INFOWATCH

АНАЛИТИЧЕСКИЙ ОТЧЁТ

Кибербезопасность облачных и гибридных инфраструктур 2025 – 2026

Читайте материалы
экспертно-аналитического
центра InfoWatch

infowatch.ru

Оглавление

Только факты

АТАКИ

25%

от общего числа кибератак в мире приходится на облачную инфраструктуру

30%

составил Рост атак на облачные и гибридные инфраструктуры в России в 2025 году

На 25%

в годовом исчислении растет число атак на облачную инфраструктуру. На первое место выходят нарушения идентификации, а почти в 38% случаев обнаруживаются неправильные настройки. API-интерфейсы являются основой облачных приложений и связаны с 31% утечек облачных данных – SentinelOne

>80%

компаний за последний год столкнулись по крайней мере с одним нарушением облачной безопасности, что свидетельствует о широком распространении этого явления в организациях всех размеров и отраслей – StationX

ИНВЕСТИЦИИ

>51%

компаний планируют увеличить инвестиции в облачную безопасность для устранения возникающих угроз – Exabeam

На 25%

выросли инвестиции компаний в России в 2025 г. в облачную безопасность

БЕЗОПАСНОСТЬ ДАННЫХ

45%

утечек данных происходят в облаке – SentinelOne

80%

организаций столкнутся с утечкой облачных данных из-за утечки идентификационных данных в 2026 году – SentinelOne

93%

облачных программ-вымогателей - это исполняемые файлы на базе Windows – Varonis

$5,17млн

средняя стоимость инцидентов с безопасностью в общедоступных облаках – IBM

ЧЕЛОВЕЧЕСКИЙ ФАКТОР

95%

сбоев в облачной системе безопасности по-прежнему связаны с неправильной настройкой из-за ошибок персонала – SC Media

79%

ИТ-специалистов и специалистов по безопасности считают себя недостаточно подготовленными для предотвращения атак, в которых используются идентификационные данные, не принадлежащие людям – например, автоматизированные боты, учетные данные API – Cloud Security Alliance

99%

сбоев в облачной безопасности будут происходить по вине пользователей – Gartner

>31%

взломов облачных сервисов происходят из-за неправильной настройки и ошибок, допущенных вручную, эти векторы атак неизменно опережают другие по частоте и результативности – GoFaster

70%

компаний сталкиваются с трудностями, которые связаны с настройкой облачных вычислений и управлением состоянием безопасности – Fortinet

66%

руководителей служб безопасности не уверены в своей способности реагировать на угрозы облачной безопасности и обнаруживать их в режиме реального времени – Fortinet

ЕДИНАЯ ПЛАТФОРМА

64% **организаций предпочли бы выбрать платформу одного поставщика,** объединяющую сетевую, облачную безопасность и безопасность приложений, если бы им приходилось строить систему защиты с нуля – Cybersecurity Insiders

БЕЗОПАСНОСТЬ ИДЕНТИФИКАЦИИ И ДОСТУПА

77%

организаций называют безопасность идентификации и доступа к данным в качестве основного риска, связанного с использованием облачных технологий – SentinelOne

>70%

взломов облачных вычислений происходят из-за скомпрометированных учетных данных, что делает компрометацию учетных данных доминирующим фактором взлома – SentinelOne

65%

В России ситуация близка к мировым тенденциям – около 65% взломов облачных инфраструктур происходило из-за компрометации учетных данных

ЦЕПОЧКИ ПОСТАВОК

19%

взломов облачных вычислений происходят из-за взлома сторонних инструментов, при этом количество атак на цепочку поставок, связанных с облачными вычислениями, увеличилось на 46% по сравнению с предыдущим годом – comparecheapssl.com

40%

в России составляет доля атак на облачные и гибридные инфраструктуры путем компрометации цепочки поставок

УЯЗВИМОСТИ

32%

облачных ресурсов по-прежнему будут оставаться неконтролируемыми, и в каждом из них будет обнаружено в среднем 115 известных уязвимостей – FortifyData

В 45%

случаях атак на облачные и гибридные инфраструктуры в России использовались уязвимости приложений

ШИФРОВАНИЕ

55% **компаний уже используют облачные средства шифрования** для управления секретными ключами и их ротации в целях повышения безопасности – SentinelOne

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

42% **Статистика облачной безопасности также показывает,** что к концу 2026 года доля фишинга, основанного на искусственном интеллекте, превысит 42% от всех глобальных вторжений – CDNetworks

ПУБЛИЧНЫЕ И ЧАСТНЫЕ ОБЛАКА

27%

На общедоступные облака приходится больше обращений, чем на частные. В 2024 году 27% организаций, использующих общедоступные облака, столкнулись с инцидентами безопасности, что на 10% больше, чем годом ранее, и включает в себя в среднем 43 неправильных настройки на учетную запись - Exabeam.

19%

Частные облака работают лучше: только в 19% случаев возникают инциденты, главным образом потому, что у них больше возможностей контроля конфигураций. Однако частные облака по-прежнему сталкиваются с рисками, связанными с поставщиками, и недостатками интеграции со сторонними разработчиками, которые могут вызвать проблемы – Microsoft Azure.

19%

компаний в России используют как частные, так и публичные облака

20%

20% компаний используют только публичные облака

15%

компаний используют только частные облака

Аннотация

Экспертно-аналитический центр InfoWatch представляет отчёт по результатам исследования мировых тенденций в сфере обеспечения безопасности облачной и гибридной инфраструктуры.

Данные, используемые в отчете, получены в результате исследования инцидентов, произошедших в мире и России, всей доступной профильной аналитики, экспертных опросов.

В рамках исследования были определены тенденции наиболее актуальных угроз и развития решений по противодействию им.

На базе матрицы MITRE ATT&CK® для облачных платформ были выделены ключевые техники, использовавшиеся злоумышленниками в отношении российских организаций в 2025 году.

Также было проанализировано влияние дополнительных факторов, которые отражаются как на специфике угроз, так и на защите – в частности, развитие инструментов искусственного интеллекта (ИИ).

В исследовании приведены также выводы на основе оригинальных методик экспертноаналитического центра «ИнфоВотч».

Отчет будет полезен специалистам по информационной безопасности, в том числе специалистам в области ICS/OT (АСУ ТП), промышленного и медицинского интернета вещей, специалистам в области информационной безопасности, работающих в финансовых и страховых компаниях, государственных организациях, предприятиях торговли и услуг.

Сокращения

API	Интерфейс программирования приложений
LotL	Living off the Land («питание подножным кормом»)
MITM	Атаки типа «Человек посередине»
NGFW	Межсетевой экран нового поколения
VPN	Виртуальные частные сети
IAM	Управление идентификацией и доступом
MFA	Многофакторная аутентификация
ВПО	Вредоносное программное обеспечение
ИИ	Искусственный интеллект
OT	Операционные технологии
RaaS	Программа-вымогатель как услуга
DLP	Защита от утечек данных
DDoS	Распределенный отказ в обслуживании
SaaS	Программное обеспечение как услуга
PaaS	Платформа как услуга
IaaS	Инфраструктура как услуга
IIoT	Промышленный интернет вещей
IoMT	Медицинский интернет вещей
UEBA	Поведенческая аналитика

Ключевые тенденции

01

В мире и в России растет число гибридных и мультиоблачных инфраструктур. Около половины компаний в мире внедрили гибридные облачные модели, интегрирующие локальные и общедоступные облачные среды для оптимизации гибкости и контроля.

02

Наблюдается резкое увеличение интенсивности атак на облачные и гибридные инфраструктуры. Злоумышленники демонстрируют растущую осведомленность об облачных средствах защиты и все чаще используют тактику обхода для препятствия обнаружению и смягчения последствий.

03

По мере того, как организации ускоряют внедрение технологий ИИ, нарушители все больше нацеливаются на внедряемые технологии. Это требует создания и использования нового класса защиты: систем ИИ, специально созданные для защиты других систем ИИ.

04

Меры обеспечения облачной и гибридной безопасности на данный момент явно недостаточны. По данным TREND MICRO | 2025 Cloud Security Report, только 21% организаций полностью уверены в том, что видят рабочие нагрузки, и только 25% доверяют своим инструментам обнаружения сложных угроз.

05

Внедрение ПО на базе Kubernetes еще больше увеличивает риски. По данным Microsoft, большинство скомпрометированных контейнеров подвергаются атакам в течение первых 48 часов после развертывания.

06

Большинство компаний планируют внедрить унифицированные платформы облачной безопасности с централизованными информационными панелями для упрощения настройки политик и обеспечения согласованности, и таким образом повысить видимость облачной инфраструктуры. Активно внедряются системы управления состоянием облачной безопасности (CSPM) и облачных приложений.

07

Одним из главных препятствий во внедрении эффективных решений в области безопасности облачных и гибридных инфраструктур является отсутствие достаточного числа квалифицированных специалистов по информационной безопасности в целом и в сфере противодействия угрозам в облачной и гибридной инфраструктурах в частности. Около трех четвертей компаний испытывают нехватку специалистов в области облачной безопасности.

Результаты исследования

ВВЕДЕНИЕ

Мы живем в эпоху облачных и цифровых преобразований. Пользователи и приложения выходят за пределы традиционного сетевого периметра. Из общедоступного облака обеспечивается доступ ко все большему числу приложений, включая программное обеспечение как услугу (SaaS), платформу как услугу (PaaS) и инфраструктуру как услугу (IaaS).

53% облачных приложений в мире размещаются на общедоступных облачных платформах, что на 8% больше, чем в прошлом году.

В России около трех четвертей компаний размещают ряд ресурсов в публичных облаках. В то же время только каждая пятая компания использует исключительно публичные облака.

Рисунок 1.
Доли публичных и частных облаков в России.
Источник:
Собственная аналитика

В отраслевом срезе и срезе по размеру компаний приоритет в пользовании публичными облаками отмечен у компаний малого и среднего бизнеса и компаний торговли, услуг.

Рисунок 2.
Изменение долей публичных и частных облаков в России.
Источник:
Собственная аналитика

Все чаще предприятия выбирают мультиоблачные или гибридные модели. Гибридное облако позволяет организациям пользоваться преимуществами облака, сохраняя при этом гибкость в использовании других сред.

В концепциях защиты сетей происходят фундаментальные изменения. 82% организаций поддерживают гибридную инфраструктуру, объединяющую локальные центры обработки данных с общедоступными облаками. Хотя эта модель обеспечивает гибкость и масштабируемость, она также разрушает традиционные сетевые границы, создавая сложную сеть соединений, которую трудно отслеживать и защищать.

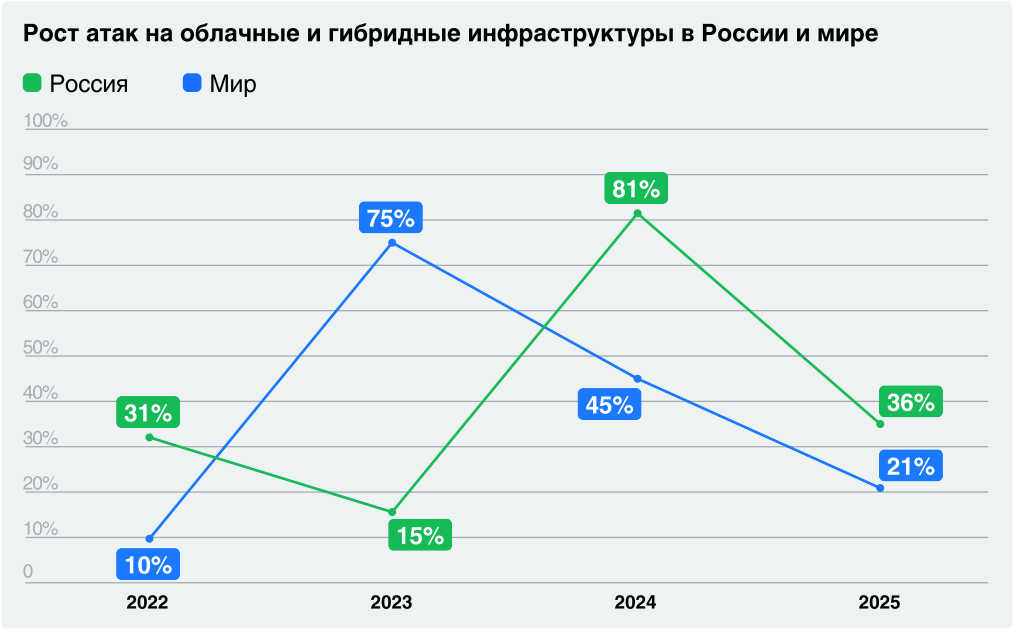
Рисунок 3.
Доля мультиоблаков и гибридных облаков в мире.
Источник: Fortinet 2025 State of Cloud Security report

Технологии облачных вычислений предоставляют организациям динамичные автоматизированные среды с облачными ресурсами по запросу. Однако многие функции противоречат требованиям сетевой безопасности. Облачные вычисления не устраняют существующие угрозы сетевой безопасности, а увеличивают их.

Злоумышленники прекрасно понимают эти проблемы. Они не видят разделения между локальным центром обработки данных и облачной средой; они видят единую расширенную сеть.

Их стратегии все чаще предполагают "межсредовую интеграцию" - закрепление в менее защищенной облачной среде с последующим переходом к высокопроизводительным локальным системам. Обнаружение злоумышленников становится все более проблематичным из-за пробелов в видимости, присущих гибридным инфраструктурам.

Рисунок 4.
Рост атак на облачные и гибридные инфраструктуры в России и мире.
Источник:
Собственная аналитика



В отчетах о состоянии облачной безопасности подчеркивается растущий «разрыв в сложности»: облачные среды стали настолько сложными, что многие организации с трудом поддерживают постоянную видимость устройств и их контроль.

Исследования показывают, что высокий процент облачных взломов остается незамеченным в течение нескольких месяцев, а время ожидания обнаружения иногда превышает 200 дней.

Эти проблемы сделали облачную безопасность приоритетной задачей, которая заключается в обеспечении баланса между гибкостью, повышением безопасности приложений и сохранением данных при их перемещении по облакам. Видимость и предотвращение атак необходимы во всех местах, где находятся приложения и данные.

Неправильно сконфигурированные хранилища, незащищенные интерфейсы управления и некорректные сетевые средства управления являются причиной большинства нарушений облачных технологий в высокоскоростных средах DevOps. В настройках облака простота использования по умолчанию ставится выше безопасности.

