Yandex Cloud × ДРТ

ДЕЛОВЫЕ РЕШЕНИЯ И ТЕХНОЛОГИИ
BUSINESS SOLUTIONS AND TECHNOLOGIES

Как и какие средства защиты CISO использовали в 2023 году

Миссия исследования

В 2023 году бюджеты на информационную безопасность в российских компаниях выросли в несколько раз

Нам, как облачному партнёру, важно отслеживать,
как именно меняются запросы бизнеса на средства защиты,
как воспринимают провайдеров на рынке и какова их роль
в построении безопасных информационных систем

Этап 1
Качественное исследование

Метод:
глубинные интервью

Количество интервью:
26 респондентов из 17 компаний*

Структура выборки:
по ролям

* Отрасли: банки и страховые компании, retail и e-commerce, крупная добывающая или перерабатывающая промышленность, крупные производственные предприятия

Этап 2
Количественное исследование

Метод:
количественный опрос

Выборка:
302 респондента

Структура выборки:
по ролям

Профиль аудитории качественного исследования

Отрасли	IT-специалист	ИБ-специалист	Бизнес-роли
Банки и страхование	8%	15%	4%
Retail и e-commerce	8%	12%	15%
Промышленность	12%	15%	12%

IT-специалисты	27%
ИБ-специалисты	42%
Бизнес-роли	31%

Банки и страхование	27%
Retail и e-commerce	35%
Промышленность	38%

Общее количество интервью — 26

Профиль аудитории количественного исследования

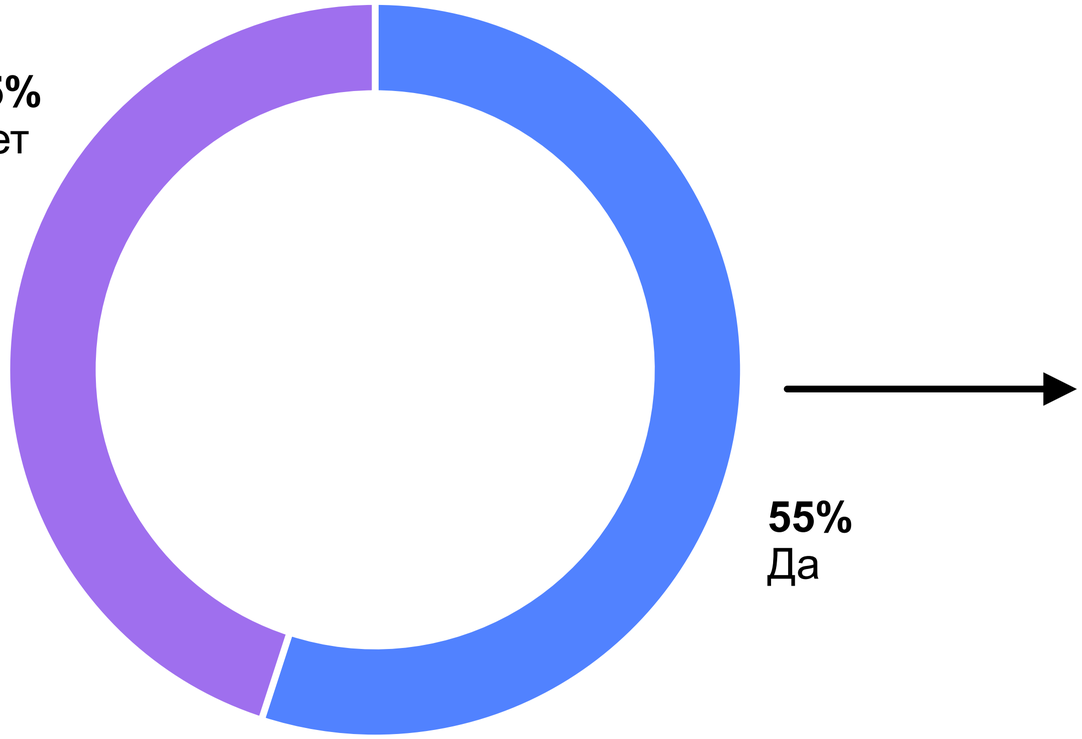
IT-специалисты	39%
ИБ-специалисты	31%
Бизнес-роли	30%
Средний бизнес	60%
Крупный бизнес	40%
Руководители	61%
Пользователи	39%

