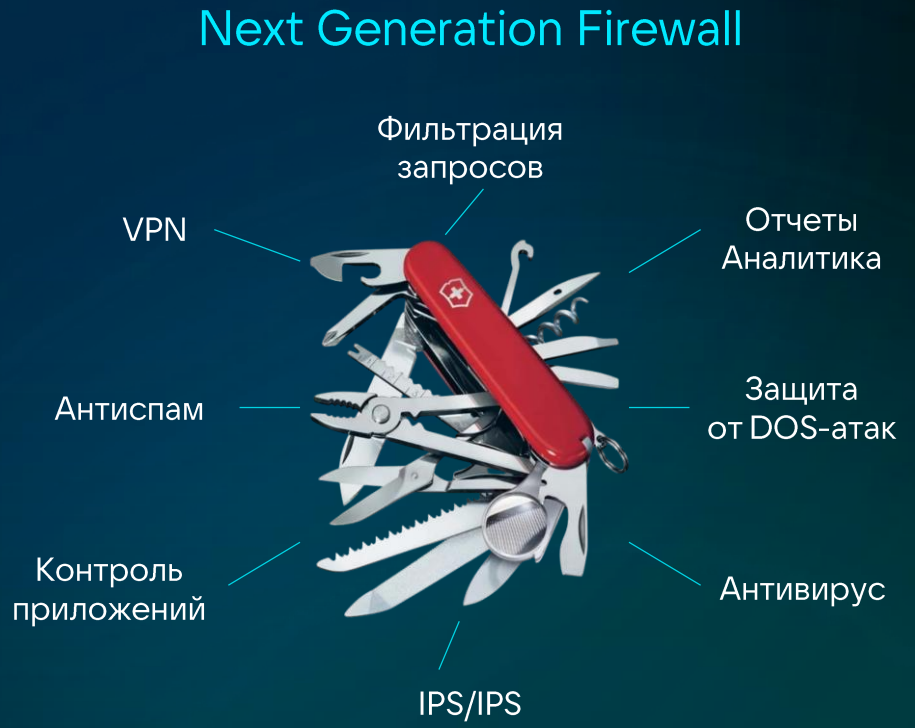
Сценарии применения

- Защита от атак OWASP Top-10
- Предотвращение логических атак
- Защита от ботов и переборных атак
- Блокировка атак на 0-day и 1-day уязвимости
- Предотвращение мошенничества
- Защита API и мобильных приложений
- Защита внутренних систем и UBA
- Защита от DoS и DDoS – атак

VK Cloud

Функции NGFW:

- Межсетевое экранирование
- Обнаружение и предотвращение атак (в т.ч. атаки на веб-приложения)
- Антиспам
- Потоковый антивирус
- Контроль приложений
- Фильтрация интернет-запросов пользователей
- VPN
- Анализ событий/формирование отчетов



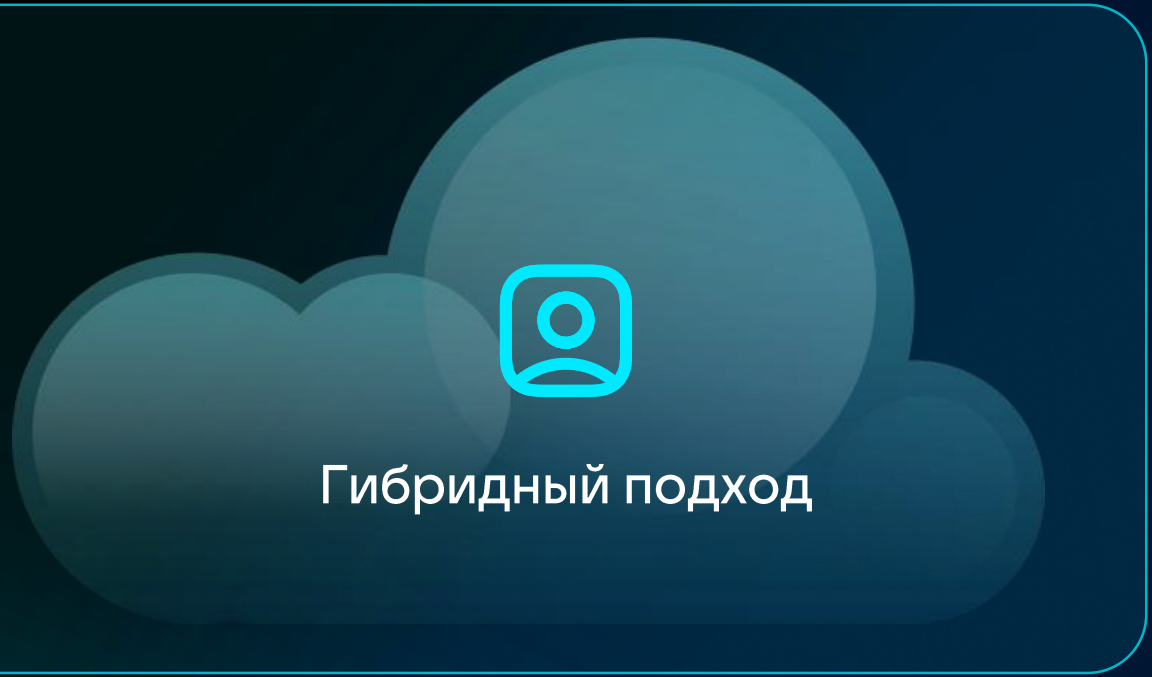
VK Cloud

Выводы

Для каждого КиберРиска – применяется свой инструмент.

НО!

1. Не забываем про требования регуляторов!
2. Как минимум: хранение ПДН на территории страны!
3. Много инструментов утомляет



1. Утечка из-за слабых навыков ИБ.
2. Утечка при внедрении AI.
3. Deepfake-атаки скомпрометировали идентичности.
4. Атака на IoT-устройства.
5. Консолидация создала точку отказа.

VK Cloud

Станислав Погоржельский
Технологический евангелист VK Cloud

Спасибо за внимание

tech