Внесение изменений в конфигурацию вручную и отсутствие контроля за использованием инфраструктуры в виде кода (IaC) создают проблемы, которые распространяются на многооблачные системы.

Рисунок 5.
Ключевые риски облачной безопасности.
Источник:
World Economic Forum

Облачным API-интерфейсам не хватает надлежащей аутентификации, ограничения скорости и контроля доступа, что делает их главными мишенями для злоумышленников. API-интерфейсы служат основой для взаимодействия приложений в многооблачных средах, но здесь часто встречаются нарушения аутентификации и чрезмерные разрешения.

Рисунок 6.
Риски облачной безопасности.
Источник: ORCA security

Злоумышленники все чаще нацеливаются на GitHub и инструменты разработки. Сторонние интеграции, поставщики SaaS и продукты с открытым исходным кодом создают косвенный риск. Нарушение в работе одного поставщика может поставить под угрозу всю многооблачную среду компании.

Рисунок 7.
Ключевые риски гибридных и облачных инфраструктур в России в 2025 г.
Источник:
Собственная аналитика

Различные облака и провайдеры по-разному обрабатывают шифрование, классификацию данных и хранение резервных копий. Например, конфиденциальные данные могут быть надежно зашифрованы в одной среде, но могут оставаться незашифрованными в хранилище резервных копий в другом месте. Нарушения соответствия требованиям возникают, когда стандарты шифрования не применяются единообразно в разных облачных системах.

Рисунок 8.
Gartner: оценки облачной безопасности.
Источник: Gartner

Вышесказанное говорит в пользу необходимости серьезного подхода к обеспечению безопасности в облачных и гибридных инфраструктурах. Более 51% компаний планируют увеличить инвестиции в облачную безопасность для устранения возникающих угроз. Такой рост расходов отражает растущее понимание того, что нарушения облачных технологий обходятся дорого, а превентивные меры безопасности обеспечивают более высокую рентабельность инвестиций, чем реагирование на инциденты и устранение неполадок.

Мы видим рост внимания нормативного регулирования к информационной безопасности в облачных инфраструктурах. Так, 19 мая 2026 года был зарегистрирован приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 02.12.2025 № 1106 "Об утверждении Требований к обеспечению информационной безопасности в рамках предоставления облачных услуг посредством государственной единой облачной платформы". В нем, в частности, говорится о необходимости проведения следующих мероприятий:

- выявление и оценка угроз безопасности информации;
- контроль конфигурации информационно-телекоммуникационной инфраструктуры;
- управление уязвимостями;
- мониторинг информационной безопасности;
- контроль уровня защищенности информации, содержащейся в информационно-телекоммуникационной инфраструктуре;
- обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты;

ТЕХНИКИ АТАК ПО MITRE

Рассмотрим наиболее часто встречаемые техники атак на облачную и гибридную инфраструктуру, которые мы отметили, изучая атаки в 2025 году.

Оранжевым цветом выделены тактики, которые встречались в более половины рассматриваемых случаев.

Желтым цветом выделены тактики, которые встречались в 26%-50% рассматриваемых случаев.

Лимонным цветом выделены тактики, которые встречались в 10% - 25% рассматриваемых случаев.

Таблица 1. Ключевые техники и тактики атак облачных инфраструктур в 2025г., согласно MITRE ATT&CK

Тактика	Initial Access Первоначальный доступ	Execution Выполнение	Persistence Настойчивость	Privilege Escalation Повышение привилегий
Описание	Закрепление в инфраструктуре	Запуск вредоносного кода	Поддержание доступа, несмотря на сбои	Получение более высоких разрешений
Техника	Drive-by Compromise	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism
Техника	Exploit PublicFacing Application	Command and Scripting Interpreter	Cloud Application Integration	Account Manipulation
Техника	Phishing	Poisoned Pipeline Execution	Create Account	Domain or Tenant Policy Modification
Техника	Supply Chain Compromise	Serverless Execution	Event Triggered Execution	Event Triggered Execution
Техника	Trusted Relationship	Software Deployment Tools	Implant Internal Image	Valid Accounts
Техника	Valid Accounts	User Execution	Modify Authentication Process	
Техника			Office Application Startup	
Техника			Valid Accounts	
Ключевые векторы /методы атаки	Фишинг/сбои в работе MFA, кража APIключей, неправильно настроенные общедоступные конечные точки, атаки на цепочки поставок (например, вредоносные изображения контейнеров).	Использование бессерверных функций (лямбдафункций/функци й Azure), вредоносных скриптов, взломов контейнеров.	Создание новых пользователей/клю чей IAM, добавление вредоносных приложений OAuth, изменение настроек безопасности контейнера.	Использование чрезмерно привилегирован ных учетных записей служб, злоупотребление ролями IAM, манипулировани е политиками IAM.

Тактика	Stealth Скрытность	Defense Impairment Ослабление защиты	Credential Access Доступ к учетным данным	Discovery Обнаружение
Описание	Снижение вероятности обнаружения	Уклонение от защиты	Кража учетных данных	Обнаружение инфраструктуры и ресурсов
Техника	Exploitation for Stealth	Disable or Modify Tools	Brute Force	Account Discovery
Техника	Hide Artifacts	Domain or Tenant Policy Modification	Credentials from Password Stores	Cloud Infrastructure Discovery
Техника	Indicator Removal	Exploitation for Defense Impairment	Exploitation for Credential Access	Cloud Service Dashboard

Техника	Social Engineering	Modify Authentication Process	Forge Web Credentials	Cloud Service Discovery
Техника	Unused/Unsuppor ted Cloud Regions	Modify Cloud Compute Infrastructure	Modify Authentication Process	Cloud Storage Object Discovery
Техника	Valid Accounts	Modify Cloud Resource Hierarchy	Multi-Factor Authentication Request Generation	Local Storage Discovery
Техника			Network Sniffing	Log Enumeration
Техника			Steal Application Access Token	Network Service Discovery
Техника			Steal or Forge Authentication Certificates	Network Sniffing
Техника			Steal Web Session Cookie	Password Policy Discovery
Техника			Unsecured Credentials	Permission Groups Discovery
Техника				Software Discovery
Техника				System Information Discovery
Техника				System Location Discovery
Техника				System Network Connections Discovery
Ключевые векторы /методы атаки	Избегание обнаружения, имитация обычных операций, без изменения средств контроля безопасности или компрометации каналов сбора и мониторинга.	Очистка облачных журналов (CloudTrail/Azure Monitor), использование методов "реального времени", использование украденных учетных данных, вредоносных программ без файлов.	Кража ключей IAM из инструментов CI/CD, вброс учетных данных, сброс данных из службы метаданных.	Обнаружение ресурсов, доступных в среде "инфраструктура как услуга" (IaaS). Это включает ресурсы вычислительных служб, такие как экземпляры, виртуальные машины и моментальные снимки, а также ресурсы других служб, включая службы хранения и базы данных.

Тактика	**Lateral Movement** Горизонтальное перемещение	**Collection** Сбор	**Exfiltration** Эксфильтрация	**Impact** Эффект
Описание	Перемещение между системами	Сбор конфиденциальных данных	Перемещение данных	Достижение конечной цели (ущерб/выкуп)

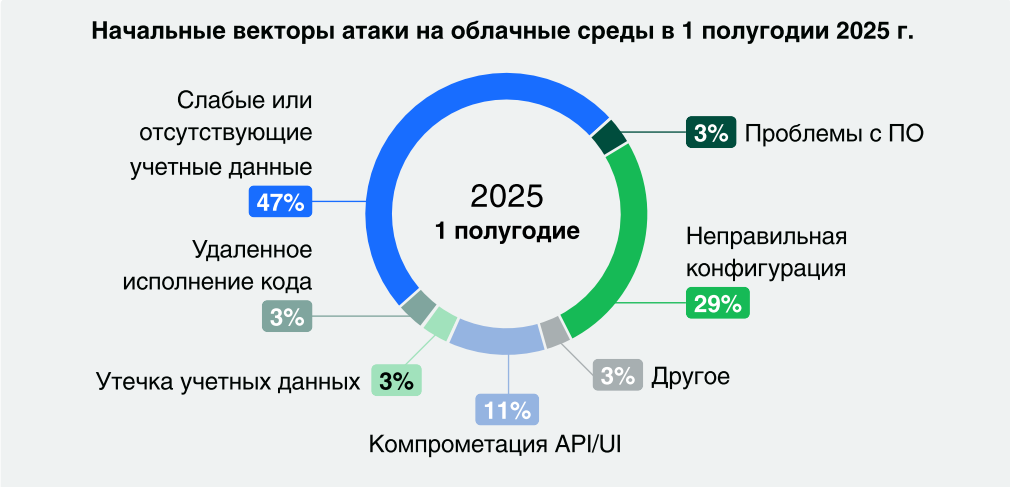
Техника	Internal Spearphishing	Automated Collection	Exfiltration Over Alternative Protoco	Account Access Removal
Техника	Remote Services	Data from Cloud Storage	Exfiltration Over Web Service	Data Destruction
Техника	Software Deployment Tools		Transfer Data to Cloud Account	Data Encrypted for Impact
Техника	Taint Shared Content	Data Staged		Defacement
Техника	Use Alternate Authentication Material	Email Collection		Email Bombing
Техника				Endpoint Denial of Service
Техника				Financial Theft
Техника				Inhibit System Recovery
Техника				Network Denial of Service
Техника				Resource Hijacking
Техника				Service Stop
Ключевые векторы /методы атаки	Переход из локальной сети в облако (или наоборот) через VPN, злоупотребление доверительными отношениями (AWS IAM, Azure Active Directory).	Извлечение данных из баз данных, клонирование блоков хранения, захват трафика API.	Перемещение украденных данных из облачной инфраструктуры во внешние системы злоумышленников.	Программывымогатели как услуга (RaaS), утечка данных, криптоджекинг, DDoS-атаки.

Рассмотрим более детально некоторые из ключевых техник проведения атак.

Initial Access - Первоначальный доступ.

- Valid Accounts (T1078.004): Злоумышленники используют украденные или взломанные облачные учетные данные (ключи AWS, Office 365, GCP) для доступа к облачным службам.
- Phishing (T1566): Злоумышленники отправляют вредоносные ссылки или вложения с целью кражи учетных данных пользователей, часто нацеливаясь на SaaS-приложения, такие как Microsoft 365 или Google Workspace.
- Exploit Public-Facing Application (T1190): Использование уязвимостей в веб-приложениях или конечных точках API для закрепления ВПО.

Рисунок 9.
Начальные векторы атаки на облачные среды.
Источник: Google H2 2025 Cloud Threat Horizons Report



Persistence - Настойчивость и Privilege Escalation - Повышение привилегий

- Account Manipulation (T1098): Злоумышленники создают скрытые учетные записи, изменяют токены OAuth или роли пользователей для обеспечения долгосрочного доступа, особенно в Azure AD.

Рисунок 10.
Ключевые злоупотребления учетными данными в 2025 г.
Источник: comparecheapssl.com

Lateral Movement - горизонтальное перемещение

Горизонтальное перемещение в облачной и гибридной инфраструктуре – один из ключевых методов, при котором злоумышленники, взломав первоначальную точку входа, перемещаются по взаимосвязанным системам, чтобы расширить доступ, повысить привилегии и найти ценные активы. В гибридных средах это перемещение часто затрагивает «стыки» между локальными центрами обработки данных и общедоступными облачными сервисами (например, AWS, Azure, GCP), используются украденные учетные данные или неправильные настройки для переключения между средами, оставаясь незамеченным в течение недель или месяцев.

Ключевые аспекты горизонтального перемещения в облачной и гибридной инфраструктурах:

- Нацеливание на идентификационные данные. Злоумышленники в основном используют слабые средства управления идентификационными данными, такие как синхронизированные учетные данные Active Directory, роли IAM с избыточными правами доступа или токены учетных записей служб, что позволяет им действовать как законным пользователям.
- "Питание подножным кормом" (LotL). Злоумышленники используют встроенные административные инструменты, такие как PowerShell, RDP, WMI или SSH, для перемещения в стороны, что делает их действия похожими на обычный системный трафик управления.

- Облачные методы. Злоумышленники используют экранирование контейнеров (например, взлом модулей Kubernetes), злоупотребляют учетными данными участников облачной службы или манипулируют ключами API для перемещения между облачными учетными записями.

- Гибридные методы. Общий путь включает в себя взлом локальной рабочей станции, сбор учетных данных и их использование для доступа к облачным ресурсам (например, Microsoft 365, Azure DevOps) с помощью механизмов доверия.

Рисунок 11.
Облачные ресурсы, способствующие горизонтальному перемещению.
Источник: ORCA security

Рисунок 12.
Облачные ресурсы, способствующие горизонтальному перемещению.
Источник: ORCA security

Reuters: *Спонсируемые государством хакеры использовали передовые устройства и действительные учетные данные для продвижения по облакам и сетям телекоммуникационных провайдеров, таких как AT&T и Verizon. Закрепившись с помощью общедоступных устройств, злоумышленники перешли к внутренним системам сетевого мониторинга, продемонстрировав, как скомпрометированная пограничная инфраструктура способствует проникновение злоумышленников вглубь корпоративной инфраструктуры.*

Impact - эффект

- Resource Hijacking (T1496): Кража вычислительных ресурсов для таких видов деятельности, как добыча криптовалюты.

Облачный криптоджекинг - злоумышленники получают доступ к облачным вычислительным ресурсам организации для добычи криптовалюты. Эти атаки приводят к увеличению стоимости облачных ресурсов, снижению производительности бизнес-операций и потенциальным нарушениям безопасности.

FastNetMon: *ShadowRay 2.0 - продолжающаяся кибератака с конца 2025 года, захватывает открытые кластеры Ray AI/GPU для создания самораспространяющегося ботнета для майнинга криптовалют (криптоджекинга), кражи данных и DDoS-атак. Обнаруженная компанией Oligo Security кампания является развитием оригинальной атаки ShadowRay, проведенной в марте 2024 года, и демонстрирует возросшую скорость, автоматизацию и скрытность атаки на высокопроизводительные вычислительные ресурсы, в частности на графические процессоры NVIDIA.*

Атаки типа DoS и DDoS

DoS и DDoS-атаки относятся к числу наиболее опасных атак на облачную инфраструктуру, которые приводят к полному нарушению работы облачного сервиса. Злоумышленники используют ботнеты и устройства Интернета вещей для проведения более масштабных атак, которые могут привести к перегрузке облачных ресурсов. Облачные сервисы взаимосвязаны друг с другом, таким образом, эффект распространяется от одного сервиса к другому, а также на организации.