Общее количество респондентов (n) — 302

1. Методология исследования
2. Особенности распределения бюджета на информационную безопасность (ИБ)
3. Актуальные средства защиты
4. Популярность технологий искусственного интеллекта (ИИ)
5. Восприятие облачных провайдеров
6. Анализ рисков и препятствия при миграции в облако
7. Преимущества использования облачных платформ для информационной безопасности (ИБ)
8. Ключевые выводы исследования

Средняя доля расходов на информационную безопасность составляет 15% от общего бюджета компании на IT

Знакомы с распределением бюджета
на информационную безопасность в компании



47%

сотрудников отмечают, что стратегия развития информационной безопасности в компании обновляется примерно раз в год

38%

респондентов затруднились с ответом на данный вопрос

Общая выборка (n) — 302 респондента

Примерно каждая четвёртая компания отмечает рост затрат на проекты информационной безопасности по сравнению с прошлым годом.
В среднем объём бюджета увеличился на 20%

В основном бюджеты на ИБ распределяются на обновление ПО, лицензий (75%) и оборудования (73%). Одна из значимых статей расходов — дополнительное обучение сотрудников

В крупной промышленности и финансах бюджет выделяют на импортозамещение и совершенствование используемых технологий, в том числе на приобретение облачных сервисов

В ритейле выросло число вакансий ИБ-специалистов, увеличились и бюджеты. Компании тестируют защищённость систем, проводя тесты на проникновение, дополнительные расходы идут на внутреннее обучение

1. Методология исследования
2. Особенности распределения бюджета на информационную безопасность (ИБ)
3. Актуальные средства защиты
4. Популярность технологий искусственного интеллекта (ИИ)
5. Восприятие облачных провайдеров
6. Анализ рисков и препятствия при миграции в облако
7. Преимущества использования облачных платформ для информационной безопасности (ИБ)
8. Ключевые выводы исследования

Компании отмечают, что одно из ключевых направлений повышения безопасности при работе с данными в облаке — это постоянное совершенствование систем и разработка новых стандартов безопасности

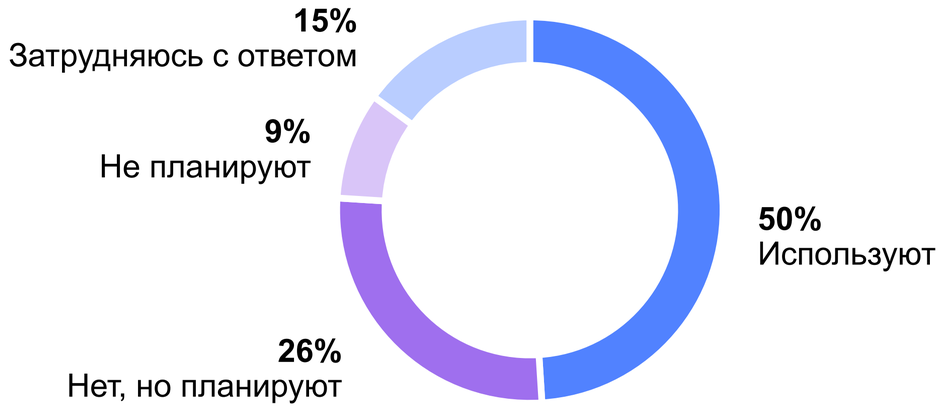
Бюджет на информационную безопасность, в частности, содержит следующие расходы

- Внедрение SOC
- Fraud-мониторинг в кластерах и анализ аномалий поведения
- Архитектурные балансировщики, DSS
- VPN
- Технологии ИИ
- Сервисы защиты от DDoS-атак

1. Методология исследования
2. Особенности распределения бюджета на информационную безопасность (ИБ)
3. Актуальные средства защиты
4. Популярность технологий искусственного интеллекта (ИИ)
5. Восприятие облачных провайдеров
6. Анализ рисков и препятствия при миграции в облако
7. Преимущества использования облачных платформ для информационной безопасности (ИБ)
8. Ключевые выводы исследования

Ландшафт киберугроз продолжает расширяться и становится более сложным. Для эффективного отслеживания и противодействия уже недостаточно обычного мониторинга security-специалистами, поэтому на рынке наблюдается тенденция к внедрению автоматизированных алгоритмов, ИИ в системы комплексной защиты

Используют ли в компании ИИ или средства автоматизации для решения задач, связанных с информационной безопасностью



Какие технологии ИИ или автоматизации используются в компании для решения задач, связанных с информационной безопасностью?