Cybersecurity Dive: *Одной из самых масштабных DDoS-атак подвергся GitHub, где пик трафика достигал 1,9 Тбит/с. В ходе атаки был использован новый вектор атаки с использованием серверов memcached на базе UDP.*

24 октября 2025 года Azure DDOS Protection автоматически обнаружила и предотвратила многовекторную DDoS-атаку со скоростью 15,72 Тбит/с и скоростью передачи почти 3,64 миллиарда пакетов в секунду (pps). Это была крупнейшая DDoS-атака, когда-либо наблюдавшаяся в облаке, и она была нацелена на единственную конечную точку в Австралии

Благодаря использованию глобально распределенной инфраструктуры защиты от DDoS-атак Azure и возможностей непрерывного обнаружения были приняты меры по предотвращению. Вредоносный трафик был эффективно отфильтрован и перенаправлен, что обеспечило бесперебойную доступность услуг для рабочих нагрузок клиентов.

Атака была осуществлена из ботнета Aisuru. Aisuru - это интернет-ботнет класса Turbo Mirai, который часто проводит рекордные DDoS-атаки, используя скомпрометированные домашние маршрутизаторы и камеры, в основном у интернет-провайдеров в США и других странах.

Атака включала в себя чрезвычайно высокоскоростные потоки UDP, нацеленные на общедоступный IP-адрес, которые были запущены с более чем 500 000 IP-адресов-источников в разных регионах. Эти внезапные всплески UDP сопровождались минимальной подменой источника и использованием случайных портов-источников, что помогло упростить отслеживание и упростило соблюдение требований провайдера.

Атаки типа "Человек посередине" (MITM)

Атаки типа "Человек посередине" (MITM) в облачных вычислениях связаны с тем, что злоумышленники тайно перехватывают или манипулируют передачей данных между пользователем и облачными сервисами или между облачными компонентами. Они используют такие лазейки, как ARP-спуфинг, перехват DNS или небезопасные соединения для кражи учетных данных, токенов сеанса и конфиденциальных данных. Современные атаки, управляемые ИИ, отличаются высокой степенью автоматизации, нацелены на конфиденциальный зашифрованный трафик и обходят традиционную систему безопасности.

Основные методы MITM-атак в облачных средах:

ARP-спуфинг. Злоумышленники связывают свой MAC-адрес с законным IP-адресом для перенаправления трафика через свое устройство, что часто встречается в виртуализированных облачных сетях.

DNS-спуфинг (отравление кэша). Перенаправляет законный трафик облачных сервисов на поддельные веб-сайты для получения учетных данных для входа.

Удаление SSL/TLS. Понижает уровень защищенных HTTPS-соединений до незашифрованного HTTP, позволяя злоумышленникам считывать трафик в виде обычного текста.

Перехват сеанса. кража файлов cookie сеанса после входа пользователя в облачное приложение, что позволяет злоумышленникам выдавать себя за них

Несанкционированные точки доступа. Перехват трафика от удаленных сотрудников, получающих доступ к облачным ресурсам через небезопасный общедоступный Wi-Fi.

Abnormal AI: В августе 2025 года более 700 организаций подверглись крупной атаке на цепочку поставок SaaS, обозначенной как UNC6395, с использованием скомпрометированных токенов OAuth, полученных в результате интеграции чат-бота Salesloft Drift AI с Salesforce. Кампания продолжалась примерно с 8 по 18 августа 2025 года, при этом злоумышленники систематически экспортировали большие объемы данных из корпоративных инстансов Salesforce, а затем и из учетных записей Google Workspace, уделяя особое внимание сбору учетных данных. Эта атака, классифицированная как эволюция Man-in-the-Middle (MitM), известная как "Противник посередине" (AiTM), была нацелена на токены OAuth для получения постоянного доступа, а не просто на перехват трафика в режиме реального времени.

Атаки программ-вымогателей

Рисунок 13.
Ключевые угрозы в мультиоблачной среде – программы вымогатели в лидерах.
Источник: TREND MICRO 2025 Cloud Security Report

Основные методы атак вымогателей в облачных средах:

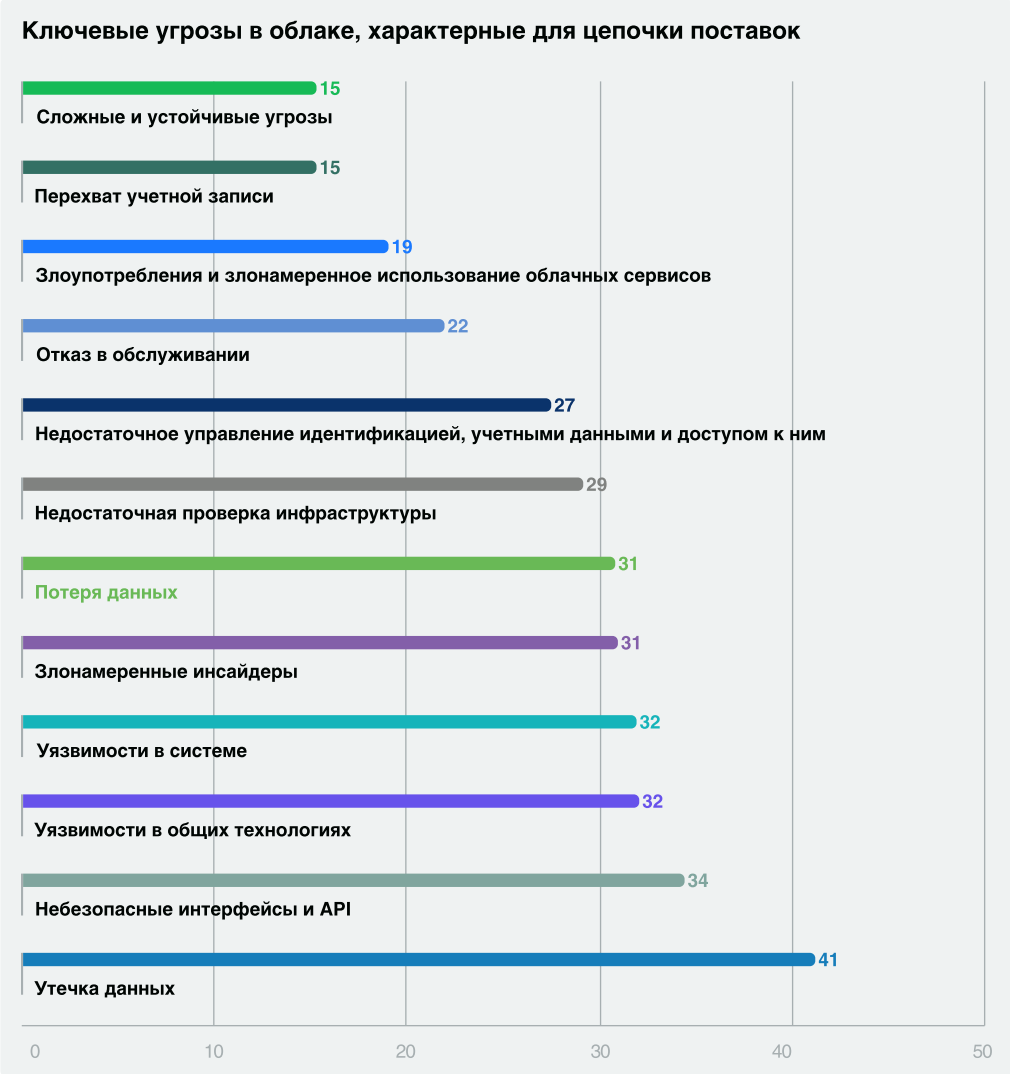
- **Двойное и тройное вымогательство (96% случаев).** Злоумышленники крадут конфиденциальные данные перед их шифрованием. Если выкуп не выплачивается, они угрожают опубликовать его (дважды), а иногда добавляют DDoS-атаки или связываются с клиентами напрямую (трижды).
- **Облачная программа-вымогатель (RansomCloud).** Атаки, нацеленные на конкретных облачных провайдеров или SaaS-приложения (например, Microsoft 365 или Google Workspace), основаны на слабой защите API, неправильно сконфигурированном хранилище (пакеты S3) или взломанных учетных записях служб.
- **Удаление данных.** Вместо шифрования злоумышленники используют скомпрометированные учетные данные администратора для уничтожения данных, резервных копий и виртуальных машин.
- **Программа-вымогатель как услуга (RaaS).** Профессиональные киберпреступные группы предоставляют начинающим хакерам программы-вымогатели, позволяющие проводить специализированные атаки на облачную инфраструктуру.

Крупнейшие атаки программ-вымогателей в 2025 году были нацелены на облачную инфраструктуру и цепочки поставок, при этом наиболее серьезными были атаки на платформу PowerSchool (потенциально более 60 миллионов записей о студентах) и Oracle EBusiness Suite cloud supply chain (6 миллионов записей). Другие крупные инциденты включали массовую кражу 31 петабайта данных у американского производителя и связанные с вымогательством отключения в Jaguar Land Rover и Ingram Micro.

Атаки на цепочки поставок

Атаки на цепочки поставок нацелены на облачные сервисы и поставщиков. Эти атаки используют уязвимости в цепочке поставок программного обеспечения для компрометации облачных сервисов или получения доступа к нескольким организациям одновременно.

Рисунок 14.
Ключевые угрозы в облаке, характерные для цепочек поставок.
Источник: ResearchGate



Sweet Security: *Червь для npm Shai-Hulud (сентябрь 2025 г.). Массированная атака на экосистему JavaScript, в ходе которой скомпрометированные пакеты npm включали постинсталляционный скрипт, автоматически крадущий учетные данные разработчика (AWS, Azure, GCP, GitHub) и публикующий их в новых общедоступных репозиториях GitHub.*

Shai-Hulud 2.0 (ноябрь 2025 г.): Усовершенствованное дополнение к сентябрьскому червю, который быстро распространился по реестру npm, скомпрометировав сотни пакетов и тысячи репозиториев GitHub всего за несколько часов.

Атаки на удаленный доступ

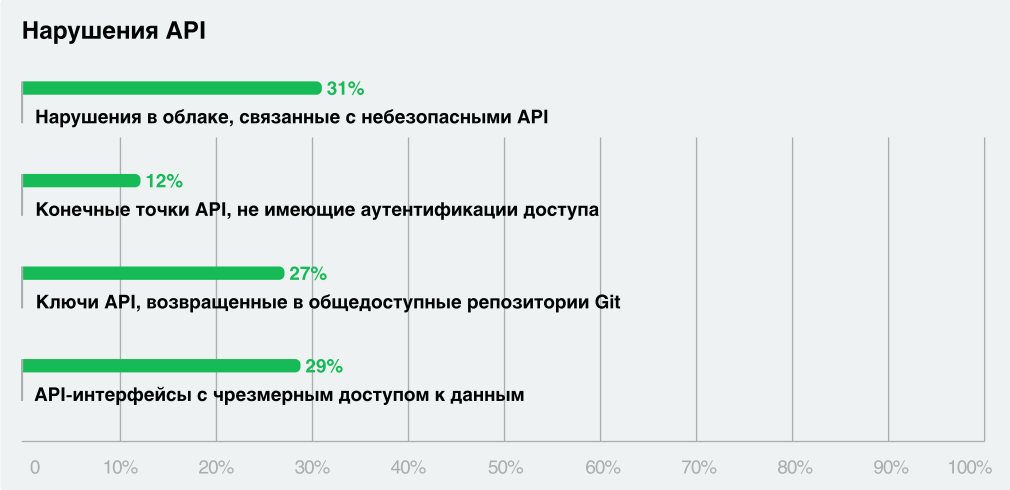
Число кибератак на удаленный доступ в облачной и гибридной инфраструктурах стремительно растет: в начале 2025 года число атак на удаленных сотрудников выросло на 238%, а число инцидентов в облачных/гибридных системах - на 26%. Эти атаки, которые часто используют скомпрометированные учетные записи пользователей и ненадежные учетные данные (97% атак), часто позволяют злоумышленникам перемещаться в разные стороны, переключаясь с локальных сред на облачные системы управления.

Скомпрометированные учетные данные/ кража личных данных: это доминирующий способ, при котором злоумышленники используют украденные пароли, перебор или распыление паролей для получения доступа к VPN, RDP и облачным консолям.

Неправильно настроенные облачные клиенты и API-интерфейсы: Неправильно настроенные хранилища, избыточные разрешения IAM и незащищенные API-интерфейсы служат точками входа.

Tenable: *В начале 2025 года наиболее масштабные атаки на облако с удаленным доступом были связаны с использованием критических уязвимостей нулевого дня в корпоративных VPN, таких как устройства Ivanti Connect Secure и SonicWall SMA, что позволяло выполнять удаленный код без проверки подлинности*

Рисунок 15.
Нарушения API.
Источник:
comparecheapssl.com



Атаки на ИИ

Статистические исследования IBM cloud security показывают, что автономные агенты ИИ изменят риски для корпоративной облачной безопасности. Мы станем свидетелями крупных инцидентов с облачной безопасностью, когда конфиденциальные IP-адреса будут скомпрометированы теневыми системами ИИ.

Злоумышленники будут использовать искусственный интеллект для более быстрого использования уязвимостей в облачной безопасности, определения путей доступа, создания вредоносных программ и обмана систем безопасности.

Vercel: *Облачная платформа Vercel в начале 2026 года сообщила о кибератаке. Кибератака была связана со сторонним инструментом искусственного интеллекта Context.ai, установленным на устройстве сотрудника.*

В марте Context.ai компания заявила, что обнаружила и предотвратила кибератаку, связанную с несанкционированным доступом к их среде AWS. Компания наняла CrowdStrike для расследования атаки и “проинформировала клиента, которого идентифицировали как пострадавшего”.

Для оказания помощи в расследовании была нанята компания Mandiant, и в настоящее время к расследованию подключены правоохранительные органы.

Хакеры, проводившие кибератаку заявили, что они получили внутренние базы данных и доступ к учетным записям нескольких сотрудников Vercel. Злоумышленники организовали каскадные атаки на глобальную цепочку поставок через несколько важных библиотек, принадлежащих Vercel, включая ту, которая уже использовалась в кибератаке в декабре. Компания Vercel заявила, что злоумышленник “очень изощренный, судя по скорости его работы и детальному пониманию систем Vercel”.