SIEM	85%
Application security	71%
EDR	70%
UEBA	70%
TIP	68%
NDR	66%
Antifraud	66%
SOAR	60%

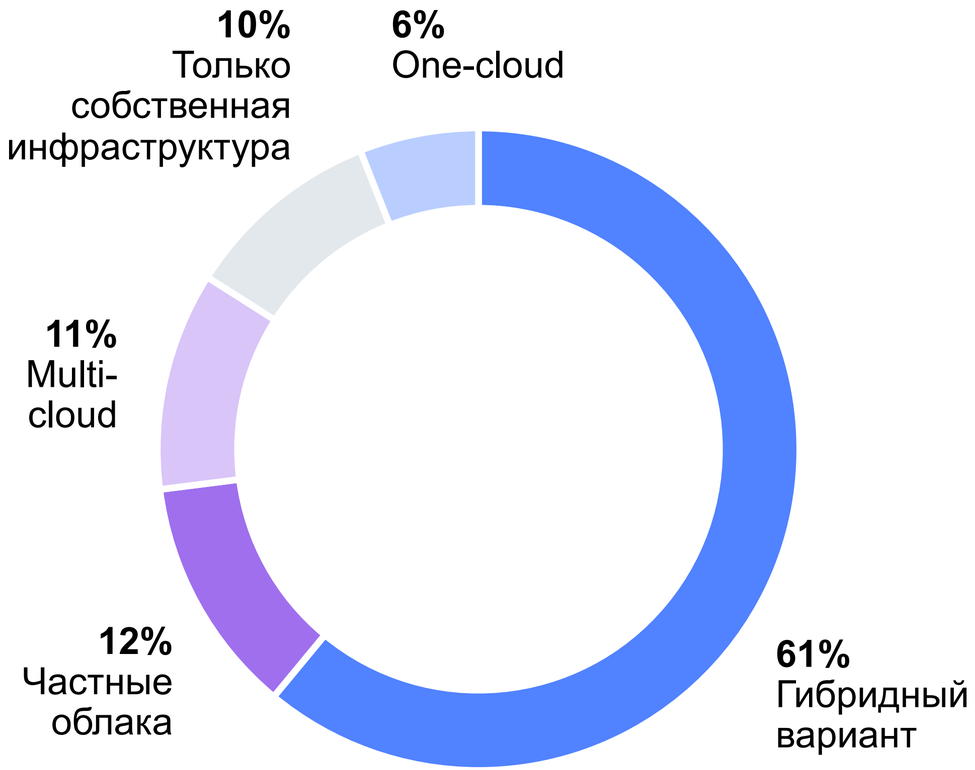
Около половины компаний использует ИИ для решения задач, связанных с информационной безопасностью. Лишь каждая десятая компания не планирует внедрять технологии ИИ для этих целей

Использование ИИ и автоматизации наиболее распространено в финансовом секторе (применяют 71% компаний), наименее — в ритейле (применяют 14% компаний). Финансовый сектор и проф. сервисы чаще заявляют об использовании NDR, SOAR и Antifraud, особенно по сравнению с промышленными компаниями

1. Методология исследования
2. Особенности распределения бюджета на информационную безопасность (ИБ)
3. Актуальные средства защиты
4. Популярность технологий искусственного интеллекта (ИИ)
5. Восприятие облачных провайдеров
6. Анализ рисков и препятствия при миграции в облако
7. Преимущества использования облачных платформ для информационной безопасности (ИБ)
8. Ключевые выводы исследования

Большинство компаний уже оценили преимущества использования облачных сервисов и платформ. При этом наблюдается стремление разделить задачи на требующие локального контроля и решаемые с помощью гибких онлайн-сервисов

Какой тип облачных платформ использует ваша компания в настоящий момент?