Компания Vercel предупредила, что удаления проектов или учетных записей Vercel недостаточно для устранения потенциального риска для клиентов. Компания заявила, что скомпрометированные секреты “все еще могут предоставлять доступ к производственным системам, поэтому вы должны изменить их, прежде чем удалять свои проекты или учетную запись”.

Рисунок 16.
Атаки на ИИ в облачных инфраструктурах.
Источник: PaloAlto networks State of Cloud Security Report

Слабые места

Неправильная настройка облака. Неправильные настройки, такие как открытые хранилища (S3) или ненужные открытые порты, приводят к утечке данных.

Что делать: использовать инструменты управления состоянием облачной безопасности (CSPM) для автоматического сканирования и исправления ошибок. Внедрить инфраструктуру в виде кода (IaC) для стандартизации установок.

Слабое управление идентификацией и доступом (IAM). Учетные записи с избыточными привилегиями, слабые пароли и отсутствие MFA.

Что делать: использовать инструменты управления состоянием облачной безопасности (CSPM) Повсеместно применять многофакторную аутентификацию (MFA). Применять принцип наименьших привилегий.

Слабое управление идентификацией и доступом (IAM). Учетные записи с избыточными привилегиями, слабые пароли и отсутствие MFA.

Что делать: использовать инструменты управления состоянием облачной безопасности (CSPM) Повсеместно применять многофакторную аутентификацию (MFA). Применять принцип наименьших привилегий.

Небезопасные API-интерфейсы. API-интерфейсы, в которых отсутствует надлежащая аутентификация или валидация, допускают несанкционированный доступ к данным.

Что делать: внедрять надежные шлюзы API, применять ключи API/OAuth и регулярно проводить тестирования на проникновение API.

Shadow IT и отсутствие видимости. Неутвержденные облачные сервисы, используемые сотрудниками, не управляются и не контролируются.

Что делать: использовать Cloud Access Security Brokers (CASB) для обнаружения и защиты неутвержденных сервисов.

Уязвимости контейнеров/образов. Уязвимые контейнеры или небезопасные готовые образы содержат вредоносное ПО или ошибки.

Что делать: сканировать образы контейнеров на наличие уязвимостей во время конвейера CI/CD. Использовать надежные, защищенные реестры.

Уязвимости в цепочке поставок. Скомпрометированное программное обеспечение, плагины или сторонние библиотеки, используемые в приложениях.

Что делать: внедрять спецификацию программного обеспечения (SBOM) и проводить тщательную проверку сторонних поставщиков.

Недостаточное ведение журнала и мониторинг. Отсутствие мониторинга в режиме реального времени препятствует своевременному обнаружению злоумышленников.

Что делать: включать журналы аудита, использовать централизованные решения для ведения журнала (SIEM) и настраивать оповещения об аномальной активности.

Рисунок 17. Угрозы безопасности облачной инфраструктуры
Источник: TREND MICRO 2025 Cloud Security Report

Необновленное программное обеспечение и системы. Использование известных уязвимостей в устаревших виртуальных машинах или операционных системах.

Что делать: автоматизировать циклы установки исправлений и использовать неизменяемую инфраструктуру, которая заменяет, а не обновляет серверы.

CVE – идентифицированные уязвимости в облаках

CVE-2025-53786 (Microsoft Exchange) – один из наиболее серьезных рисков, связанных с гибридными системами. Злоумышленник, получивший доступ администратора к локальному серверу Exchange, может использовать этот недостаток для полной компрометации домена в подключенной облачной среде Azure.

Windows Admin Center (WAC) Flaws (CVSS 7.8) – недостатки в этом инструменте управления работают в обоих направлениях: локальный взлом может скомпрометировать виртуальные машины Azure, а облачный взлом может привести к распространению вредоносного ПО на локальных серверах.

CVE-2025-55182 "React2Shell" (CVSS 10.0) – Эта уязвимость в React Server Components (RSC) вызвала ажиотаж у хакеров из-за своей большой поверхности атаки (уязвимо 39% облачных сред).

CVE-2026-30242 (Plane SSRF) (CVSS 8.5) – Представляет собой новые обнаруженные недостатки в инструментах разработки. Эта уязвимость позволяет злоумышленникам запрашивать службу метаданных AWS/GCP/Azure (IMDS) через веб-узлы, похищая учетные данные IAM, которые управляют всей облачной средой.

CVE-2025-69233 (Apache CloudStack) (TOCTOU) – Состояние "гонки", позволяющее пользователям обходить квоты на ресурсы. В общих или многопользовательских гибридных облаках это позволяет одному клиенту использовать ресурсы процессора и оперативной памяти для всех, что приводит к отказу в обслуживании.

CVE-2025-10725 (Red Hat OpenShift AI) (CVSS 9.9) – Поскольку рабочие нагрузки ИИ перемещаются в гибридные облака, была обнаружена ошибка, позволяющая специалисту по обработке данных с низкими привилегиями (через ноутбук) получить статус полноценного администратора кластера, что ставит под угрозу все модели ИИ и данные на платформе.

CVE-2025-38464 (CVSS 9.8) – Критическая уязвимость службы Windows Server (LanmanServer), позволяющая выполнять удаленный код без проверки подлинности.

CVE-2021-4034 (Polkit Privilege Escalation) – По-прежнему используется злоумышленниками для получения root-доступа в облачных средах Linux.

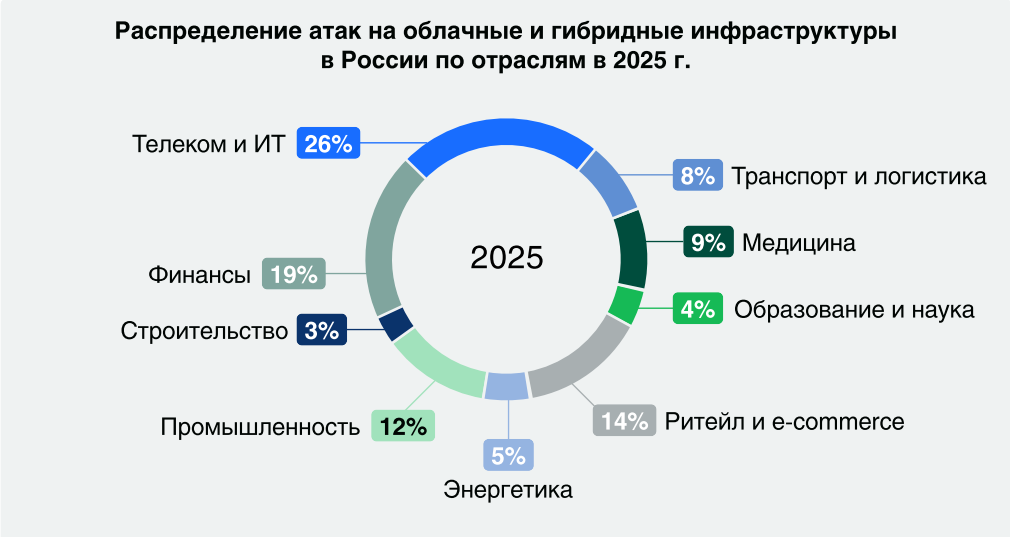
Факты об уязвимостях в облаках:

- 72% организаций имеют по крайней мере один пакет с серьезной уязвимостью (CVSS > 7) в репозитории кода
- 97% организаций имеют по крайней мере один уязвимый пакет в репозитории кода, который можно исправить.
- 16% всех обнаруженных уязвимых пакетов имеют CVE с оценкой CVSS 9 или выше. Из этих CVE 95% можно исправить.

Атакуемые отрасли

Поскольку все больше ресурсов переносится в облако у предприятий разных отраслей, соответственно, практически во всех отраслях растут атаки на облачные и гибридные инфраструктуры. Разумеется, со своей спецификой для каждой отрасли.

Рисунок 18. Распределение атак на облачные и гибридные инфраструктуры в России по отраслям в 2025 г. Источник: Собственная аналитика



НЕФТЕГАЗОВАЯ ОТРАСЛЬ

- В разведке и добыче решения по облачной и гибридной кибербезопасности защищают передачу данных с буровых установок и сейсморазведочных работ в облако для анализа. Основное внимание уделяется защите передовых вычислений и устройств IIoT.
- В транспортировке и хранении защищают SCADA-системы и удаленные терминалы (RTU) на трубопроводах, компрессорных станциях и резервуарах для хранения.
- В переработке и распределении защищают системы управления нефтеперерабатывающими и нефтехимическими заводами. Основное внимание уделяется обеспечению гибридных соединений между промышленными датчиками Интернета вещей и облачными платформами моделирования или аналитики для предотвращения сбоев в работе.

Таблица 2. Риски и угрозы в локальной, гибридной и облачной инфраструктурах в нефтегазовой промышленности. Источник: Собственная аналитика

Уровень	Локальная инфраструктура	Гибрид	Облако
Корпоративный ИТ	Фишинг, кража учетных данных, использование VPN	Неправильно сконфигурированные гибридные межсетевые экраны/VPN	Использование SaaS/API, неправильная настройка
Операции	SCADA/HMI ВПО, Плохая сегментация сети	Потеря данных на границах сред	Компрометация хранилищ данных, размещенных в облаке
Контроль /Процессы	PLC/RTU модификации, Вмешательств о в систему безопасности	Горизонтальное перемещение из ИТ в ОТ	Несанкционированный удаленный доступ к ресурсам в облаке
Сквозной /Все	Внутренние угрозы	Риски цепочки поставок	Распределенный отказ в обслуживании (DDoS)

Huntress: *Кибератака на компанию Halliburton, одного из крупнейших в мире поставщиков нефтесервисных услуг привела к значительным сбоям в работе, краже данных и, по оценкам, к убыткам в размере 35 миллионов долларов. Компания обнаружила несанкционированный доступ к своим системам и впоследствии сообщила об этом в отчете SEC, указав, что хакеры украли данные. Halliburton была вынуждена отключить системы, чтобы предотвратить дальнейшее поражение систем, что привело к сбоям в работе бизнес-приложений, включая выставление счетов и закупки. В отчетах об инциденте указывается, что, атаковав облачные ресурсы, злоумышленники переместились во внутреннюю сетевую инфраструктуру.*

ХИМИЧЕСКАЯ И НЕФТЕХИМИЧЕСКАЯ ОТРАСЛИ

Неправильно сконфигурированные облачные среды, небезопасные API и уязвимости цепочки поставок могут привести к серьезным простоям производства, краже интеллектуальной собственности и экологическим рискам. Защита этих систем требует надежной аутентификации, сегментации и постоянного мониторинга.

Киберугрозы в химическом и нефтехимическом секторах все чаще переходят от изолированных ИТ-фишинговых атак к сложным гибридным кампаниям, нацеленным как на корпоративные данные, так и на средства управления технологическими процессами.

Интеграция ИТ/ОТ и внедрение облачных сервисов расширили возможности для атак, позволив злоумышленникам нацеливаться на интеллектуальную собственность, нарушать работу производства и манипулировать системами безопасности.

Таблица 3.
Риски и угрозы в локальной, гибридной и облачной инфраструктурах в химической и нефтехимической промышленности.
Источник: Собственная аналитика

Уровень	Угрозы и векторы атаки	Ущерб
Облако	Неправильно настроенное облачное хранилище, уязвимости API, скомпрометированные учетные данные SaaS, облачное вредоносное ПО, нацеленное на цифровых двойников	Кража интеллектуальной собственности, нарушение поставок, утечка данных из инструментов оценки химической безопасности (CSAT)
Гибрид	Небезопасный удаленный доступ (VPN), переход от корпоративных ИТ к ОТ, переход от устройств IIoT к устаревшим ПЛК	Вредоносное ПО распространяется от бизнес-систем к производственным линиям Программы-вымогатели нарушают работу производства, контроль и видимость производственных процессов
Локальная инфраструктура	Вредоносное ПО (Trisis/Triton), устаревшие системные уязвимости, атаки с использованием USB, манипулирование SCADA-системой, атаки на персонал ОТ	Фальсификация рецептуры химикатов, физический ущерб оборудованию, загрязнение окружающей среды

The Register: *В январе 2024 года инструмент оценки химической безопасности CISA (CSAT) был взломан с использованием уязвимостей в защищенных устройствах Ivanti Connect, что потенциально привело к раскрытию конфиденциальных данных о химических объектах высокого риска. Хотя утечка данных подтверждена не была, доступ к информации включал планы обеспечения безопасности, запасы химических веществ и записи о проверке персонала.*

ПИЩЕВАЯ ПРОМЫШЛЕННОСТЬ

Угрозы облачной безопасности в пищевой промышленности стремительно растут по мере того, как компании оцифровывают цепочки поставок. Поскольку пищевая промышленность считается критически важной инфраструктурой с низким уровнем простоев, она является одной из главных мишеней для киберпреступников, а общие затраты на инциденты часто превышают $10-20 млн долларов.

Киберугрозы в пищевой промышленности и производстве напитков развиваются от простой кражи ИТ-данных до сложных атак на операционные технологии (ОТ) и цепочки поставок. Зависимость отрасли от поставок "точно в срок" в сочетании с устаревшими системами и растущим внедрением Интернета вещей делает ее привлекательной целью для программвымогателей и сбоев в работе.

Ключевые моменты, характерные для облачной безопасности в пищевой промышленности:

- Рост числа программ-вымогателей. В начале 2025 года число атак на продовольственный и сельскохозяйственный сектор удвоилось.
- Двойное вымогательство. Злоумышленники не только шифруют данные, но и крадут их, угрожая разглашением конфиденциальной информации для принудительного осуществления платежей.
- Искусственный интеллект/дипфейки. Все чаще используется социальная инженерия на базе искусственного интеллекта для обхода многофакторной аутентификации (MFA).
- Риски для поставщиков. Уязвимости сторонних поставщиков используются в качестве бэкдоров (15% атак).

Таблица 4.
Риски и угрозы в локальной, гибридной и облачной инфраструктурах в пищевой промышленности.
Источник: Собственная аналитика

Уровень	Локальная инфраструктура	Гибрид	Облако
ОТ	Вмешательство в работу ПЛК/SCADAсистемы: злоумышленники изменяют рецептуру, добавки или температурные датчики	Использование VPN: небезопасные соединения, соединяющие ОТ с ИТ-сетями	Неправильная настройка SaaS IoT. Неправильно защищенные датчики интеллектуального земледелия, подключенные к облаку
	Уязвимости устаревшей системы: старая ОС Windows на заводских компьютерах	Атаки на пограничные устройства: скомпрометированные датчики Интернета вещей, подделывающие данные	
Сеть	Программа-вымогатель/ блокировщики: остано вка производства	Сбой в системе совместной ответственности: утраченное доверие между службой информационной безопасности предприятия и поставщиком услуг CSP	DDoS-атаки на платформы для заказов/логистики
Уязвимости	Горизонтальное перемещение: злоумышленник перемещается из ИТ в другие сети	Уязвимости API: уязвимость логистических API для DDoS-атак	Эксплойты нулевого дня: использование уязвимостей в управляемой передаче файлов (например, GoAnywhere MFT)
Данные и приложения	Кража интеллектуальной собственности: кража патентованных рецептов или рецептур.	Риски передачи данных: перехват конфиденциальных данных, передаваемых из сети в облако	Нарушения/утечка данных: неправильн о защищенные сегменты S3 или неправильная настройка базы данных
Доступ	Угрозы со стороны недовольных сотрудников	Украденные учетные данные: фишинг для получения удаленного доступа к гибридным системам	Социальная инженерия на базе искусственного интеллекта: дипфейки в обход MFA

SecurityWeek: *В июне 2025 года компания United Natural Foods, Inc. (UNFI) подверглась крупной кибератаке, связанной с программой-вымогателем, которая парализовала дистрибуцию, задержала поставки и привела к порче продукции, что значительно нарушило цепочку поставок в более чем 30 000 торговых точках. Атака, связанная с группой Spider, привела, по оценкам, к падению чистых продаж в 2025 финансовом году на сумму от 350 до 400 миллионов долларов, поскольку компания отключила критически важные системы, включая складские помещения и систему заказа, чтобы предотвратить инцидент.*

Этот инцидент выявил уязвимость моделей цепочки поставок "точно в срок", подключенных к облаку, когда сбой в работе одной центральной системы останавливает или значительно замедляет доставку в тысячи мест.

Угрозы облачной безопасности в металлургическом секторе возникают в результате взаимодействия традиционных промышленных систем управления (ICS/OT) и современных облачных ИТ-систем, создавая гибридную среду риска. Основные угрозы включают промышленный шпионаж, программы-вымогатели, нацеленные на бесперебойную работу, и атаки на серверы, используемые в производственных средах.

Таблица 5.
Риски и угрозы в локальной, гибридной и облачной инфраструктурах в металлургии.
Источник:
Собственная аналитика

Описание	Локальная инфраструктура	Облако/Гибрид
Уровень 4-5 I Бизнес		
ERP-системы, электронная почта, офисные сети, корпоративные данные	Фишинг/социальная инженерия: кража учетных данных для получения доступа к сети	Взлом SaaS/облачной учетной записи: кража учетных данных сотрудников для облачных сервисов (например, Office 365, Salesforce)
	Программа-вымогатель: шифрование корпоративных данных и финансовых записей	Неправильно сконфигурированное хранилище: доступ к интеллектуальной собственности с помощью неправильно сконфигурированных облачных блоков
Уровень 3 I Производственные операции		
MES, Historians, планирование производства, SCADA-мониторинг	Горизонтальное перемещение: злоумышленни ки переходят из IT в OT-сети из-за плохой сегментации	Небезопасные API: злоумышленники используют слабые API, связывающие OTсистемы с облачной аналитикой
	Зараженные USB-устройства: вредоносное ПО обходит системы с воздушными зазорами	Фальсификация данных: манипулирование историческими производственными данными в облаке, влияющими на контроль качества
Уровень 2 – Контроль/Процессы		
ПЛК, HMI, Датчики, Исполнительные механизмы (печи, конвертеры)	Управление ПЛК/ЧМИ: изменение логики с целью нанесения физического ущерба (например, остановка охлаждения печи)	Перехват периферийных компонентов: взлом промышленных устройств Интернета вещей (IIoT), напрямую подключенных к облачным платформам
	Отказ в обслуживании: для прекращения мониторинга в режиме реального времени	Скомпрометированные облачные обновления: вредоносный код, доставляемый с помощью средств удаленного обслуживания поставщика (аналогично SolarWinds)
Кросс уровневые		
Цепочка поставок, удаленный доступ	Эксплуатация устаревших систем: известные уязвимости в старых ПЛК/операционных системах, которые невозможно исправить	Гибридные пути атаки: Использование фрагментированной защиты, переключение между локальной и облачной системами
		Уязвимости третьих лиц: скомпрометирова ны системы поставщиков, обеспечивающие доступ

Cybersecurity Dive: *Одним из главных примеров кибератак, повлиявших на сектор металлургии и производства стали в 2025 году, стала атака на корпорацию Nucor, крупнейшего производителя стали в Северной Америке. Nucor обнаружила несанкционированный доступ к некоторым своим компьютерным системам, что вынудило компанию остановить производство на нескольких своих предприятиях. Нарушение вынудило компанию перевести уязвимые системы в автономный режим и временно приостановить работу в США, Канаде и Мексике, чтобы предотвратить дальнейший ущерб. Этот инцидент высветил уязвимость крупномасштабного промышленного производства перед угрозами, которые переходят из ИТсистем, использующих облачные хранилища в операционные технологии.*

МАШИНОСТРОЕНИЕ

Кибербезопасность на производстве защищает данные и приложения в локальных (ИТ/ОТ) и общедоступных облачных средах, что имеет решающее значение для реализации инициатив smart factory в 2026 году. Ключевые меры включают унифицированную видимость, IAM, шифрование данных и соблюдение таких нормативных требований, как GDPR/HIPAA. Безопасность охватывает как ИТ (ERP), так и операционные системы (MES/PLC).

Таблица 6.
Влияние факторов на рост затрат на кибербезопасность облачных и гибридных инфраструктур в машиностроении.
Источник:
Собственная аналитика

Фактор	Влияние	Диапазон
Растущая сложность многооблачных систем увеличивает площадь атаки	**высокое**	**3-5 лет**
Нормативные требования ускоряют расходы на обеспечение безопасности	**высокое**	**1-2 года**
Искусственный интеллект сокращает MTTR - среднее время восстановления после сбоя	**среднее**	**3-5 лет**
Рост установок платформы для защиты облачных приложений (CNAPP)	**среднее**	**3-5 лет**
Влияние API на экономию средств, определяющее бюджеты на обеспечение безопасности	**среднее**	**1-2 года**
Пилотные проекты квантово-безопасного шифрования в гиперскейлерах	**низкое**	**3-5 лет**
Идентификационный долг из-за неуправляемых машинных идентификаторов	**среднее**	**1-2 года**
Нехватка инженеров по безопасности, владеющих облачными технологиями	**высокое**	**3-5 лет**

Таблица 7.
Риски и угрозы в локальной, гибридной и облачной инфраструктурах в машиностроении.
Источник:
Собственная аналитика

Уровень	Облако	Гибрид	Локальная инфраструктура
Операционные технологии	Захват устройства IIoT, подделка прошивки через API	Вредоносное ПО, мигрирующее из IT в OT, горизонтальное перемещение из облака на локальный компьютер	Прямой физический саботаж, устаревшее вредоносное ПО (например, типа Stuxnet), несанкционированный доступ по USB
Сеть	Небезопасные API-соединения, DDoS-атаки на облачные шлюзы	Перехват данных при передаче (сбой VPN, TLS), неправильно настроенные межсетевые экраны между средами	Отсутствие сегментации сети, незашифрованный трафик, атаки типа "Человек посередине" (MITM)
Данные и приложения	Утечка данных, неправильно сконфигурированное хранилище (например, пакеты S3), риски интеграции SaaS	Несогласованные политики IAM, потерянные ключи доступа, утечка данных во время синхронизации	Внутренние угрозы, кража данных, программы-вымогатели, блокирующие локальные SQL/файловые серверы
Доступ и идентификация	Украденные учетные данные (основной вектор атаки)	Устаревшие учетные записи, повышение привилегий в облаке	Политика использования слабых паролей, атаки методом перебора, несанкционированный доступ администратора

The Record: *Серьезное нарушение работы ИТ-систем и подключенных к облаку ОТ-сетей привело к остановке заводов Jaguar Land Rover в Великобритании на пять недель. Этот инцидент привел к прямым затратам примерно в 196 миллионов фунтов стерлингов и более широкому экономическому эффекту в 1,9 миллиарда фунтов стерлингов, что привело к падению выручки за квартал на 24%.*

Группа программ-вымогателей Qilin зашифровала производственные и логистические системы Asahi Group Holdings в сентябре 2025 г., что привело к остановке работы шести пивоваренных заводов в Японии. Атака привела к краже 27 ГБ данных и привела к значительному падению продаж напитков.

СТРОИТЕЛЬСТВО

- Злоумышленники нацелены на облачные хранилища и резервные копии для шифрования проектных данных, файлов BIM (Building Information Modeling) и финансовых записей.
- В 2025 году 75% всех предупреждений о безопасности в строительной отрасли связаны с раскрытием учетных данных, что на 83% больше, чем в прошлом году.
- Злоумышленники используют инфостилеры и покупают поддельные учетные данные для получения несанкционированного доступа к облачным платформам, таким как Procore, QuickBooks и Bluebeam.
- Используя сложную сеть субподрядчиков, злоумышленники проникают в облачные системы мелких поставщиков, чтобы получить доступ к более крупным строительным фирмам. Злоумышленники используют слабую защиту подключенных устройств (беспилотных летательных аппаратов, интеллектуальных датчиков, оборудования) для проникновения в корпоративные сети и получения доступа к облачным данным, расширяя зону атаки.

Таблица 8.
Риски и угрозы в локальной, гибридной и облачной инфраструктурах в строительстве.
Источник:
Собственная аналитика

Уровень	Угрозы	Риски
Облако (SaaS, IaaS)	Программа-вымогатель как услуга, захват учетной записи	Неправильно настроенные хранилища, небезопасные API, чрезмерно разрешительные роли IAM, отсутствие шифрования
Гибрид	Утечка данных между системами, злоупотребление учетными данными, боковое перемещение	Несогласованные политики безопасности, неправильная настройка на разных платформах, пробелы в видимости
Локальная инфраструктура	Вредоносные программы, программы-вымогатели (шифрование файлов)	Устаревшие системы, устаревшее программное обеспечение (Windows XP/7), отсутствие EDR, незащищенный Wi-Fi
ОТ	Ботнеты (DDoS-атаки), захват устройств, несанкционированный доступ к системам контроля доступа	Слабые учетные данные по умолчанию, отсутствие обновлений для системы безопасности, несегментированные сети

Rapid7: *Ярким примером облачной кибератаки в строительной отрасли является атака программвымогателей на Builder Co Brothers Ltd, которая серьезно повлияла на их деятельность, поскольку была нацелена как на локальные, так и на вторичные облачные резервные копии.*

Другим примером является атака программ—вымогателей на Bouygues Construction во Франции, когда хакеры заблокировали 200 гигабайт данных, включая конфиденциальные файлы, хранящиеся в облачных средах, и потребовали выкуп.

BBC: *Манчестер/Солфорд/Болтон (август 2024 г.): В ходе атаки на стороннего поставщика программного обеспечения для жилищного строительства (Locata) был использован облачный фишинг. Злоумышленники использовали взломанные системы для отправки электронных писем с просьбой к жителям активировать "варианты аренды" и передать личную информацию.*

ФИНАНСЫ

- Облачная безопасность в финансовой сфере обеспечивается быстрым внедрением решений в области ИБ(98% случаев использования) и соблюдением высоких требований.
- В 2025 году стоимость каждого инцидента, связанного с утечкой данных, составит в среднем $6,08 млн, что на 22% выше, чем в среднем по остальным отраслям.
- Финансовые компании активно внедряют гибридные (59%) и мультиоблачные (56%) стратегии.

Таблица 9.
Риски и угрозы в локальной, гибридной и облачной инфраструктурах в финансовых организациях.
Источник:
Собственная аналитика

Уровень	Облако	Гибрид	Локальная инфраструктура
Ключевая угроза	Неправильная настройка и злоупотребление идентификационным и данными	Несоответствия в системе безопасности и пробелы в видимости	Программывымогатели и уязвимости устаревших систем
Идентификация /Доступ	Перехват идентификационных данных, отличных от человеческих (межмашинный), учетные записи служб с избыточными привилегиями, кража API-ключей	Горизонтальное перемещение между облачными и текущими сервисами, кража токенов сеанса, утечка учетных данных	Атаки на Active Directory, использование неактивных учетных записей, уязвимые пароли
Инфраструктура	Доступ к открытым массивам облачных хранилищ, уязвимости в бессерверных функциях, небезопасные API	Несогласованные политики безопасности на разных платформах, утечка данных во время миграции	Устаревшее оборудование, физический доступ к серверам, устаревшие операционные системы (например, Windows Server 2012)
Приложение	Внедрение конвейера CI/CD, небезопасные APIконнекторы/плагины, неправильное использование OAuth-приложений	Уязвимости API между базовыми банковскими и финтех-партнерами SaaS	SQL-инъекции, межсайтовый скриптинг (XSS), использование устаревших вебприложений
Данные	Утечка данных из хранилища, заражение моделей искусственного интеллекта	Неправильное управление конфиденциальностью данных в разных юрисдикциях, передача незашифрованных данных	Кража данных из локальных баз данных, отсутствие сегментации, кража физических носителей
Внутренние угрозы	Случайная неправильная настройка облака DevOps, "vibe coding" (небезопасный код, сгенерированный искусственным интеллектом)	Фишинг, мошеннические действия, направленные на ИТ-службу поддержки	Инсайдерские угрозы, продажа данных злоумышленниками, ошибки по неосторожности

Cybersecurity Insiders: *В октябре 2025 года в EuroFin Bank произошла серьезная утечка облачных данных, в результате которой злоумышленники получили несанкционированный доступ к конфиденциальной информации, хранящейся в его облачных системах. Этот инцидент, вошедший в число крупнейших нарушений в финансовом секторе в 2025 году, послужил поводом для проведения расследований в области безопасности цифровой инфраструктуры банка.*

ТЕЛЕКОММУНИКАЦИИ

- Устройства Интернета вещей, широко используемые в телекоммуникациях, являются основными объектами для взлома и использования ботнетов (например, ботнет Mirai).
- Быстрое распространение устройств Интернета вещей (IoT) и виртуализированной инфраструктуры 5G расширяет возможности для атак, создавая новые уязвимости.
- Утечка идентификационных данных, уязвимости API и неправильные настройки – ключевые риски в телекоме.