61%

опрошенных компаний используют гибридный формат — внутренние IT-ресурсы компании, объединённые с инфраструктурой и услугами, размещёнными в облаке

«

Дело в том, что у нас нет цели содержать ЦОДы. У нас цель предоставлять качественный сервис покупателям магазина, а не заниматься железками и чем-то ещё

Дмитрий Кузеванов,
CISO, руководитель Центра мониторинга и реагирования (MRC) UserGate (экс-CISO и CTO «Азбуки вкуса»)

Основные критерии оценки провайдера: наличие сертификации, разнообразие сервисов (в том числе security) и техническая поддержка со стороны провайдера. Компании воспринимают облачные платформы как инструмент для автоматизации работы со средствами информационной безопасности

В департаментах ИБ акцентируют внимание на российском размещении дата-центров, возможности интеграции систем мониторинга или использовании систем мониторинга провайдера

IT-специалисты отмечают важность экспертизы в продукте на стороне провайдера для поддержания процесса интеграции или переноса

Бизнес-роли рассматривают провайдера с точки зрения стабильности компании на рынке, а также условий контрактации и ответственности. Некоторые крупные заказчики отметили важность фиксированной цены

Технологичность, способность выдерживать большие нагрузки и обеспечение безопасной работы (за счёт внутренних сервисов и безопасной разработки) — ключевые факторы оценки облачного провайдера

К 2023 году большинство провайдеров добились соответствия требованиям законодательства. На первое место, помимо вопросов безопасности и стабильности платформ, выходят вопросы предоставления разнообразных сервисов и технологий для эффективной реализации поставленных задач

Другими словами, компании стремятся опираться на технологии, предоставляемые самими провайдерами, поскольку они эффективно поддерживаются

На что обращают внимание при выборе облачного провайдера?	
Отказоустойчивая платформа, обеспечивающая сохранность данных	98%
Платформа с безопасной внутренней разработкой	97%
Платформа предоставляет необходимый стек технологий	96%
Достаточный набор сервисов для информационной безопасности	96%
Стабильный провайдер, работа которого не зависит от внешних факторов	96%
Высокая скорость и качество технической поддержки	94%
Платформа проста и удобна в использовании	94%
Соответствует законодательным требованиям	93%
Понятное ценообразование	84%
Бренд, которому я доверяю	83%

1. Методология исследования
2. Особенности распределения бюджета на информационную безопасность (ИБ)
3. Актуальные средства защиты
4. Популярность технологий искусственного интеллекта (ИИ)
5. Восприятие облачных провайдеров
6. Анализ рисков и препятствия при миграции в облако
7. Преимущества использования облачных платформ для информационной безопасности (ИБ)
8. Ключевые выводы исследования

Общим трендом является нехватка во многих компаниях ИБ-специалистов, обладающих специфическими знаниями в технологиях. Как следствие, в компаниях отмечается значительное количество нарушений регламентов в области обновлений аппаратных и программных средств, а также несвоевременное противодействие возникающим уязвимостям

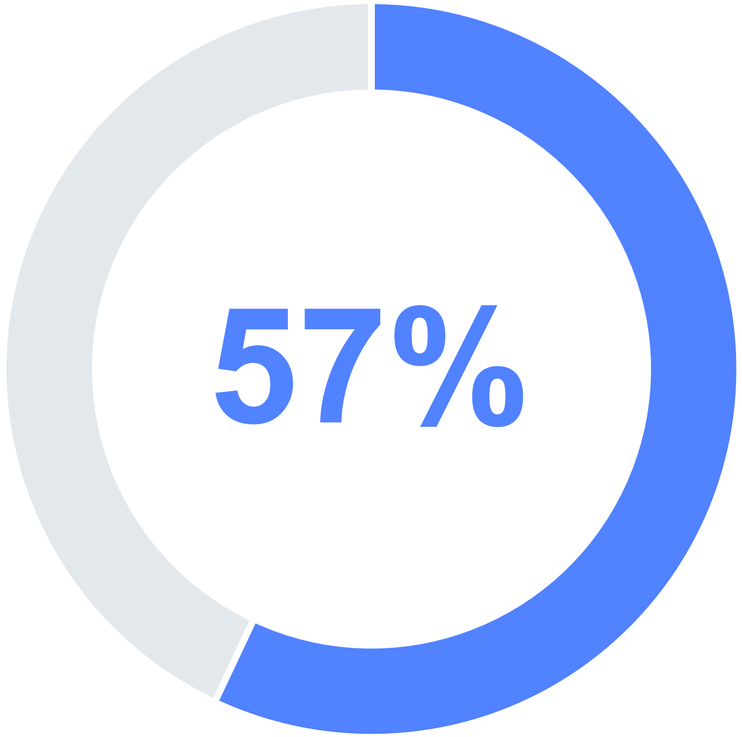
Причины инцидентов, связанных с информационной безопасностью