Таблица 10.
Риски и угрозы в локальной, гибридной и облачной инфраструктурах в телекоммуникациях.
Источник:
Собственная аналитика

Уровень	Облако	Гибрид	Локальная инфраструктура
Приложения и данные	Утечки данных (незащищенные корзины), небезопасные API	Доступ к конфиденциальным данным при передаче из облака в сеть, взлом SaaSприложений	Кража данных, SQL-инъекции, несанкционированный внутренний доступ, уязвимости устаревшего программного обеспечения
Идентификация и доступ	Захват учетной записи, недостаточное управление идентификацией, кража учетных данных	Устаревшие/ синхронизированные учетные записи, слабая многофакторная аутентификация (MFA) в разных средах	Атаки методом перебора, инсайдерские угрозы, повышение привилегий, риски, связанные с общими учетными данными
Сеть и инфраструктура	DDoS-атаки на провайдера, уязвимости виртуализации/ гипервизора	Неправильно настроенные VPN/Direct Connect, несогласованные политики безопасности в разных средах	Нарушение периметра сети, DDoS-атаки, отсутствие сегментации, необновленные серверы
Регулирование и процессы	Неправильные настройки, пробелы в распределении ответственности, риски блокировки поставщика	Высокая сложность ведения журнала/ просмотра, пробелы в соблюдении нормативных требований	Отсутствие управления исправлениями, слабое соответствие требованиям, неадекватное планирование аварийного восстановления
Цепочка поставок	Скомпрометированные сторонние облачные сервисы/плагины	Использование API в облачных/оперативны х системах, уязвимости SaaS сторонних производителей	Скомпрометированное программное обеспечение

United States Forces Korea: *В 2025 году крупнейшим инцидентом, связанным с облачной безопасностью, повлиявшим на телекоммуникационный сектор, стала утечка данных SK Telecom в апреле, когда злоумышленники похитили записи аутентификации почти 27 миллионов абонентов, что привело к потенциальному клонированию SIM-карт и краже личных данных. Другой серьезной угрозой была шпионская кампания "Salt Typhoon", целью которой были устройства, подключенные к глобальной телекоммуникационной сети, для кражи данных конфигурации и мониторинга коммуникаций.*

ЭНЕРГЕТИКА

- Энергетическая инфраструктура сталкивается с растущим числом киберфизических гибридных угроз, в частности, нацеленных на системы управления энергосистемой. Злоумышленники используют искусственный интеллект для улучшения вредоносного ПО и ускорения атак.
- Индустрия переходит к системам безопасности с нулевым уровнем доверия, используя средства защиты, дополненные искусственным интеллектом, для прогнозного обнаружения угроз и внедряя строгое шифрование данных, особенно в условиях стремительного роста числа устройств Интернета вещей.
- Помимо обеспечения безопасности, внедрение облачных технологий обеспечивает более высокую эффективность работы, позволяя управлять сетями в режиме реального времени, улучшать управление данными и ускорять восстановление во время стихийных бедствий или киберугроз.

Таблица 11.
Риски и угрозы в локальной, гибридной и облачной инфраструктурах в энергетике

Облако	Гибрид	Локальная инфраструктура
Использование APIинтерфейсов CSP, неправильная настройка облака, взлом учетной записи	Горизонтальное перемещение между средами	Взлом SCADA-систем, вредоносное ВПО (Triton) для систем безопасности

SaaS-программывымогатели, утечка данных из хранилища данных	Программы-вымогатели распространяются из облака в производственный сегмент	Специализированное вредоносное ПО (Industroyer2, FrostyGoop), предназначенное для взломщиков/ПЛК
Кража учетных данных с использованием консоли управления облаком	Несогласованные политики IAM, потерянные учетные записи в разных системах	Злоумышленники, нерадивые работники, несанкционированные USBустройства в SCADA
Уязвимости API, небезопасные сетевые подключения	Незашифрованный трафик между облачными периферийными устройствами и локальным SCADA	Необновленные устаревшие ОС Windows/Linux, незашифрованный трафик Интернета вещей/ интеллектуальных счетчиков

A-STAR7_DOCTOR: *Подразделение HUNTER выявило всплеск вредоносной активности, направленной против предприятий ядерной энергетики, с заметным акцентом на уязвимости облачной инфраструктуры и конвергенции ИТ/ОТ. Полученные данные свидетельствуют о растущем риске, исходящем от злоумышленников, использующих украденные учетные данные и фишинг для проникновения в критически важную инфраструктуру.*

ТРАНСПОРТ И ЛОГИСТИКА

- Примерно 74% транспортных компаний используют как локальные центры обработки данных, так и облачные ресурсы.
- Транспортный сектор входит в тройку основных объектов кибератак, при этом число инцидентов с использованием программ-вымогателей только в морском транспорте выросло на 467% в годовом исчислении.
- Утечка данных на транспорте может обойтись в среднем в 4,18 миллиона долларов.
- По мере перехода логистики на "Логистику 4.0" — цифровизацию складов, автопарков и мониторинг движения — каждый незащищенный API, устройство Интернета вещей или партнерское соединение становятся воротами для злоумышленников.
- Плохо защищенные GPS-трекеры, телематические системы и складские датчики легко поддаются взлому.

Таблица 12.
Риски и угрозы в локальной, гибридной и облачной инфраструктурах в транспорте и логистике

Облако	Гибрид	Локальная инфраструктура
Компрометация цепочки поставок: Злоумышленники нацеливаются на поставщиков SaaS (например, TMS/WMS), чтобы получить доступ к нескольким клиентам	**Горизонтальное перемещение:** злоумышленники используют украденные учетные данные для перемещения между локальной и облачной инфраструктурами	**Программывымогатели/двойное вымогательство:** блокировка и кража данных с устаревших серверов, захват важных транспортных документов
Утечка данных: Конфиденциальные данные о поставках, хранящиеся в облаке, похищаются ботами, управляемыми искусственным интеллектом	**Неправильная настройка:** автоматизация создает пробелы в безопасности в разных средах	**Внутренние угрозы:** недовольные сотрудники получают доступ к локальным системам
Атаки по API/ идентификационным данным: Использование небезопасных API в облачных TMS или взлом учетных записей администраторов	**Кража токенов/учетных данных:** кража токенов сеанса в системах идентификации для обхода MFA	**Атаки на конвергенцию ОТ/ИТ:** вредоносное ПО (например, VPNFilter), распространяющееся из ИТсистем в системы ОТ (конвейерные ленты, сортировочные машины)
DDoS-атаки: взлом клиентских порталов или сайтов бронирования	**Несогласованность данных:** ошибки при синхронизации данных в режиме реального времени	**Отсутствие исправлений:** используется уязвимое устаревшее программное обеспечение

Взлом Интернета вещей/ датчиков: Подделка RFID-меток или телематических средств, подключенных к облаку	**Незащищенные пограничные шлюзы:** устройства Интернета вещей, соединяющие внешние сети с Интернетом без надлежащих межсетевых экранов	Прямое вмешательство в работу локальных терминальных серверов или складских роботов
Подмена GPS: сбивание с толку автономных транспортных средств или интеллектуальных контейнеров		Небезопасные локальные сети - отсутствие сегментации Wi-Fi

Cybersecurity Dive: *Порт Сиэтла, контролирующий международный аэропорт Сиэтл-Такома и морские терминалы, подвергся атаке программы-вымогателя, которая вывела из строя ключевые системы. Целью хакеров стали облачные системы и локальная инфраструктура, включая сортировку багажа, дисплеи с информацией о рейсах и Wi-Fi. Системы были отключены для предотвращения угрозы, что привело к многодневным задержкам в работе, а багаж пришлось сортировать вручную.*

ТОРГОВЛЯ И УСЛУГИ

- Основные направления обеспечения кибербезопасности в торговле и услугах включают борьбу с программами-вымогателями, обеспечение соответствия требованиям PCI и устранение ошибок в настройках, которые являются причиной 95% взломов.
- Ключевые стратегии включают в себя нулевое доверие, обнаружение угроз с помощью искусственного интеллекта и модели совместной ответственности.
- Розничные продавцы сталкиваются с серьезными рисками, связанными с утечкой данных, которая может стоить в среднем 3,27 миллиона долларов из-за большого объема конфиденциальных личных и платежных данных.
- К основным угрозам относятся программы-вымогатели, фишинг и атаки на облачные сервисы на основе API.
- Розничные продавцы внедряют архитектуры с нулевым доверием для защиты фрагментированных систем в облачных средах и в магазинах.

Таблица 13.
Риски и угрозы в локальной, гибридной и облачной инфраструктурах в торговле и услугах

Среда	Угрозы и атаки	Уязвимости
Облако и Гибрид	Использование API, очистка инвентаря с помощью ботов, внедрение вредоносного платежного плагина, SQL-инъекция	Устаревшие плагины / темы, незащищенные админ-панели, слабая защита API
Облако и Гибрид	Кража учетных данных/Инфокрадов, захват учетной записи (ATO), обход защищенного от фишинга MFA, злоупотребление логином	Высокая текучесть кадров, плохая конфигурация IAM, использование "теневого искусственного интеллекта"
Локальная инфраструктура и гибрид	Программы-вымогатели как услуга (RaaS), распределенный отказ в обслуживании (DDoS), использование VPN/межсетевого экрана	Устаревшие системы, незащищенные периферийные устройства RDP/VPN, неправильная настройка IoT/POS
Облако и Гибрид	Двойное/тройное вымогательство, утечка данных, неправильно настроенное облачное хранилище (Пакеты S3), теневые данные	Несогласованные политики безопасности, отсутствие видимости расположения данных
Локальная инфраструктура	Вредоносное ПО для торговых точек (POS), снятие наличных в банкоматах	Неиспользуемые устаревшие терминалы, незащищенный Wi-Fi в магазине

Blackfog: *Группа Spider запустила скоординированные атаки с использованием программ-вымогателей на крупных розничных продавцов и их партнеров по логистике, включая Marks & Spencer и Co-op. Зашифрованные системы привели к шестинедельной приостановке онлайн-заказов, сервисов приложений и логистики Marks & Spencer по*

принципу "нажми и забирай". Компании столкнулись со значительными перебоями в управлении запасами и логистике. Первоначальный доступ был получен с помощью социальной инженерии (замена SIMкарты/выдавали себя за службу поддержки) с целью кражи учетных данных Active Directory, предназначенных для использования в облачных технологиях розничной торговли и логистики.

МЕДИЦИНА

- К основным угрозам относятся неправильные настройки, фишинг и атаки сторонних поставщиков. Эффективная защита требует модели совместной ответственности, строгого соблюдения нормативных требований, шифрования и доступа с нулевым уровнем доверия.
- Более 90% нарушений в сфере здравоохранения начинаются с фишинга.
- На выявление и пресечение нарушений в сфере здравоохранения уходит в среднем 279 дней — на пять недель больше, чем в среднем.
- 98,3% медицинских организаций работают со сторонними поставщиками, которые пострадали от кибератак.

Рисунок 19. Угрозы для облачных сред в медицине. Источник: ResearchGate

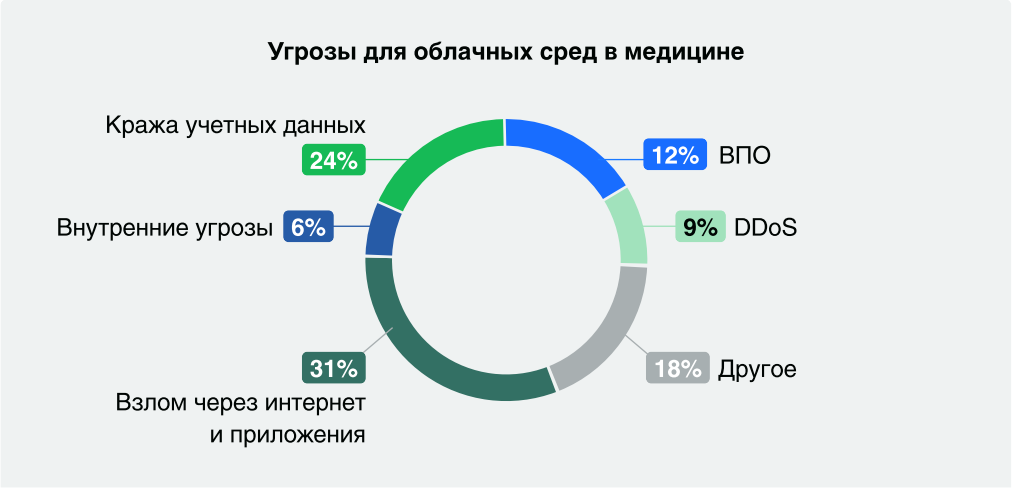


Таблица 14. Риски и угрозы в локальной, гибридной и облачной инфраструктурах в медицине

Уровень	Облако	Гибрид	Локальная инфраструктура
Угрозы	Неправильные настройки (например, открытые корзины S3)	Сбой унифицированной идентификации/IAM (доступ к обеим средам)	Программы-вымогатели в критически важных устаревших системах
Инфраструктура	Небезопасное использование API	Нарушение безопасности VPN/удаленного доступа	Сбой в работе устаревших ОС/устаревших исправлений
Данные	Кража учетных данных (агенты искусственного интеллекта)	Горизонтальное перемещение между облачными и локальными системами	Злоупотребление инсайдерской информацией (случайное/ злонамеренное)
Приложения и доступ	Внедрение без сервера / неправильное использование API	Атаки с использованием гибридной рекламы (уязвимости синхронизации)	Необновленные системы IoMT/обработки изображений
Цепочка поставок	Неправильное использование SaaS сторонними разработчиками	Утечка данных сторонних поставщиков	Атаки на цепочки поставок (Медицинские устройства)

Hyperproof: *Ярким примером кибератаки на облачную систему здравоохранения является атака программы-вымогателя на Change Healthcare. Эта атака нарушила работу рецептурных и платежных систем по всей стране, после появились сообщения о выплате хакерам выкупа в размере 22 миллионов долларов. Атака вынудила компанию закрыть свои облачные сервисы, что на несколько недель повлияло на работу тысяч провайдеров.*

ОБРАЗОВАНИЕ

Ключевые моменты, характерные для облачной безопасности в образовании:

- Более 90% школ используют облачные сервисы.
- Основные проблемы включают ограниченные ИТ-бюджеты, рост числа программвымогателей и необходимость соблюдения нормативных требований.
- Рост атак программ-вымогателей, нацеленных на школы, что приводит к отмене занятий и массовой утечке данных.
- Около 70% образовательных организаций сообщают о недостаточных бюджетах на обеспечение облачной безопасности при минимальных инвестициях в специализированный персонал службы безопасности.
- Основные риски включают фишинг, вредоносное ПО, DDoS-атаки и неправильно сконфигурированное облачное хранилище.

Таблица 15.
Риски и угрозы в локальной, гибридной и облачной инфраструктурах в образовании

Среда	Угрозы	Среднее образование	Высшее образование
Облако	Программы-вымогатели, утечка данных, захват учетной записи, неправильная настройка	Программавымогатель нацелена на облачные информационные системы для учащихся (SIS), взлом SaaSплатформы (например, Google Workspace, Microsoft 365) с помощью фишинга	Злоумышленники нацелены на хранение исследовательских данных, утечка учетных данных с использованием систем единого входа (SSO).
Гибрид	Неправильно настроенные API, доступ к данным, несогласованные политики безопасности	Уязвимые платформы удаленного обучения, подключающие домашние устройства к школьным серверам, незащищенные VPN и порталы удаленного доступа	Использование устаревших систем, интегрированных с современной облачной инфраструктурой, атаки во время удаленного доступа к исследованиям.
Локальная инфраструктура	Программывымогатели, DDoSатаки, Внутренние угрозы, уязвимости Интернета вещей	Фишинговые электронные письма (92% в начальных и 89% в средних школах). Вредоносное ПО на незащищенных школьных устройствах.	DDoS-атаки на критически важную инфраструктуру (периоды экзаменов/ приема)внутренние угрозы (несанкционированный доступ студентов/ сотрудников)

Inside Higher Ed: *В начале мая 2026 года Instructure, материнская компания широко используемой системы управления обучением Canvas (LMS), подтвердила крупную утечку данных, совершенную хакерской группой ShinyHunters. Злоумышленники утверждают, что похитили 3,65 терабайта данных, включая личные записи примерно 275 миллионов пользователей — студентов, преподавателей и персонала — почти в 9000 учебных заведениях. Хакеры атаковали облачную среду Instructure, получив доступ к Canvas Data 2, бета-версии Canvas и потенциально связанным данным Salesforce.*

Bitdefender: *Утечка данных городского совета Хельсинки. Целью взлома была облачная система образования города Хельсинки, в результате чего личная информация учащихся и опекунов была передана через сервер удаленного доступа.*

ГОСУДАРСТВЕННЫЙ СЕКТОР

- Более 92% центральных органов власти в мире используют облачные технологии.
- Злоумышленники используют ИИ для более быстрой разведки, фишинга и автоматизации атак, при этом 34% госорганизаций в мире уже сталкиваются с нарушениями, связанными с ИИ.
- Неправильная настройка остается на первом месте: несмотря на более широкое внедрение 80% госорганизаций в мире столкнулись с инцидентами облачной безопасности, основной причиной которых были неправильные настройки (например, незащищенные хранилища).
- Злоумышленники нацеливаются на учетные записи служб и агентов с искусственным интеллектом, чтобы перемещаться по облачным средам.

Программы-вымогатели эволюционируют в автоматизированные операции, управляемые искусственным интеллектом, которые нацелены на распределенные хранилища и SaaSданные. Госорганизации развитых стран активно внедряют облачные платформы защиты приложений (CNAPPs) для объединения функций безопасности, обеспечивая прозрачность между IaaS, SaaS и PaaS.

Таблица 16.
Риски и угрозы в локальной, гибридной и облачной инфраструктурах в государственных организациях

Уровень Среда	Риски	Угрозы	Цели
Облако	Неправильная настройка, небезопасные APIинтерфейсы	Программы-вымогатели, использующие искусственный интеллект, несанкционированный доступ к Identity fabric/ machine-to-machine, разрастание данных	Данные граждан, SaaS-приложения, файлы состояния
Гибрид	Фрагментированная видимость, кража учетных данных	Перемещение между облачными и текущими сервисами, захват учетных записей на основе API, несогласованные политики безопасности	IaC Роли IAM, VPN/точки доступа, публичные центры обработки данных
Локальная инфраструктура	Устаревшая инфраструктура, внутренние угрозы	Сложные программы-вымогатели, нарушения физического доступа, задержка с исправлением устаревших систем	Критически важная инфраструктура, локальные серверы, записи о персонале
Цепочка поставок	Доступ сторонних поставщиков	Скомпрометированные обновления, программные/ аппаратные бэкдоры, неправильное использование OAuth третьими лицами	Обновления программного обеспечения, порталы поставщиков, библиотеки надежного программного обеспечения

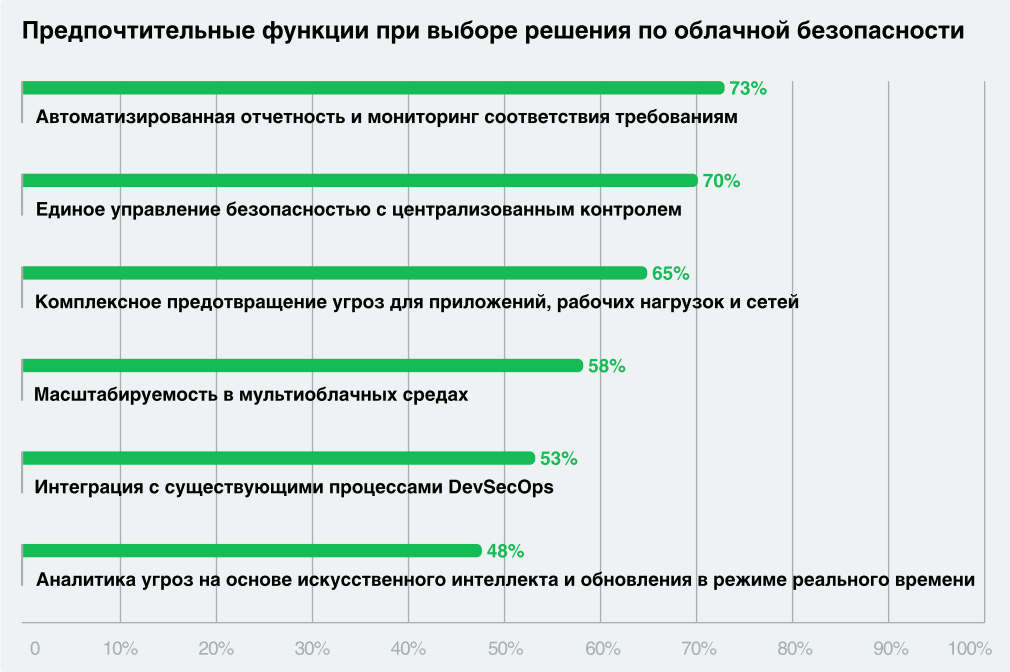
City of Columbus: *Город Колумбус, штат Огайо, подвергся атаке программ-вымогателей в июле 2024 г. Группа программ-вымогателей Rhysida получила доступ к 3,1 ТБАЙТ данных, включая файлы облачного управления, базы данных и записи о заработной плате сотрудников. Нарушение затронуло более 500 000 жителей, и конфиденциальная информация, включая номера социального страхования и водительские права, была загружена в даркнет после того, как город отказался платить.*

Методы защиты

НУЛЕВОЕ ДОВЕРИЕ И ПЛАТФОРМЕННЫЕ РЕШЕНИЯ

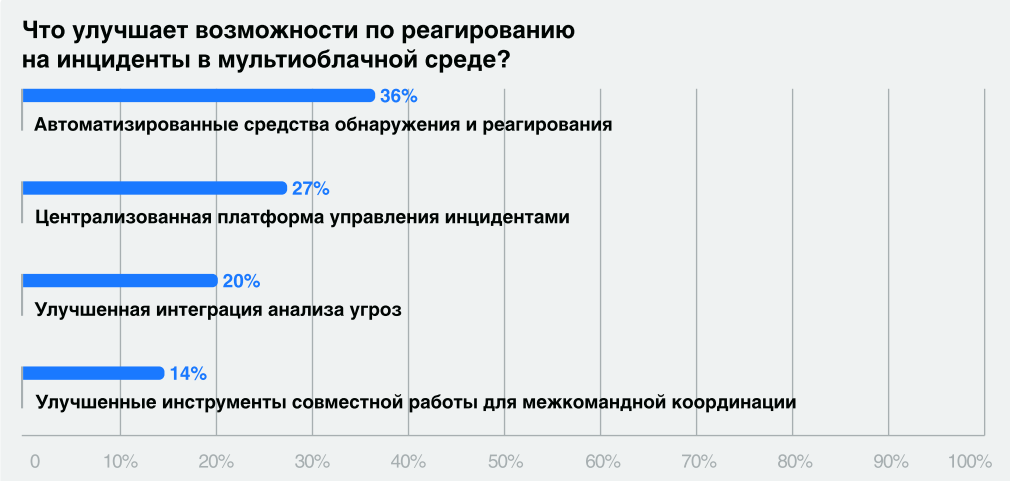
Нулевое доверие по умолчанию – "никогда не доверяй, всегда проверяй" – становится стандартом для гибридных инфраструктур, ориентированным на непрерывную проверку пользователей, устройств и приложений независимо от их местоположения. Если консолидация обеспечивает обзор, то нулевое доверие обеспечивает контроль.

Рисунок 20. Предпочтительные функции при выборе решения по облачной безопасности. Источник: TREND MICRO 2025 Cloud Security Report



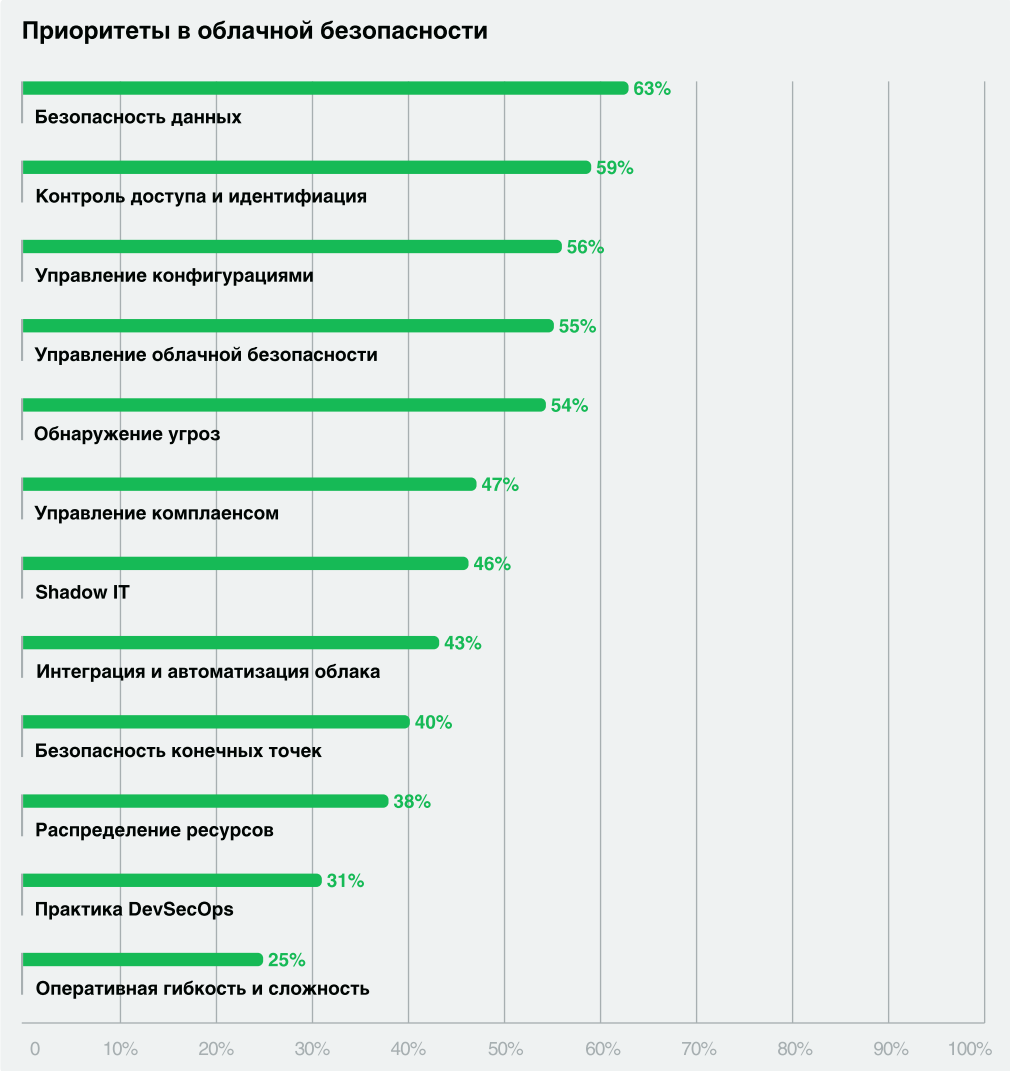
Рынок переходит к решениям CNAPPs (платформы для защиты облачных приложений). Эти платформы собирают телеметрию из любого уголка гибридной среды — от контейнеров Kubernetes до устаревших готовых серверов - обеспечивая "единое окно", в котором отчаянно нуждаются аналитики. Этот сдвиг настолько заметен, что в отчете AlgoSec за 2026 год текущий этап описывается как переход "от экспериментов к оптимизации", когда организации активно пересматривают свои наборы инструментов, чтобы расставить приоритеты в отношении платформ, обеспечивающих сквозную видимость.

Рисунок 21. Что улучшает возможности по реагированию на инциденты в мультиоблачной среде. Источник: TREND MICRO 2025 Cloud Security Report



Управление состоянием облачной безопасности: CSPM (Cloud Security Posture Management) имеет жизненно важное значение для предотвращения утечек данных, вызванных неправильно настроенным облачным хранилищем или общедоступными ресурсами.

Рисунок 22. Приоритеты облачной безопасности Источник: Fortinet 2025 State of Cloud Security report



МИКРОСЕГМЕНТАЦИЯ И МЕЖСЕТЕВЫЕ ЭКРАНЫ НОВОГО ПОКОЛЕНИЯ

Вместо того, чтобы полагаться на IP-адреса, микросегментация использует идентификаторы и ярлыки. Политики зависят от рабочей нагрузки, независимо от того, находится ли она в центре обработки данных или в облаке.