37%

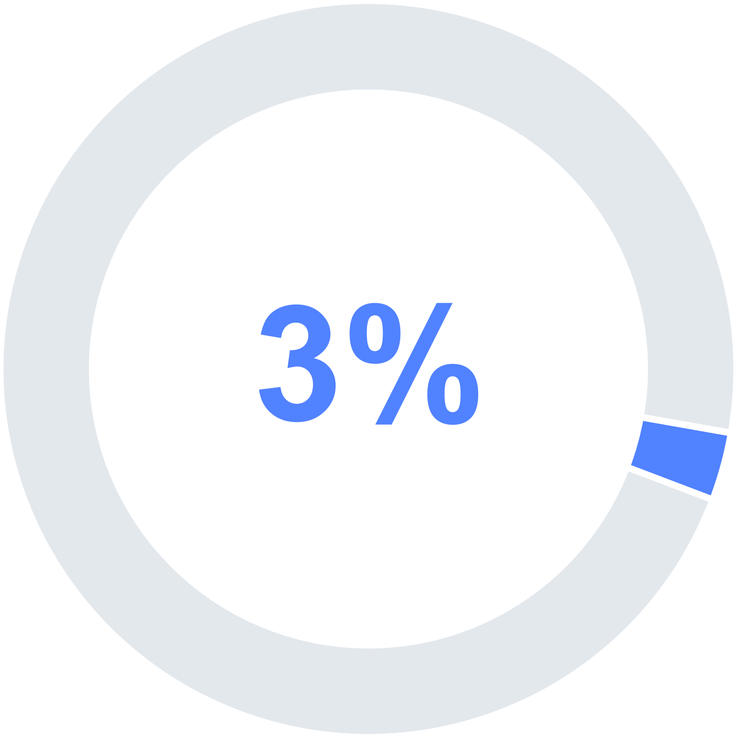
(представители ритейла), в отличие от финансового сектора и других отраслей, также выделяют низкую квалификацию сотрудников как одну и важных причин

Рост инцидентов, связанных с ИБ в РФ за последний год, и введение оборотных штрафов за утечку персональных данных повлияли на включение рисков ИБ в модель рисков компании. Теперь они проходят оценку в общем объёме и влияют на стратегическое планирование

Доля компаний, в которых проводится анализ рисков при планировании перехода на облачные решения (по мнению опрошенных сотрудников)



Доля компаний, в которых высоко оцениваются риски от компрометации, утечки и потери данных в облачных решениях (по мнению опрошенных сотрудников)



Актуальность препятствий для перехода на облачные платформы по сравнению с 2022 годом

Какие препятствия для перехода на облачные платформы актуальны для вашей компании в 2023 году?

>85%

в среднем опрошенных отметили, что все перечисленные препятствия для перехода на облачные платформы также остаются актуальными в 2023 году