Использование устаревших межсетевых экранов в гибридной и облачной инфраструктурах создает значительные риски для безопасности, прежде всего потому, что они не имеют возможности проверять современный зашифрованный трафик и не могут адаптироваться к динамическим облачным нагрузкам. Эти устаревшие системы часто служат незащищенными уязвимыми точками входа, которые позволяют злоумышленникам перемещаться между локальными и общедоступными облачными средами.

Без современных возможностей микросегментации устаревшие межсетевые экраны не могут ограничить перемещение между облачными рабочими нагрузками, что позволяет программамвымогателям быстро распространяться.

В старых системах часто отсутствует глубокая проверка пакетов, аналитические каналы об угрозах и средства управления на уровне приложений, что делает их недоступными для сложных атак, нацеленных на современные приложения.

В общедоступных облаках часто используются встроенные средства управления безопасностью, в то время как в локальных системах используются устаревшие межсетевые экраны, что приводит к 32% неправильных настроек в гибридных инфраструктурах.

Злоумышленники часто нацеливаются на слабые звенья, такие как устаревшие агенты синхронизации идентификационных данных, и используют их для повышения привилегий как в локальной, так и в облачной среде. Чтобы снизить эти риски, организации должны внедрять межсетевые экраны нового поколения (NGFW), которые поддерживают архитектуру с нулевым уровнем доверия, автоматизированное внесение исправлений и обеспечивают единую видимость во всех средах.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ПЛАТФОРМАХ БЕЗОПАСНОСТИ

Искусственный интеллект внедряется в платформы безопасности для обеспечения возможности прогнозного обнаружения угроз. Модели искусственного интеллекта могут определять нормальные схемы трафика в гибридной сети и автономно выявлять аномалии, такие как внезапная попытка сервера базы данных установить исходящее соединение с неизвестным IP— адресом, которые указывают на нарушение.

Ключевые области применения искусственного интеллекта в облачной/гибридной безопасности:

- Обнаружение аномалий и угроз. Искусственный интеллект анализирует огромные объемы сетевого трафика, системные журналы и поведение пользователей в режиме реального времени, чтобы выявить закономерности, указывающие на кибератаки, такие как горизонтальные перемещения злоумышленников.
- Автоматическое реагирование на инциденты. Инструменты, управляемые искусственным интеллектом, могут изолировать скомпрометированные устройства, блокировать вредоносные IP-адреса и автономно применять исправления безопасности, сокращая время реагирования в среднем на 55%.
- Поведенческая аналитика (UEBA). Аналитика поведения пользователей и организаций создает базовые показатели нормальной активности для выявления отклонений, что помогает выявлять внутренние угрозы и атаки нулевого дня, особенно в сложных гибридных установках.
- Защита кода, созданного с помощью искусственного интеллекта. Платформы безопасности с использованием искусственного интеллекта (например, Snyk AI, Mend) сканируют код и зависимости с открытым исходным кодом на наличие уязвимостей во время разработки, в частности, устраняя уязвимости, которые могут быть вызваны инструментами кодирования с использованием искусственного интеллекта.
- Управление идентификацией и доступом (IAM). ИИ оценивает риск каждой попытки входа в систему, анализируя такие факторы, как поведение пользователя и географическое местоположение, чтобы при необходимости инициировать дополнительную проверку (например, MFA).
- ИИ предоставляет унифицированную видимость, объединяя данные из различных облачных сервисов для получения всестороннего представления об облачных рисках и уязвимостях.
- ИИ динамически настраивает политики безопасности и средства контроля доступа у разных облачных провайдеров, обеспечивая согласованное применение политик по мере миграции рабочих нагрузок.
- ИИ помогает создавать динамические границы для рабочих нагрузок, чтобы уменьшить вероятность атаки и предотвратить горизонтальное перемещение.

ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ДАННЫХ

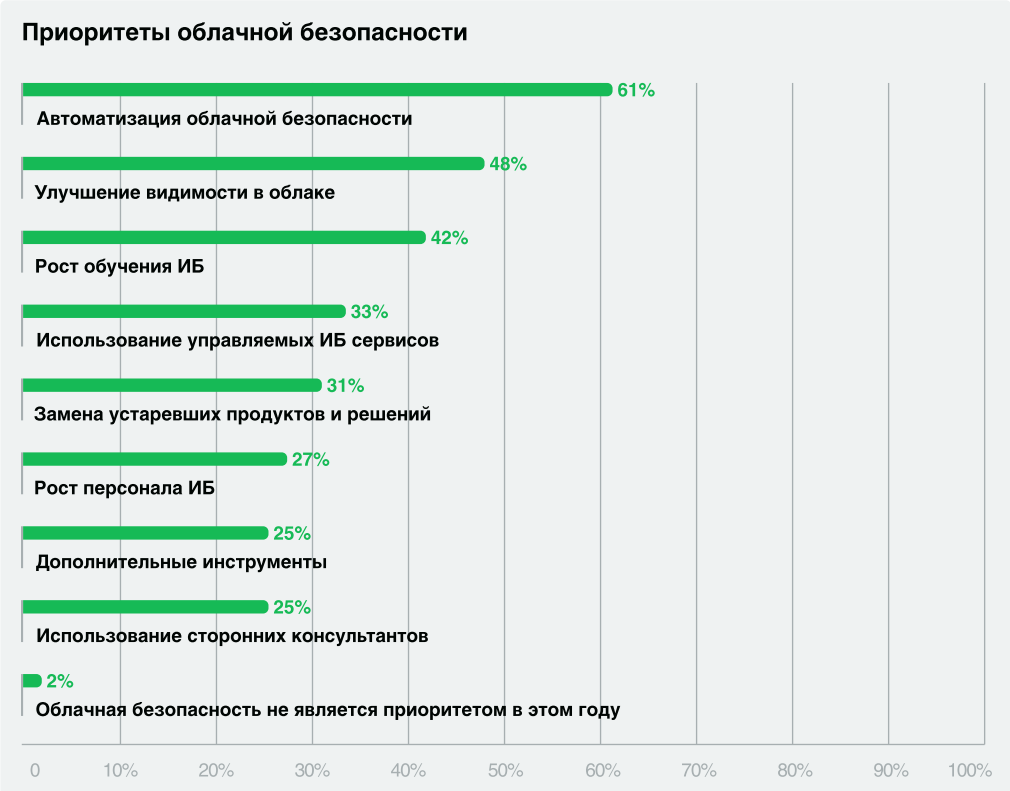
Предотвращение утечек данных (DLP) в облачной безопасности имеет решающее значение для обнаружения, мониторинга и защиты конфиденциальных данных от случайного или вредоносного воздействия при их перемещении по облачным средам. Это важно для обеспечения соблюдения нормативных требований, защиты интеллектуальной собственности, поддержания доверия клиентов и предотвращения серьезного финансового, операционного и репутационного ущерба от нарушений. По мере того как организации внедряют мультиоблачные и гибридные среды, данные становятся децентрализованными, что затрудняет их отслеживание без централизованного управления DLP.

Рисунок 23. Размещение критических данных. Источник: PaloAlto networks State of Cloud Security Report

НЕПРЕРЫВНЫЙ МОНИТОРИНГ

Неправильная настройка - распространенная уязвимость, и 67% респондентов либо используют, либо планируют внедрить автоматизированные средства для решения этой проблемы. Решения для непрерывного мониторинга и исправления ошибок в режиме реального времени позволяют заблаговременно выявлять риски, такие как неправильно настроенное хранилище или чрезмерные разрешения, и эффективно устранять их. Эти инструменты также упрощают соблюдение отраслевых нормативных требований.

Рисунок 24. Приоритеты облачной безопасности. Источник: 2026 CISO Budget Benchmark



БЕЗОПАСНОСТЬ ПРИЛОЖЕНИЙ

Безопасность на уровне приложений становится все более приоритетной задачей. Комплексная защита приложений от разработки до выполнения обеспечивает индивидуальную защиту рабочих нагрузок при одновременной поддержке согласованных политик в разных средах. Решения, которые интегрируются с контейнерными средами и средствами защиты во время выполнения, эффективно решают эту задачу.

Безопасность API и конфиденциальность данных: Защита API становится главным приоритетом по мере роста использования API, наряду с ужесточением требований к хранению и конфиденциальности данных.

Прогноз в области кибербезопасности облачных и гибридных инфраструктур в 2026 году

Распространение искусственного интеллекта: злоумышленники перейдут от использования ИИ в качестве исключения к рутинномуиспользованию для автоматизированных крупномасштабных эксплойтов. Злоумышленники будут использовать ИИ для перехода от первоначального доступа к боковому перемещению.

Agentic SOC: чтобы противостоять угрозам, управляемым искусственным интеллектом, команды безопасности будут использовать автономных агентов искусственного интеллекта для обнаружения, расследования и реагирования, переходя от ручного мониторинга к "непрерывному расследованию"

Непрерывное управление выявлением угроз (CTEM): периодическое сканирование "на определенный момент" станет устаревшим. Проактивное управление уязвимостями в режиме 24/7, которое позволяет отслеживать пути атак, заменит традиционное управление уязвимостями.

Идентификация как новый периметр: поскольку более 70% взломов облачных сервисов происходят из-за скомпрометированных учетных данных, решения для идентификации являются приоритетом национальной безопасности, что приводит к переходу к непрерывным поведенческим биометрическим проверкам доступа, управляемым искусственным интеллектом.

Распространение идентификационных данных, отличных от человеческих. 79% специалистов считают, что они не в состоянии справиться с ростом числа идентификационных данных, отличных от человеческих, таких как API-ключи, учетные записи служб и агенты искусственного интеллекта, которых сейчас больше, чем пользователей-людей.

Унифицированный GRC и облачный суверенитет: организации будут использовать инструменты унифицированного управления, контроля рисков и соответствия требованиям для работы с фрагментированными нормативными актами.

Бюджеты на программное обеспечение превысят расходы на персонал, поскольку организации будут автоматизировать системы кибербезопасности.

Выводы

Атаки на облачную систему безопасности сложны и постоянно меняются со временем. Они включают в себя утечку данных, захват учетных записей, программы-вымогатели и атаки на цепочки поставок, которые происходят в облачных средах. Эти атаки приводят к огромным штрафам, репутационному ущербу и проблемам с соблюдением требований регулирующих органов.

Различные направления и методы атак включают неправильно настроенные облачные сервисы, слабые средства контроля аутентификации и уязвимости в общих технологиях. Такие угрозы подталкивают организации к внедрению современных механизмов безопасности, выходящих за рамки их традиционных подходов к обеспечению безопасности.

Рисунок 25.
Основные трудности в обеспечении безопасности мультиоблачных сред.
Источник: Fortinet 2025 State of Cloud Security report

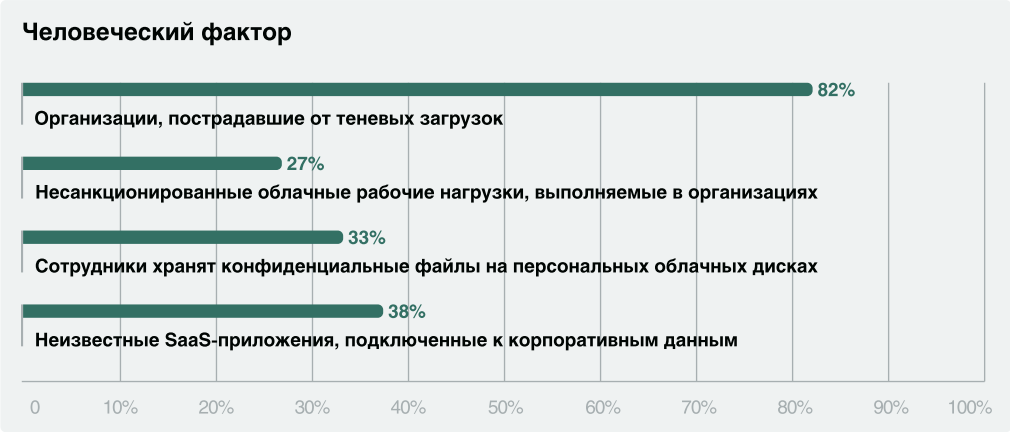
Интеграция межсетевых экранов нового поколения (NGFW) в гибридную облачную среду необходима для поддержания согласованных политик безопасности в локальных центрах обработки данных и общедоступных облачных инфраструктурах. Такой подход позволяет организациям распространить существующую систему безопасности на «облако», используя гибридную сетчатую модель брандмауэра для защиты трафика как в облако/из облака, так и межоблачного трафика.

Риск возникновения и реализации угроз в облаке высок, что означает необходимость использования надежных механизмов аутентификации. Под этим подразумевается не просто создание системы аутентификации с использованием имени пользователя и пароля. Вместо этого организациям придется внедрять многофакторную аутентификацию для всех учетных записей, особенно для тех, у которых больше разрешений, чем у других (привилегированных).

Рисунок 26.
Какие технологии конечные пользователи планируют использовать в 2026 году.
Источник: Fortinet 2025 State of Cloud Security report

Организации должны проводить регулярные аудиты и оценки безопасности для повышения безопасности в облаке. Для оценки следует использовать как внутренних экспертов, так и сторонние сервисы, чтобы гарантировать, что будут охвачено в аспекты (требования) обеспечения информационной безопасности. Некоторые из областей, которые необходимо охватить в ходе аудита безопасности, - это контроль доступа, меры сетевой безопасности, меры по защите данных от несанкционированного использования и соблюдение различных стандартов и положений.

Рисунок 25.
Основные трудности в обеспечении безопасности мультиоблачных сред.
Источник: Fortinet 2025 State of Cloud Security report



Человеческий фактор может быть одним из главных факторов, лежащих в основе нарушений, и надлежащая подготовка сотрудников во многом поможет предотвратить их. Обучение и повышение осведомленности персонала будут включать в себя такие темы, как выявление попыток фишинга, правильная обработка конфиденциальных данных, безопасное использование облачных сервисов и понимание важности политик безопасности.

Мониторинг утечек на сайте InfoWatch

На сайте Экспертно-аналитического центра InfoWatch регулярно публикуются отчеты по утечкам информации и самые громкие инциденты с комментариями экспертов InfoWatch.

СЛЕДИТЕ ЗА НОВОСТЯМИ УТЕЧЕК, НОВЫМИ ОТЧЕТАМИ, АНАЛИТИЧЕСКИМИ И ПОПУЛЯРНЫМИ СТАТЬЯМИ НА НАШИХ КАНАЛАХ:

Рассылка InfoWatch

infowatchout

infowatch