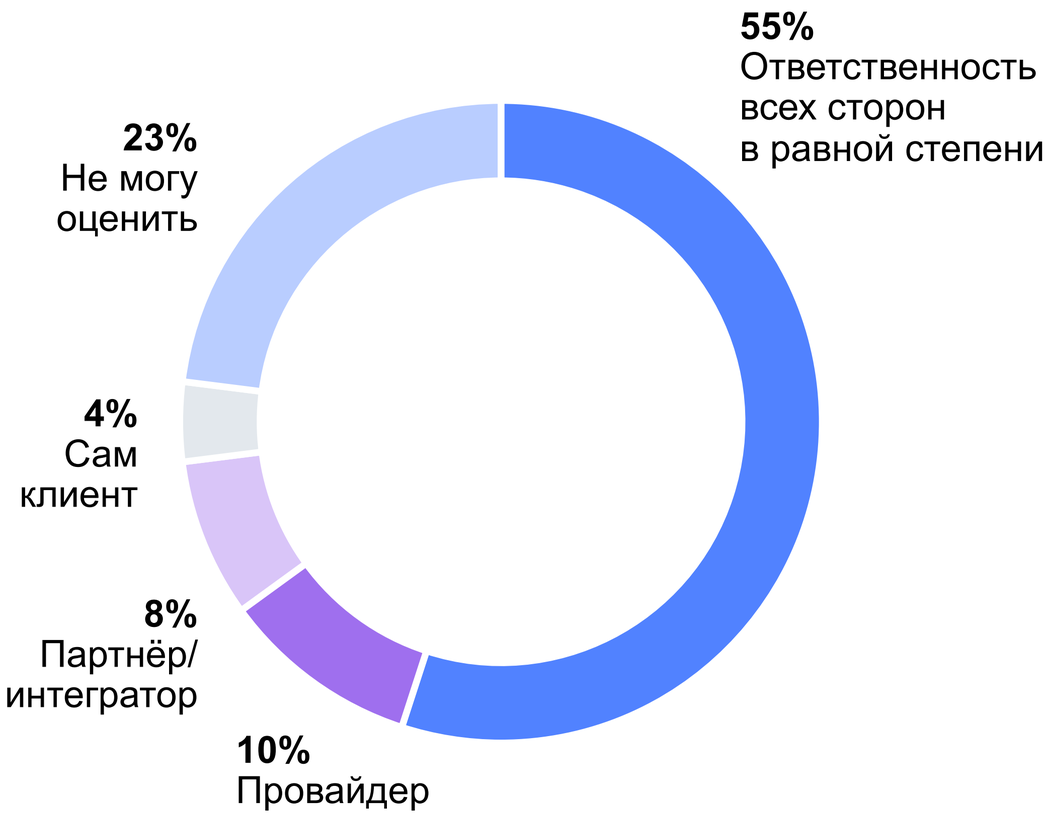
Наиболее актуальная проблема — это интеграция существующих систем мониторинга в действующие системы провайдера

Изменение актуальности по сравнению с 2022 годом рассчитано как разница между % ответов «стало более актуальным, чем в 2022 году» и «стало менее актуальным, чем в 2022 году»

1. Методология исследования
2. Особенности распределения бюджета на информационную безопасность (ИБ)
3. Актуальные средства защиты
4. Популярность технологий искусственного интеллекта (ИИ)
5. Восприятие облачных провайдеров
6. Анализ рисков и препятствия при миграции в облако
7. Преимущества использования облачных платформ для информационной безопасности (ИБ)
8. Ключевые выводы исследования

Большинство компаний считает, что провайдер и клиент в равной степени ответственны за инциденты

Кто в большей степени несёт ответственность за информационную безопасность в облаке



77%

респондентов знакомы с концепцией совместной ответственности

Более половины опрошенных (55%) считают, что все участники в равной степени несут ответственность за информационную безопасность в облаке

На уровне отраслей выделяется ритейл: представители чаще выбирают провайдера в качестве ответственного лица (24% vs 10%)

Общая выборка (n) — 302 респондента

«

Клиент и провайдер используют модель совместной ответственности, в которой часть функций по защите инфраструктуры ложится на провайдера, а часть на клиента. Однако надо понимать, что для провайдера это во многом вопрос репутации и он не менее заинтересован в безопасности инфраструктуры клиента, чем сам клиент. Чтобы обеспечить высокий уровень защиты данных, провайдер делает настройки по умолчанию максимально безопасными, а также развивает cloud native средства безопасности, которые позволяют клиенту легче и эффективнее организовать безопасность в своей области ответственности.

Евгений Сидоров,
CISO, Yandex Cloud

Что может помочь в предотвращении проблемы утечки данных при использовании облачного провайдера?

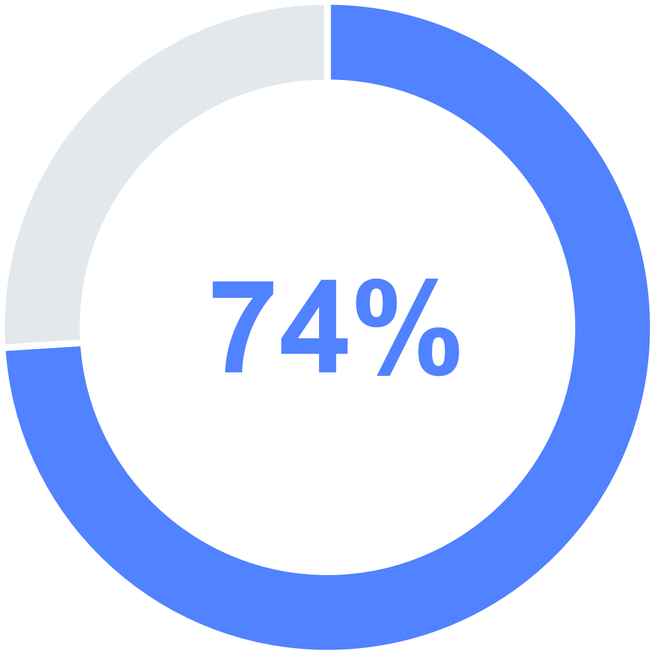
- Чёткие инструкции и рекомендации от провайдера. Повышение безопасности хранения данных провайдером
- Доработки способов улучшения безопасности, новые ГОСТы шифрования и сертификации
- Возможность шифрования всех видов данных, загружаемых в облако

Как облачный провайдер может помочь в предотвращении проблемы утечки данных при использовании облака?

- Увеличить штат сотрудников, отвечающих за безопасность, уменьшить риски утечки данных о технологии работы системы безопасности
- Предоставлять клиентам инструкции, как правильно использовать облако
- Проводить сертификацию соответствия сотрудников, анализ блогов

Активное внедрение клиентских онлайн-сервисов со стороны компаний, а также опыт использования облачных сервисов для внутренних задач привели к значительному повышению уровня доверия к облачным технологиям

Уровень доверия к безопасности облачных сервисов достаточно высокий, 74% оценивают безопасность работы с провайдерами выше среднего



43% vs 75%

Непосредственная работа с облачными платформами укрепляет уровень доверия к использованию облачных сервисов: восприятие безопасности решений среди потенциальных пользователей ниже, чем среди текущих клиентов

Общая выборка (n) — 302 респондента

Общий рост доверия среди компаний, пользующихся услугами облачных провайдеров, подкрепляется следующими преимуществами облачных решений

Экономия ресурсов команды и бюджета внутри компании: есть возможность воспользоваться готовыми пакетными решениями и отдельными сервисами

Наличие в облаке security-специалистов с экспертизой в работе с инцидентами и решении проблем, связанных с безопасностью в облаке

Крайне низкая доля компаний на рынке с негативными кейсами о безопасном использовании облачных решений

Работа с облачными технологиями позволяет улучшить подход к безопасности внутри компаний в целом, отсюда рост компетенций команды в использовании облачных решений и работе с данными

1. Методология исследования
2. Особенности распределения бюджета на информационную безопасность (ИБ)
3. Актуальные средства защиты
4. Популярность технологий искусственного интеллекта (ИИ)
5. Восприятие облачных провайдеров
6. Анализ рисков и препятствия при миграции в облако
7. Преимущества использования облачных платформ для информационной безопасности (ИБ)
8. Ключевые выводы исследования

Результаты исследования

- Бюджеты, выделяемые в 2023 году на информационную безопасность, увеличились примерно у половины опрошенных компаний
- Больше всего компании инвестировали в обновление ПО и лицензий
- Среди основных трат — инвестиции в ИИ и облачные решения для повышения общего уровня защиты
- Половина компаний использует ИИ для решения задач, связанных с ИБ, ещё около трети планирует его внедрять
- 61% компаний уже используют или готовы использовать облачные платформы по гибридной модели

>50%

компаний поддерживают концепцию совместной ответственности за возникновение инцидентов

52%

опрошенных считают, что провайдеры должны быть застрахованы от рисков, связанных с утечками данных, чтобы упростить процедуру их решения

Желаемые действия провайдеров для решения проблем, связанных с человеческим фактором

- Повышать прозрачность
- Предоставлять инструменты для реагирования на инциденты

Мы будем рады ответить на ваши вопросы!

Yandex Cloud

Рами Мулейс
Менеджер продуктов безопасности

Кристина Попкова
Менеджер по количественным исследованиям

Екатерина Узлова
Менеджер по стратегии и исследованиям

Наталия Куданова
Продуктовый маркетолог Security

Деловые Решения и Технологии

Андрей Сотников
Партнёр департамента управленческого консультирования

Алексей Яковлев
Директор департамента управленческого консультирования

Александр Юрочкин
Старший менеджер департамента управленческого консультирования

Виталий Михальчук
Руководитель исследовательского центра ДРТ

Связаться с нами: cloud-sales@yandex-team.ru